VPN

# Deploying Cisco ASA VPN Solutions

## Volume 2

Version 1.0

## Student Guide

Text Part Number: 97-2923-01

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

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

**Europe Headquarters**
Cisco Systems International BV Amsterdam,
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.**

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 2

## Deploying a Basic Clientless VPN Solution 4-3

## Deploying Advanced Application Access for Clientless SSL VPN 4-61

## Deploying Advanced Authentication and SSO in a Clientless SSL VPN 4-111

## Customizing the Clientless SSL VPN User Interface and Portal 4-155

## Module 3

# Deployment of Cisco ASA Adaptive Security Appliance AnyConnect Remote Access VPN Solutions

## Overview

The Cisco AnyConnect VPN Client and Cisco ASA adaptive security appliance acting as a Secure Sockets Layer (SSL) virtual private network (VPN) gateway provide full tunnel SSL VPN services to remote workers. This module describes how to deploy full tunnel SSL VPNs using basic and certificate-based authentication. The module also describes advanced deployments of Cisco AnyConnect VPN Client software.

## Module Objectives

Upon completing this module, you will be able to implement and maintain remote-access VPNs based on Cisco AnyConnect technology 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 basic features of a Cisco AnyConnect full tunnel SSL VPN
- Deploy and manage the advanced centrally configured features of the Cisco AnyConnect client
- Deploy and manage the advanced authentication features of a Cisco AnyConnect full tunnel SSL VPN

## Lesson 1

# Deploying a Basic Cisco AnyConnect Full Tunnel SSL VPN Solution

## Overview

A basic Cisco AnyConnect full tunnel Secure Sockets Layer (SSL) virtual private network (VPN) provides users with flexible client-based access to sensitive resources over a remote access VPN gateway, implemented on the Cisco ASA adaptive security appliance. A basic Cisco AnyConnect full tunnel SSL VPN uses basic user authentication by using usernames and passwords. It also provides IP address assignment to the full tunnel client from the Cisco ASA adaptive security appliance, and uses a basic access control policy. This lesson enables you to configure, verify, and troubleshoot a basic Cisco AnyConnect full tunnel SSL VPN solution.

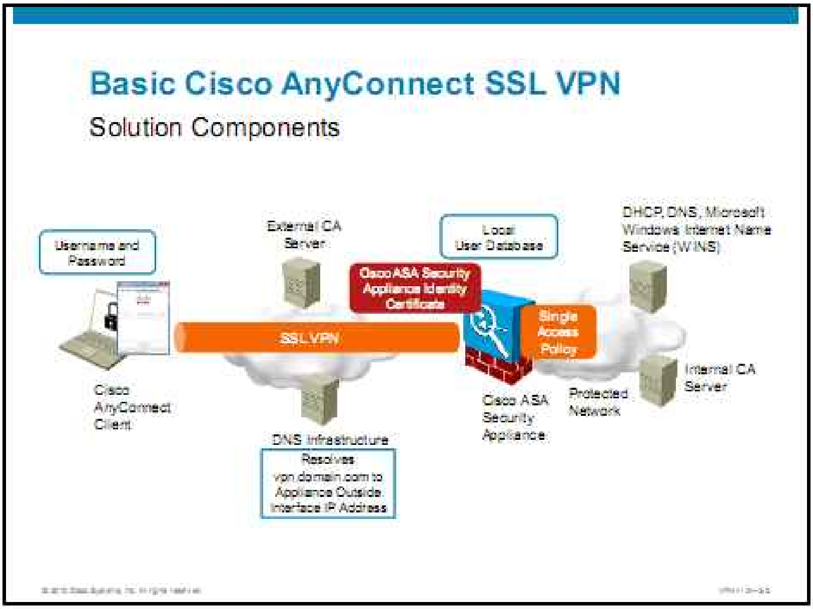
### Objectives

Upon completing this lesson, you will be able to deploy and manage basic features of Cisco AnyConnect full tunnel SSL VPNs. This ability includes being able to meet these objectives:

- Plan the configuration of a Cisco AnyConnect full tunnel SSL VPN solution
- Configure and verify basic Cisco ASA adaptive security appliance gateway features in Cisco AnyConnect full tunnel SSL VPNs
- Configure and verify password-based local user authentication in a Cisco AnyConnect full tunnel SSL VPN
- Configure and verify local IP address management, basic access control, and split tunneling in a Cisco AnyConnect full tunnel SSL VPN
- Install, configure, and verify the predeploy version of the Cisco AnyConnect client
- Troubleshoot VPN session establishment between a Cisco AnyConnect client and a Cisco ASA adaptive security appliance VPN gateway

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic provides an overview of how to plan the configuration of a Cisco AnyConnect full tunnel SSL VPN solution.



## Basic Cisco AnyConnect SSL VPN

Solution Components

Username and Password

Cisco AnyConnect Client

SSL VPN

External CA Server

DNS Infrastructure

Resolves vpn.domain.com to Appliance Outside Interface IP Address

Cisco ASA Security Appliance Identity Certificate

Local User Database

Cisco ASA Security Appliance

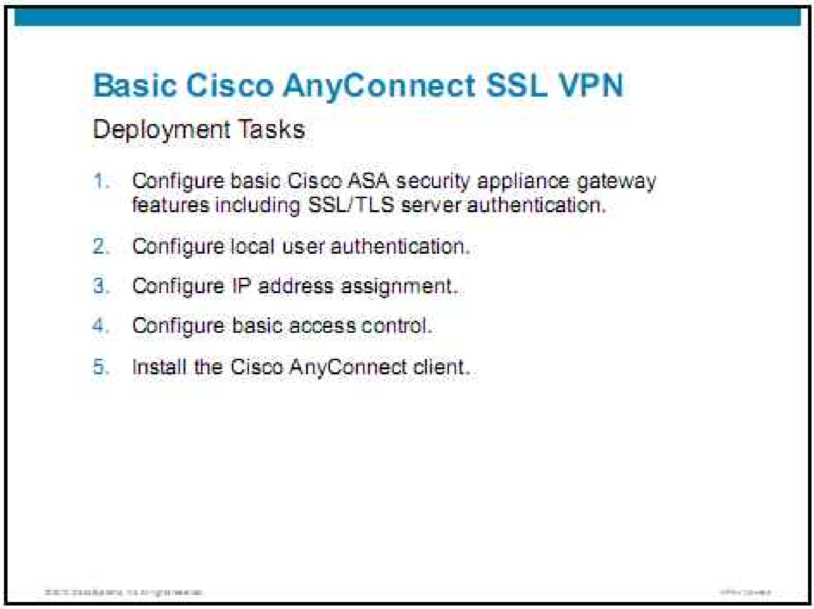
Single Access Policy

Protected Network

DHCP, DNS, Microsoft Windows Internet Name Service (WINS)

Internal CA Server

In a basic Cisco ASA adaptive security appliance full tunneling remote access Secure Sockets Layer (SSL) virtual private network (VPN) solution, remote users use the Cisco AnyConnect VPN Client to establish an SSL/Transport Layer Security (TLS) tunnel with the Cisco ASA adaptive security appliance. The basic solution uses bidirectional authentication, where the client authenticates the Cisco ASA adaptive security appliance with a certificate-based authentication method, and the Cisco ASA adaptive security appliance authenticates the user based on a username and password against its local user database. After authentication, the security appliance applies a set of authorization and accounting rules to the user session. After the Cisco ASA adaptive security appliance establishes an acceptable VPN environment with the remote user, the remote user can forward raw IP traffic into the SSL/TLS tunnel. This action occurs as the Cisco AnyConnect client creates a virtual network interface to provide this functionality. The client can use any application to access any resource behind the Cisco ASA adaptive security appliance VPN gateway, subject to access rules applied to the VPN session.



## Basic Cisco AnyConnect SSL VPN

Deployment Tasks

1. Configure basic Cisco ASA security appliance gateway features including SSL/TLS server authentication.
2. Configure local user authentication.
3. Configure IP address assignment.
4. Configure basic access control.
5. Install the Cisco AnyConnect client.

These are the general deployment tasks to create a basic Cisco AnyConnect full tunnel SSL VPN:

1. Configure the Cisco ASA adaptive security appliance with basic SSL VPN gateway features, including provisioning the identity certificate of the Cisco ASA adaptive security appliance to enable SSL/TLS server authentication.
2. Configure basic user authentication by configuring the local user database of the Cisco ASA adaptive security appliance by creating user accounts with static passwords.
3. Configure an IP address assignment method by using either IP address pools or per-user IP addresses that are configured locally on the Cisco ASA adaptive security appliance.
4. Configure basic access control, limiting access to the enterprise internal network.
5. Install the Cisco AnyConnect client on the remote PCs, and configure it to connect to the SSL VPN gateway.

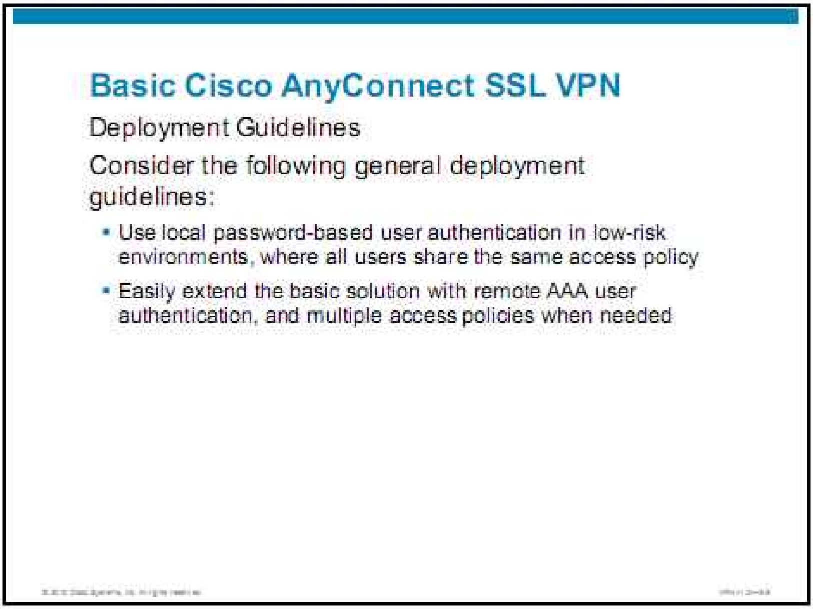
Before implementing a basic Cisco AnyConnect full tunnel SSL VPN, you will need to obtain and analyze several pieces of information that are related to the network and system environment:

- The IP addressing plan that will dictate the VPN gateway addressing, and the enterprise naming plan that will dictate the name of the VPN gateway. This data is needed to assign an IP address to the Cisco ASA adaptive security appliance VPN-terminating interface, and to assign a name inside the VPN gateway SSL/TLS identity certificate.
- The enterprise certificate policy and certificate settings. This information is needed in order to enroll the Cisco ASA adaptive security appliance into a public key infrastructure (PKI) (if so desired) and include all relevant fields inside a PKI-provisioned certificate.
- The enterprise policy for the user-naming format and the enterprise password policy, in order to create the local user database on the Cisco ASA adaptive security appliance.
- The enterprise cryptographic policy, in order to choose the optimal SSL/TLS protocol versions and algorithm bundles (cipher suites) for SSL/TLS sessions on the Cisco ASA adaptive security appliance.

- The IP addressing plan for remote clients. In a full tunneling SSL VPN, the Cisco ASA adaptive security appliance must assign IP addresses to remote clients, and these addresses must be unique and routed to the Cisco ASA adaptive security appliance in order for VPN connectivity to work.

- Access policies that dictate which sensitive internal resources the remote users can access. This information is needed to configure an access control policy on the Cisco ASA adaptive security appliance that will be applied to remote access VPN sessions.

- A list of client platforms of remote users. This information is needed to correctly provision the Cisco AnyConnect software images to the remote users, and to store on the Cisco ASA adaptive security appliance flash memory.



## Basic Cisco AnyConnect SSL VPN

Deployment Guidelines

Consider the following general deployment guidelines:

- Use local password-based user authentication in low-risk environments, where all users share the same access policy
- Easily extend the basic solution with remote AAA user authentication, and multiple access policies when needed

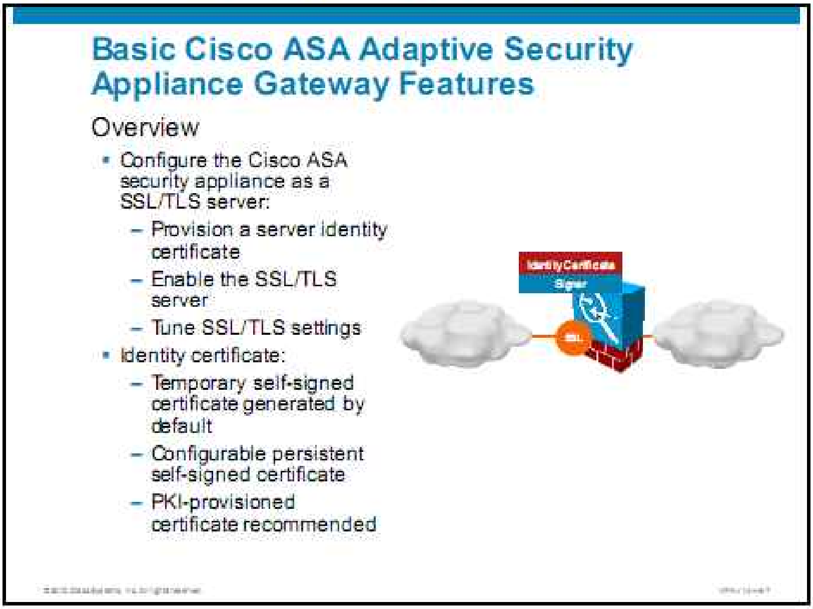
Consider the following deployment guidelines when deploying a basic Cisco AnyConnect full tunnel SSL VPN solution:

- Use local password-based user authentication in low-risk environments where all users share the same access policy

- Easily extend the basic solution with remote authentication, authorization, and accounting (AAA) user authentication and multiple access policies when needed

# Configuring Basic Cisco ASA Adaptive Security Appliance SSL VPN Gateway Features

This topic enables you to configure and verify basic Cisco ASA adaptive security appliance SSL VPN gateway features in Cisco AnyConnect full tunnel SSL VPNs.



## Basic Cisco ASA Adaptive Security Appliance Gateway Features

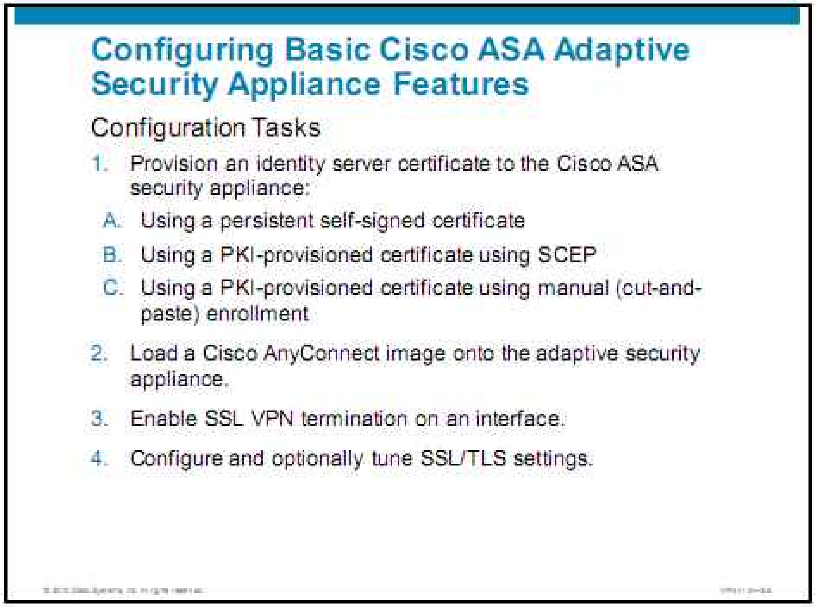
Overview

- Configure the Cisco ASA security appliance as a SSL/TLS server:
  - Provision a server identity certificate
  - Enable the SSL/TLS server
  - Tune SSL/TLS settings
- Identity certificate:
  - Temporary self-signed certificate generated by default
  - Configurable persistent self-signed certificate
  - PKI-provisioned certificate recommended

The first deployment step when configuring a full tunnel SSL VPN solution is to configure basic SSL/TLS server parameters on the Cisco ASA adaptive security appliance. This step includes provisioning a server identity certificate, which the Cisco ASA adaptive security appliance will send to remote clients so that they can authenticate the Cisco ASA adaptive security appliance. This step also includes enabling the SSL/TLS server functionality on an interface, and optionally tuning SSL/TLS parameters to be compliant with local cryptographic policies.

By default, the security appliance will create a self-signed X.509 certificate on each reboot, resulting in many client warnings when you attempt SSL VPN access, as the certificate cannot be verified by any means. You can address this issue by using one of two approaches:

- By creating a permanent self-signed certificate that is persistent across reboots, and that you can save on the client. This approach is possible if the remote users have the option of initially accessing the Cisco ASA adaptive security appliance over a trusted network and saving the identity certificate of the appliance to their local storage. This approach is usually not supported by most clients and is generally not recommended.
- By enrolling the Cisco ASA adaptive security appliance into an existing PKI, with the clients authenticating the identity certificate of the appliance on each access by validating it using a relevant certificate authority (CA) certificate that was used to issue the identity certificate of the security appliance. This CA certificate needs to be preprovisioned to all clients in order for such authentication to work.



## Configuring Basic Cisco ASA Adaptive Security Appliance Features

### Configuration Tasks

1. Provision an identity server certificate to the Cisco ASA security appliance:
   - A. Using a persistent self-signed certificate
   - B. Using a PKI-provisioned certificate using SCEP
   - C. Using a PKI-provisioned certificate using manual (cut-and-paste) enrollment
2. Load a Cisco AnyConnect image onto the adaptive security appliance.
3. Enable SSL VPN termination on an interface.
4. Configure and optionally tune SSL/TLS settings.

To configure basic Cisco ASA adaptive security appliance SSL VPN gateway features, complete the following configuration tasks:

1. Provision an identity server SSL/TLS certificate to the Cisco ASA adaptive security appliance. The security appliance will use this certificate to identify itself to remote clients, and, based on this certificate, remote clients will be able to authenticate the Cisco ASA adaptive security appliance. You have three options to install a certificate on the Cisco ASA adaptive security appliance:

   — Option A is to create and install a permanent self-signed certificate that is persistent across reboots.

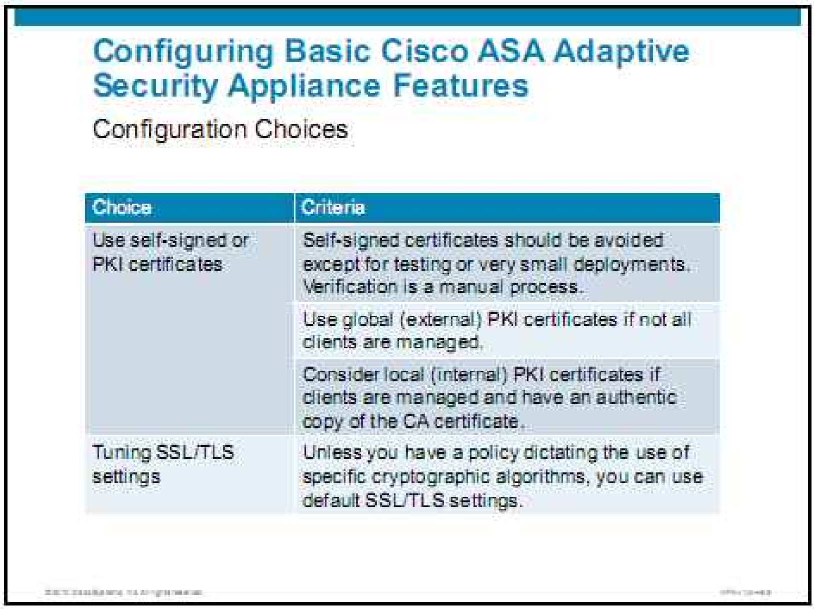
   — Option B is to create and install a persistent, PKI-provisioned certificate by enrolling the Cisco ASA adaptive security appliance into an existing PKI. You can use either a PKI internal to your organization, an externally managed PKI, or an external, global PKI. In option B, you will use the Simple Certificate Enrollment Protocol (SCEP) to enroll to the PKI and obtain an identity certificate.

   — Option C is essentially the same as option B, but should be used with PKIs that do not support SCEP enrollment. Instead, you will use manual (cut-and-paste) enrollment by exchanging raw enrollment data with the PKI manually.

2. Load a Cisco AnyConnect client software image onto the Cisco ASA adaptive security appliance, placing it into the persistent flash storage of the security appliance.

3. Enable SSL VPN traffic termination on a Cisco ASA adaptive security appliance interface, and therefore enable the security appliance SSL VPN server function.

4. Configure and optionally tune the SSL/TLS settings. You will need to assign the installed identity certificate of the Cisco ASA adaptive security appliance to the chosen VPN traffic termination interface. Optionally, you will need to choose SSL/TLS versions and algorithm bundles (cipher suites) that you desire to use for traffic encapsulation.



## Configuring Basic Cisco ASA Adaptive Security Appliance Features

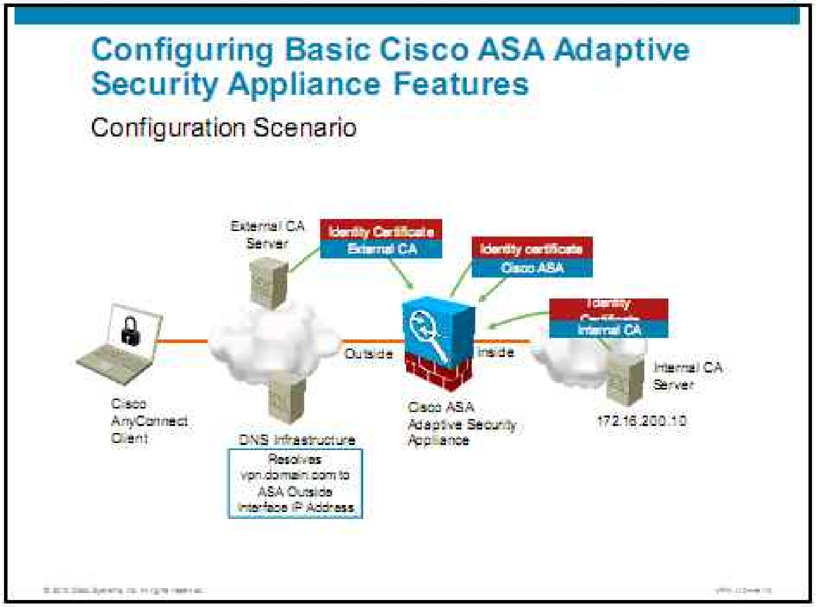
Configuration Choices

| Choice | Criteria |
|---|---|
| Use self-signed or PKI certificates | Self-signed certificates should be avoided except for testing or very small deployments. Verification is a manual process. |
| | Use global (external) PKI certificates if not all clients are managed. |
| | Consider local (internal) PKI certificates if clients are managed and have an authentic copy of the CA certificate. |
| Tuning SSL/TLS settings | Unless you have a policy dictating the use of specific cryptographic algorithms, you can use default SSL/TLS settings. |

There are several configuration choices that you need to make based on locally significant criteria.

The first choice is whether you will use self-signed or PKI-provisioned certificates. Using any kind of self-signed certificate is generally not recommended, as the clients typically cannot verify it properly if they do not already have an authentic copy of it locally preinstalled. Self-signed certificates should generally only be used for test purposes, and not for production use over untrusted networks. Deploying a permanent self-signed certificate is simpler compared to using PKI-provisioned certificates, as it requires no interaction with the PKI. However, using a PKI-provisioned certificate is a recommended and a more scalable solution. You can use a local (internal to the enterprise, or a managed, private PKI service) PKI if all of your clients are managed, and you can be reasonably sure that all clients have an authentic copy of the CA certificate installed. Alternatively, you should use a certificate from a global PKI if not all of your clients are managed and you have to rely on the operating system default store of global CA certificates (trusted roots).

The second choice involves tuning the SSL/TLS settings of the Cisco ASA adaptive security appliance SSL/TLS server function. You may consider tuning these settings if you have a local policy dictating the use of particular SSL/TLS protocol types, or particular cryptographic algorithms. In most cases, the default Cisco ASA adaptive security appliance SSL/TLS settings are optimal for most users.



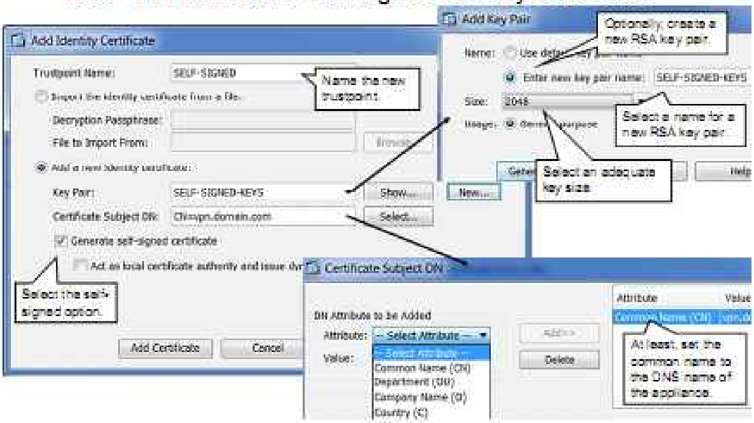
## Configuring Basic Cisco ASA Adaptive Security Appliance Features

Configuration Scenario

The figure presents the configuration scenario that is used in upcoming configuration tasks. The Cisco ASA adaptive security appliance can either issue a self-signed certificate, or receive its identity certificate from an external or internal CA server. You will also need to configure your Domain Name System (DNS) infrastructure to resolve the name of the Cisco ASA adaptive security appliance (inside its identity certificate) to its VPN-terminating interface IP address (the IP address of the outside interface in the example).

## Configuring Basic Cisco ASA Adaptive Security Appliance Features

### Task 1A: Provision a Self-signed Identity Certificate



Add Identity Certificate

Trustpoint Name: SELF-SIGNED

○ Import the identity certificate from a file:

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: SELF-SIGNED-KEYS

Certificate Subject DN: CN=vpn.domain.com

☑ Generate self-signed certificate

□ Act as local certificate authority and issue dy

Add Key Pair

Name: ○ Use default key pair name

● Enter new key pair name: SELF-SIGNED-KEYS

Size: 2048

Usage: ● General purpose

Certificate Subject DN

DN Attribute to be Added

Attribute: -- Select Attribute --

Value:

| Attribute | Value |
|---|---|
| Common Name (CN) | vpn.d |

Name the new trustpoint.

Optionally, create a new RSA key pair.

Select a name for a new RSA key pair.

Select an adequate key size.

Select the self-signed option.

At least, set the common name to the DNS name of the appliance.

Configuration > Device Management > Certificate Management > Identity Certificates

In the first task, you will generate a permanent self-signed certificate that does not change across Cisco ASA adaptive security appliance reboots. The use of a permanent self-signed certificate is discouraged, as it offers little benefit over the temporary self-signed certificate.

To deploy a new permanent self-signed certificate, perform the following steps:

**Step 1** Using Cisco Adaptive Security Device Manager (Cisco ASDM), choose **Configuration > Device Management > Certificate Management > Identity Certificates** (not shown in the figure).

**Step 2** Click **Add** to create a new PKI trustpoint. Assign a local name to the new trustpoint.

**Step 3** Choose **Add a New Identity Certificate**, and choose the named Rivest, Shamir, and Adleman (RSA) key pair to be used as the basis for the SSL VPN server certificate.

**Step 4** Optionally, create an RSA key pair of appropriate strength by clicking the **New** button. It is recommended to create a separate key pair for each trustpoint. Make sure that you generate a key of appropriate strength (key size).

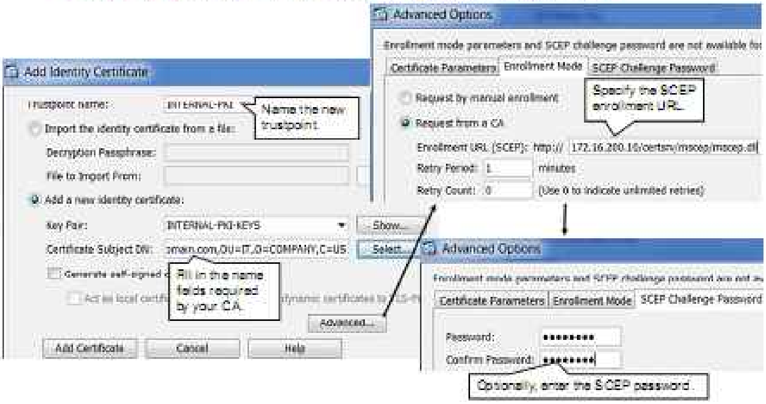
**Step 5** In the Certificate Subject DN field, enter the canonical name of the security appliance in the form of CN=hostname.domainname (you can click the **Select** button to construct a more complex subject name, if needed; however, this is not required for self-signed certificates).

**Step 6** Check the **Generate Self-signed Certificate** check box.

**Step 7** Click **Add Certificate** to immediately generate the permanent self-signed X.509 certificate.

## Configuring Basic Cisco ASA Adaptive Security Appliance Features

Task 1B: Provision a PKI Identity Certificate Using SCEP



Add Identity Certificate

Trustpoint name: INTERNAL-PKI

○ Import the identity certificate from a file:

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: INTERNAL-PKI-KEYS

Certificate Subject DN: omain.com,OU=IT,O=COMPANY,C=US

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for

○ Request by manual enrollment

● Request from a CA

Enrollment URL (SCEP): http:// 172.16.200.16/certsrv/mscep/mscep.dll

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimited retries)

Advanced Options

Enrollment mode parameters and SCEP challenge password are not av

Password: ••••••••

Confirm Password: ••••••••

Name the new trustpoint.

Fill in the name fields required by your CA.

Specify the SCEP enrollment URL.

Optionally, enter the SCEP password.

Configuration > Device Management > Certificate Management > Identity Certificates

Alternatively, you can deploy a PKI-provisioned certificate to the security appliance. This procedure is similar to installing a self-signed certificate, except that you have to forward your certificate request (containing the Cisco ASA adaptive security appliance name and public RSA key) to a PKI enrollment server (a registration authority or a certificate authority).

Perform the following steps:

**Step 1** Ensure that the Cisco ASA adaptive security appliance hostname and domain name are set correctly.

**Step 2** Optionally, if you have not already done so, create an RSA key pair of appropriate strength. Or you can reuse existing keys, if they are of appropriate strength.

**Step 3** Using Cisco ASDM, choose **Configuration > Device Management > Certificate Management > Identity Certificates** (not shown in the figure).

**Step 4** Click **Add** to create a new PKI trustpoint. Assign a local name to the new trustpoint.

**Step 5** Choose **Add a New Identity Certificate**, and select an RSA key pair (or create a new key pair) to be used as the basis for the HTTPS server certificate.

**Step 6** In the Certificate Subject DN field, enter the canonical name of the security appliance in the form of CN=hostname.domainname (you can click the **Select** button to construct a more complex subject name if needed).

**Step 7** Click the **Advanced** button to display PKI enrollment parameters.

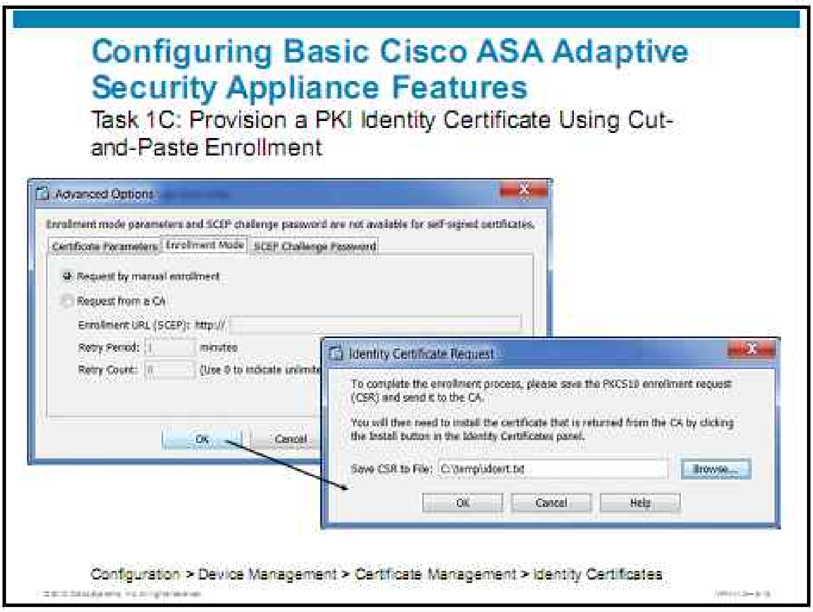
**Step 8** In the Certificate Parameters tab, verify that the fully qualified domain name (FQDN) is properly set to the appliance hostname and domain name (not shown in the figure).

**Step 9** In the Enrollment Mode tab, click the **Request from a CA** radio button. Enter the enrollment parameters (like the enrollment URL) depending on the PKI that you are using.

Use the SCEP Challenge Password tab to optionally enter the SCEP password if required by the PKI CA server.

**Step 10** Click **Add Certificate** to generate the certificate request.

**Step 11** When the PKI approves your certificate request, choose your request and click **Install** to install the identity certificate.



## Configuring Basic Cisco ASA Adaptive Security Appliance Features

Task 1C: Provision a PKI Identity Certificate Using Cut-and-Paste Enrollment

Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

● Request by manual enrollment

○ Request from a CA

Enrollment URL (SCEP): http://

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimite

Identity Certificate Request

To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.

You will then need to install the certificate that is returned from the CA by clicking the Install button in the Identity Certificates panel.

Save CSR to File: C:\temp\idcert.txt

Configuration > Device Management > Certificate Management > Identity Certificates

If the PKI does not support SCEP enrollment, you can also enroll using a manual cut-and-paste method. In this method, you will generate a certificate request, and then send this request (as a file, or paste it into a PKI enrollment user interface) to a PKI certificate or registration authority. The CA will issue you a certificate (in the form of a file, or as text data) that you can copy and paste into the Cisco ASA adaptive security appliance.

Perform the following steps in order to complete the cut-and-paste enrollment method:

**Step 1** Using Cisco ASDM, choose **Configuration > Device Management > Certificate Management > Identity Certificates** (not shown in the figure).

**Step 2** Click **Add** to create a new PKI trustpoint. Assign a local name to the new trustpoint (not shown in the figure).

**Step 3** Choose **Add a New Identity Certificate**, and choose an RSA key pair (or create a new key pair) to be used as the basis for the HTTPS server certificate (not shown in the figure).

**Step 4** In the Certificate Subject DN field, enter the canonical name of the security appliance in the form of CN=hostname.domainname (you can click the **Select** button to construct a more complex subject name if needed) (not shown in the figure).

**Step 5** Click the **Advanced** button to display PKI enrollment parameters (not shown in figure).

**Step 6** In the **Certificate Parameters** tab, verify that the FQDN is properly set to the appliance hostname and domain name (not shown in the figure).

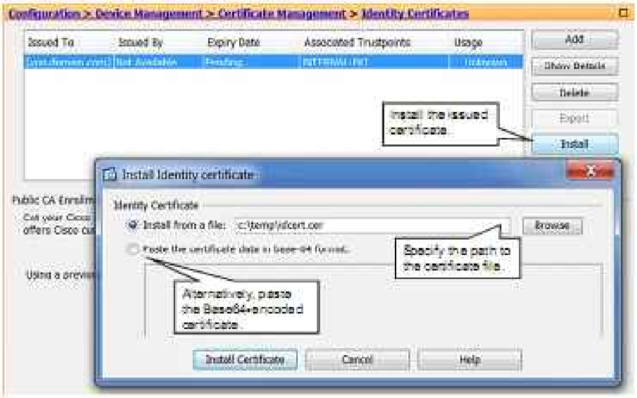
**Step 7** In the Enrollment Mode tab, choose the **Request by Manual Enrollment** (cut-and-paste) method. Enter the enrollment parameters depending on the PKI that you are using.

**Step 8** Click **Add Certificate** to generate the certificate request (not shown in the figure).

**Step 9** Save the certificate signing request (CSR) data into a file and use it to enroll into the PKI.

## Configuring Basic Cisco ASA Adaptive Security Appliance Features

Task 1C: Provision a PKI Identity Certificate Using Cut-and-Paste Enrollment (Cont.)



Configuration > Device Management > Certificate Management > Identity Certificates

| Issued To | Issued By | Expiry Date | Associated Trustpoints | Usage |
|---|---|---|---|---|
| [illegible] | Not Available | Pending | INTERNAL-PKI | Unknown |

Install Identity certificate

Identity Certificate

● Install from a file: c:\temp\idcert.cer

○ Paste the certificate data in base-64 format:

Install the issued certificate.

Specify the path to the certificate file.

Alternatively, paste the Base64-encoded certificate.

Configuration > Device Management > Certificate Management > Identity Certificates

To finish the manual enrollment procedure, perform these steps:

**Step 1** When the PKI approves your certificate request, obtain the certificate file or text data, and import it to the Cisco ASA adaptive security appliance as a file, or paste it into the Cisco ASDM GUI.

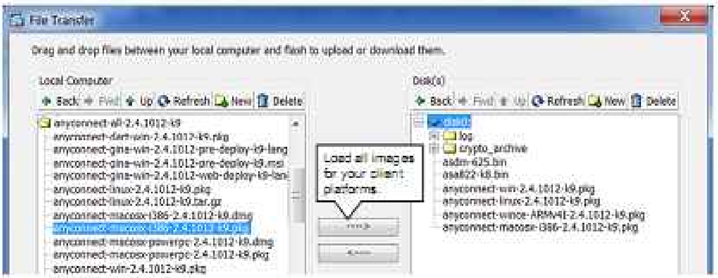
**Step 2** Choose **Configuration > Device Management > Certificate Management > Identity Certificates** and select the trustpoint that was configured in one of the previous steps.

**Step 3** Choose **Install Certificate** to install the identity certificate that was obtained from the CA by selecting the certification file or by manually pasting in the Base64-encoded certificate.

## Configuring Basic Cisco ASA Adaptive Security Appliance Features

### Task 2: Load a Cisco AnyConnect Image onto the Cisco ASA Adaptive Security Appliance

- Download Cisco AnyConnect PKG packages from Cisco.com
- Load them into the flash memory of the appliance
- Download and copy PKGs for all required platforms to the appliance



File Transfer

Drag and drop files between your local computer and flash to upload or download them.

Local Computer

```
anyconnect-all-2.4.1012-k9
  anyconnect-dart-win-2.4.1012-k9.pkg
  anyconnect-gina-win-2.4.1012-pre-deploy-k9-lang
  anyconnect-gina-win-2.4.1012-pre-deploy-k9.msi
  anyconnect-gina-win-2.4.1012-web-deploy-k9-lan
  anyconnect-linux-2.4.1012-k9.pkg
  anyconnect-linux-2.4.1012-k9.tar.gz
  anyconnect-macosx-i386-2.4.1012-k9.dmg
  anyconnect-macosx-i386-2.4.1012-k9.pkg
  anyconnect-macosx-powerpc-2.4.1012-k9.dmg
  anyconnect-macosx-powerpc-2.4.1012-k9.pkg
  anyconnect-win-2.4.1012-k9.pkg
```

Disk(s)

```
disk0:
  log
  crypto_archive
  asdm-625.bin
  asa822-k8.bin
  anyconnect-win-2.4.1012-k9.pkg
  anyconnect-linux-2.4.1012-k9.pkg
  anyconnect-wince-ARMv4I-2.4.1012-k9.pkg
  anyconnect-macosx-i386-2.4.1012-k9.pkg
```

Load all images for your client platforms.

Tools > File Management

In Task 2 of the configuration sequence, download the Cisco AnyConnect web deployment client software packages from Cisco.com, and transfer them to the Cisco ASA adaptive security appliance flash memory. You should transfer the PKG format of the Cisco AnyConnect software image to the Cisco ASA adaptive security appliance (as shown in the figure), for all client platforms that you intend to use. The Cisco ASA adaptive security appliance will use these web deployment (or web launch) packages to dynamically install the Cisco AnyConnect client to all users visiting the SSL VPN portal, if so configured.

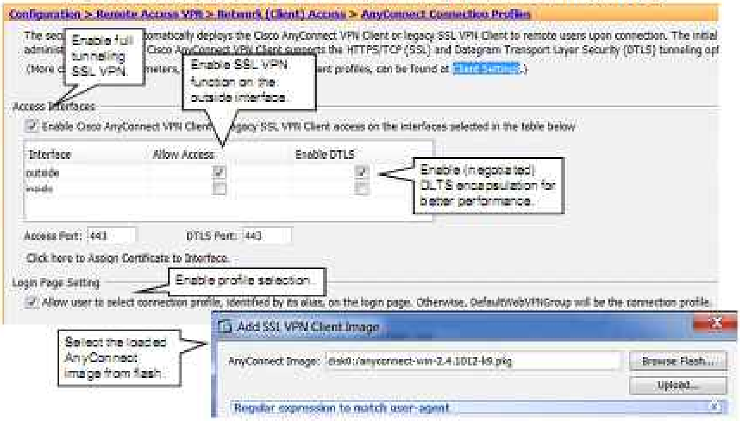
**Note** In the configuration scenario example that is used in this lesson, you will also be shown how to use the predeployment (Microsoft Windows Installer [MSI]) installer package, and not the web deployment package. However, installing a web deployment is a mandatory step in the SSL VPN gateway configuration.

If you are using Cisco ASDM, you can use the ASDM File Transfer user interface from the **Tools > File Management** ASDM menu to transfer these files from your local storage location to the Cisco ASA adaptive security appliance.

**Note** The Cisco AnyConnect client that is loaded on the Cisco ASA adaptive security appliance is a Microsoft Windows-based client. Other operating system environments are also supported.

## Configuring Basic Cisco ASA Adaptive Security Appliance Features

### Task 3: Enable SSL VPN Termination on an Interface



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

The sec... ...tomatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial administ... Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling opt (More c... ...meters, ...ent profiles, can be found at Client Settings.)

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client ...gacy SSL VPN Client access on the interfaces selected in the table below

| Interface | Allow Access | Enable DTLS |
|---|---|---|
| outside | ☑ | ☑ |
| inside | □ | □ |

Access Port: 443 DTLS Port: 443

Click here to Assign Certificate to Interface.

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

Add SSL VPN Client Image

AnyConnect Image: disk0:/anyconnect-win-2.4.1012-k9.pkg

Enable full tunneling SSL VPN.

Enable SSL VPN function on the outside interface.

Enable (negotiated) DLTS encapsulation for better performance.

Enable profile selection.

Select the loaded AnyConnect image from flash.

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

In Task 3, you will globally enable the SSL VPN function on the Cisco ASA adaptive security appliance, and select the interfaces on which the appliance will accept SSL VPN sessions. You can also optionally configure support for Datagram Transport Layer Security (DTLS), which will be automatically negotiated if the path between the client and the Cisco ASA adaptive security appliance supports it. Additionally, you will enable user connection profile selection, which is required if you want to assign users into a specific connection profile, and not use the default DefaultWebVPNGroup profile for all users.

Perform the following steps:

**Step 1** In the Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

**Step 2** Choose **Enable Cisco AnyConnect VPN Client or Legacy SSL VPN Client Access** check box to globally enable SSL VPN functionality. A window appears, asking you to continue to designate a Cisco AnyConnect image, click **Yes** to continue.

**Step 3** The Add SSL VPN Client Image window appears, prompting you to select a Cisco AnyConnect image that the Cisco ASA adaptive security appliance will use to deploy the client to users who use a browser to initially connect to the full tunneling VPN. Select the .pkg image in the Cisco ASA adaptive security appliance flash that you have previously uploaded. You can also upload an image at this point.

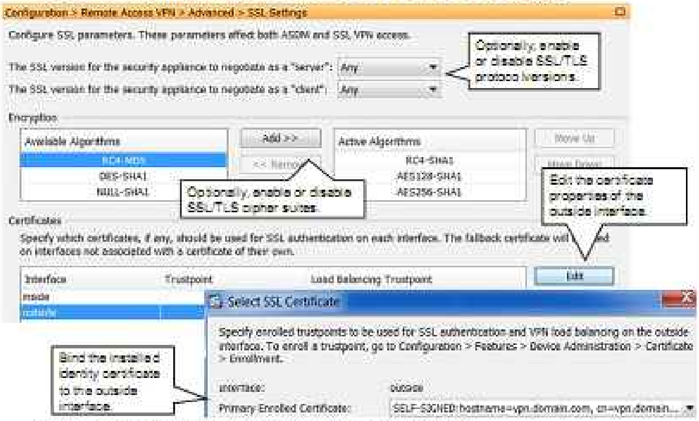
**Step 4** Check the **Allow Access** check box, and optionally check the **Enable DTLS** check box, on the interface on which you want to terminate SSL VPN connections. In this example, these connections are enabled on the outside interface. It is generally recommended to enable DTLS access to provide low-latency tunneling to support real-time applications, such as software IP phones.

**Step 5** In the Login Page Setting, check the **Allow User to Select Connection Profile** check box to allow users to select their connection profile at login.

**Step 6** Click **Apply** and save your configuration, if necessary.

## Configuring Basic Cisco ASA Adaptive Security Appliance Features

### Task 4: Configure and Tune SSL/TLS Settings



Configuration > Remote Access VPN > Advanced > SSL Settings

Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

The SSL version for the security appliance to negotiate as a "server": Any

The SSL version for the security appliance to negotiate as a "client": Any

Encryption

| Available Algorithms | Active Algorithms |
|---|---|
| RC4-MD5 | RC4-SHA1 |
| DES-SHA1 | AES128-SHA1 |
| NULL-SHA1 | AES256-SHA1 |

Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate wil ed on interfaces not associated with a certificate of their own.

| Interface | Trustpoint | Load Balancing Trustpoint |
|---|---|---|
| inside | | |
| outside | | |

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the outside interface. To enroll a trustpoint, go to Configuration > Features > Device Administration > Certificate > Enrollment.

Interface: outside

Primary Enrolled Certificate: SELF-SIGNED:hostname=vpn.domain.com, cn=vpn.domain...

Optionally, enable or disable SSL/TLS protocol versions.

Optionally, enable or disable SSL/TLS cipher suites.

Edit the certificate properties of the outside interface.

Bind the installed identity certificate to the outside interface.

Configuration > Remote Access VPN > Advanced > SSL Settings

In Task 4, you need to attach the installed identity certificate of the Cisco ASA adaptive security appliance to the appropriate network interface that you configured for SSL VPN termination.

Perform the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Advanced > SSL Settings** (or choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**, and click the **Click Here to Assign Certificate to Interface** link).

**Step 2** At the top of the SSL Settings pane, you can select the SSL and TLS protocol versions that the appliance will support as the SSL/TLS server. If you need to change the default values, you have the following options:

### SSL Settings

| Value | Description |
|---|---|
| any | The adaptive security appliance accepts SSL version 2 (SSLv2) client hellos, and negotiates either SSL version 3 (SSLv3) or TLS version 1 (TLSv1). This option is selected by default. |
| Negotiate SSL v3 | The adaptive security appliance accepts SSLv2 client hellos, and negotiates to SSLv3. |
| SSL v3 only | The security appliance accepts only SSLv3 client hellos, and uses only SSLv3. |
| Negotiate TLS v1 | The adaptive security appliance accepts SSLv2 client hellos, and negotiates to TLSv1. |
| TLS v1 only | The security appliance accepts only TLSv1 client hellos, and uses only TLSv1. |

**Step 3**

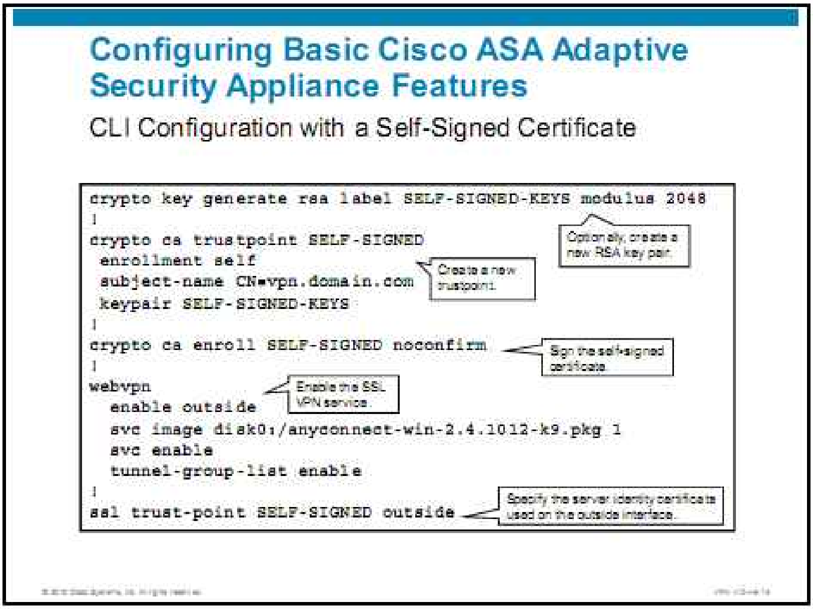
**Step 4** In the Encryption section of the SSL Settings pane, you can select or deselect the cryptographic algorithm bundles (cipher suites) that the Cisco ASA adaptive security appliance will accept in the initial SSL/TLS negotiation. If you need to change these settings based on a local cryptographic policy, you can enable or disable specific bundles in this pane.

**Step 5** In the SSL Settings pane, where the interfaces are listed, click **Edit** to edit the interface (or interfaces) on which the security appliance will accept SSL VPN connections.

**Step 6** In the Primary Enrolled Certificate drop-down menu, choose the installed identity certificate of the Cisco ASA adaptive security appliance.

**Step 7** Click **OK**, and click **Apply**.

**Step 8** Save your configuration, if necessary.



## Configuring Basic Cisco ASA Adaptive Security Appliance Features

CLI Configuration with a Self-Signed Certificate

```
crypto key generate rsa label SELF-SIGNED-KEYS modulus 2048
!
crypto ca trustpoint SELF-SIGNED
 enrollment self
 subject-name CN=vpn.domain.com
 keypair SELF-SIGNED-KEYS
!
crypto ca enroll SELF-SIGNED noconfirm
!
webvpn
  enable outside
  svc image disk0:/anyconnect-win-2.4.1012-k9.pkg 1
  svc enable
  tunnel-group-list enable
!
ssl trust-point SELF-SIGNED outside
```

Optionally, create a new RSA key pair.

Create a new trustpoint.

Sign the self-signed certificate.

Enable the SSL VPN service.

Specify the server identity certificate used on the outside interface.

This output shows the command-line interface (CLI) commands that are required to configure the basic Cisco ASA adaptive security appliance SSL VPN gateway features using a self-signed identity certificate of the appliance.

In the CLI, use the **crypto key generate** command to generate an RSA key pair, if required. Use the **crypto ca trustpoint** command to create a self-signed trustpoint. Inside the trustpoint configuration, use the **enrollment self** command to specify that this trustpoint will automatically generate a persistent self-signed certificate upon enrollment. Use the **subject-name** command to specify the name that the Cisco ASA adaptive security appliance will use inside its identity certificate. Optionally, use the **keypair** command to specify the dedicated RSA key pair (if generated) that the Cisco ASA adaptive security appliance will use when generating the self-signed certificate.

Next, use the **crypto ca enroll** command to actually generate the self-signed certificate based on the trustpoint settings.

Next, enter SSL VPN server configuration submode on the Cisco ASA adaptive security appliance using the **webvpn** command, and enable the SSL VPN server on the outside interface using the **enable** command. Designate the Cisco AnyConnect image that is present in the local Cisco ASA adaptive security appliance storage using the **svc image** command, and enable full tunnel SSL VPN connections using the **svc enable** command. To finish the configuration, enable user selection of connection profiles using the **tunnel-group-list enable** command.

Finally, assign the installed self-signed interface to the SSL-VPN-enabled interface by using the **ssl trust-point** command.

## crypto key generate rsa

To generate RSA key pairs for identity certificates, use the **crypto key generate rsa** command in global configuration mode.

**crypto key generate rsa** [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

### crypto key generate rsa Parameters

| Parameter | Description |
|---|---|
| `general-keys` | Generates a single pair of general-purpose keys. This type is the default key pair. |
| `label` *`key-pair-label`* | Specifies the name to be associated with the key pair (or pairs). This key pair must be uniquely labeled. If you attempt to create another key pair with the same label, the adaptive security appliance displays a warning message. If no label is provided when the key is generated, the key pair is statically named <Default-RSA-Key>. |
| `modulus` *`size`* | Specifies the modulus size of the key pair (or pairs): 512, 768, 1024, and 2048. The default modulus size is 1024. |
| `noconfirm` | Suppresses all interactive prompting. |
| `usage-keys` | Generates two key pairs, one for signature use and one for encryption use. The implication is that two certificates for the corresponding identity are required. |

## crypto ca trustpoint

To enter trustpoint configuration mode for the specified trustpoint, use the **crypto ca trustpoint** command in global configuration mode. To remove the specified trustpoint, use the **no** form of this command.

**crypto ca trustpoint** *trustpoint-name*

**no crypto ca trustpoint** *trustpoint-name* [**noconfirm**]

### crypto ca trustpoint Parameters

| Parameter | Description |
|---|---|
| `noconfirm` | Suppresses all interactive prompting. |
| *`trustpoint-name`* | Identifies the name of the trustpoint to manage. The maximum name length is 128 characters. |

## subject-name (crypto ca trustpoint)

To include the indicated subject distinguished name (DN) in the certificate during enrollment, use the **subject-name** command in crypto CA trustpoint configuration mode. The DN represents the person or system that uses the certificate. To restore the default setting, use the **no** form of the command.

**subject-name** *X.500_name*

### subject-name (crypto ca trustpoint) Parameters

| Parameter | Description |
|---|---|
| *X.500_name* | Defines the X.500 distinguished name. Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains commas or spaces. For example: **cn=crl,ou=certs,o="cisco systems, inc.",c=US**. The maximum length is 500 characters. |

## keypair

To specify the key pair whose public key is to be certified, use the **keypair** command in crypto CA trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

**keypair** *name*

### keypair Parameters

| Parameter | Description |
|---|---|
| *name* | Specify the name of the key pair. |

## 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, as well as the appearance of WebVPN screens that end users see.

**webvpn**

## enable (webvpn)

To enable WebVPN or email proxy access on a previously configured interface, use the **enable** command. For WebVPN, use this command in webvpn mode. For email proxies (Internet Message Access Protocol version 4 Secure (IMAP4S), Post Office Protocol version 3 Secure [POP3S], and Simple Mail Transfer Protocol Secure [SMTPS]), use this command in the applicable email proxy mode. To disable WebVPN on an interface, use the **no** version of the command.

**enable** *ifname*

### enable (webvpn) Parameters

| Parameter | Description |
|---|---|
| *ifname* | Identifies the previously configured interface. Use the **nameif** command to configure interfaces. |

## svc image

To specify an SSL VPN client package file that the adaptive security appliance expands in cache memory for downloading to remote PCs, use the **svc image** command from webvpn configuration mode. To remove the command from the configuration, use the **no** form of the command.

**svc image** *filename order* [**regex** *expression*]

### svc image Parameters

| Parameter | Description |
|---|---|
| *filename* | Specifies the filename of the package file, up to 255 characters. |
| *order* | With multiple client package files, *order* specifies the order of the package files, from 1 to 65,535. The security appliance downloads portions of each client, in the order that you specify, to the remote PC until it achieves a match with the operating system. |
| **regex** *expression* | Specifies a string that the adaptive security appliance uses to match against the user agent string that is passed by the browser. |

## svc enable

To enable the adaptive security appliance to download an SSL VPN client to remote computers, use the **svc enable** command from webvpn configuration mode. To remove the command from the configuration, use the **no** form of the command.

**svc enable**

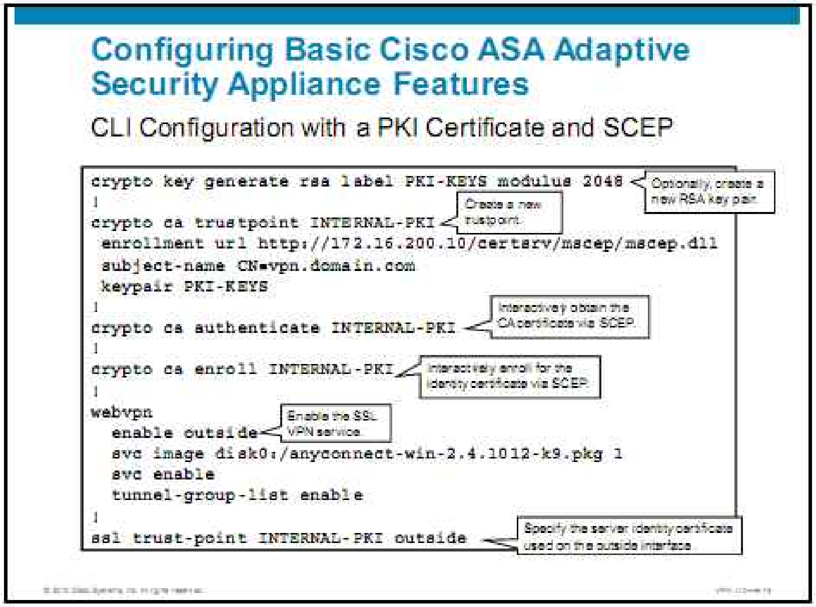
## ssl trust-point

To specify the certificate trustpoint that represents the SSL certificate for an interface, use the **ssl trust-point** command with the *interface* argument in global configuration mode. If you do not specify an interface, this command creates the fallback trustpoint for all interfaces that do not have a trustpoint configured. To remove an SSL trustpoint from the configuration that does not specify an interface, use the **no** version of this command. To remove an entry that does specify an interface, use the **no ssl trust-point** {*trustpoint* [*interface*]} version of the command.

**ssl trust-point** {*trustpoint* [*interface*]}

### ssl trust-point Parameters

| Parameter | Description |
|---|---|
| *interface* | The name for the interface to which the trustpoint applies. The **nameif** command specifies the name of the interface. |
| *trustpoint* | The *name* of the CA trustpoint as configured in the **crypto ca trustpoint** {*name*} command. |



## Configuring Basic Cisco ASA Adaptive Security Appliance Features

CLI Configuration with a PKI Certificate and SCEP

```
crypto key generate rsa label PKI-KEYS modulus 2048
!
crypto ca trustpoint INTERNAL-PKI
 enrollment url http://172.16.200.10/certsrv/mscep/mscep.dll
 subject-name CN=vpn.domain.com
 keypair PKI-KEYS
!
crypto ca authenticate INTERNAL-PKI
!
crypto ca enroll INTERNAL-PKI
!
webvpn
  enable outside
  svc image disk0:/anyconnect-win-2.4.1012-k9.pkg 1
  svc enable
  tunnel-group-list enable
!
ssl trust-point INTERNAL-PKI outside
```

Optionally, create a new RSA key pair.

Create a new trustpoint.

Interactively obtain the CA certificate via SCEP.

Interactively enroll for the identity certificate via SCEP.

Enable the SSL VPN service.

Specify the server identity certificate used on the outside interface.

This output shows the CLI commands that are required to configure the basic Cisco ASA adaptive security appliance SSL VPN gateway features using a PKI-provisioned identity certificate of the appliance. The procedure is generally the same as when using a self-signed certificate, except for the trustpoint configuration and enrollment procedure.

Inside the trustpoint configuration, use the **enrollment url** command to specify the SCEP enrollment URL provided to you by the PKI administrator. Use the **subject-name** command to specify the FQDN that the security appliance will use inside its identity certificate in the canonical name certificate field, and any other components of the name that the PKI requires (provided to you by the PKI administrator). Optionally, use the **keypair** command to specify the RSA key pair that the security appliance will use when requesting its identity certificate.

Use the **crypto ca authenticate** command to download the identity certificate of the PKI CA to the Cisco ASA adaptive security appliance. A fingerprint of the downloaded certificate will be displayed, and you should accept it after verifying that it is the correct CA certificate fingerprint. To verify the fingerprint, use a secure communication channel with the PKI administrator, or perform this transaction over a trusted network.

Next, use the **crypto ca enroll** command to request the identity certificate of the Cisco ASA adaptive security appliance from the PKI, sending the name parameters and the public key of the configured key pair to the PKI CA. The PKI CA will issue you an identity certificate, which the Cisco ASA adaptive security appliance will automatically download by periodically polling the PKI CA server.

Other CLI steps and commands are the same as when enabling the SSL VPN gateway functions with a self-signed certificate.

## enrollment url

To specify automatic enrollment (SCEP) to enroll with this trustpoint and to configure the enrollment URL, use the **enrollment url** command in crypto CA trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

**enrollment url** *url*

### enrollment url Parameters

| Parameter | Description |
|---|---|
| `url` | Specifies the name of the URL for automatic enrollment. The maximum length is 1000 characters (effectively unbounded). |

## crypto ca authenticate

To install and authenticate the CA certificates that are associated with a trustpoint, use the **crypto ca authenticate** command in global configuration mode. To remove the CA certificate, use the **no** form of this command.

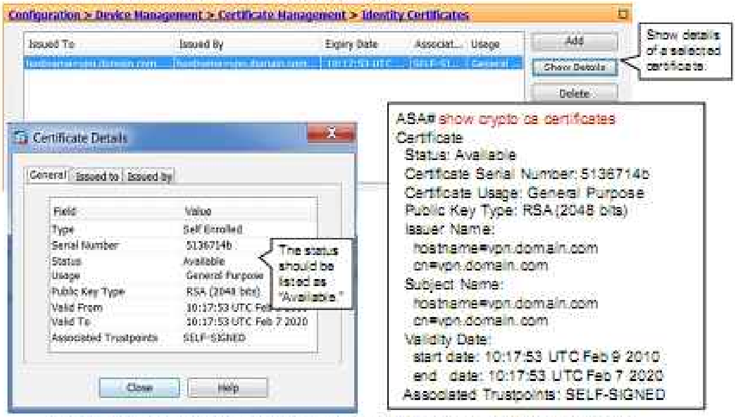
**crypto ca authenticate** *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive**]

### crypto ca authenticate Parameters

| Parameter | Description |
|---|---|
| **`fingerprint`** | Specifies a hash value consisting of alphanumeric characters that the adaptive security appliance uses to authenticate the CA certificate. If a fingerprint is provided, the adaptive security appliance compares it to the computed fingerprint of the CA certificate and accepts the certificate only if the two values match. If there is no fingerprint, the adaptive security appliance displays the computed fingerprint and asks whether to accept the certificate. |
| *`hexvalue`* | Identifies the hexadecimal value of the fingerprint. |
| **`nointeractive`** | Obtains the CA certificate for this trustpoint by using no interactive mode. It is intended for use by the device manager only. In this case, if there is no fingerprint, the adaptive security appliance accepts the certificate without question. |
| *`trustpoint`* | Specifies the trustpoint from which to obtain the CA certificate. Maximum name length is 128 characters. |

## Configuring Basic Cisco ASA Adaptive Security Appliance Features

### Identity Certificate Verification



Configuration > Device Management > Certificate Management > Identity Certificates
Issued To
Issued By
Expiry Date
Associat...
Usage
Add
Show Details
Delete
Show details of a selected certificate.
Certificate Details
General
Issued to
Issued by
Close
Help
The status should be listed as "Available."

| Field | Value |
|---|---|
| Type | Self Enrolled |
| Serial Number | 5136714b |
| Status | Available |
| Usage | General Purpose |
| Public Key Type | RSA (2048 bits) |
| Valid From | 10:17:53 UTC Fe |
| Valid To | 10:17:53 UTC Feb 7 2020 |
| Associated Trustpoints | SELF-SIGNED |

```
ASA# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 5136714b
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Issuer Name:
    hostname=vpn.domain.com
    cn=vpn.domain.com
  Subject Name:
    hostname=vpn.domain.com
    cn=vpn.domain.com
  Validity Date:
    start date: 10:17:53 UTC Feb 9 2010
    end   date: 10:17:53 UTC Feb 7 2020
  Associated Trustpoints: SELF-SIGNED
```

Configuration > Device Management > Certificate Management > Identity Certificates

To verify that the identity certificate of the Cisco ASA adaptive security appliance has been successfully installed, choose **Configuration > Device Management > Certificate Management > Identity Certificates** by using Cisco ASDM. Select the identity certificate of the Cisco ASA adaptive security appliance and click the **Show Details** button. The certificate status should be listed as "Available." In the CLI, use the **show crypto ca certificates** command and verify that the certificate status shows as "Available."

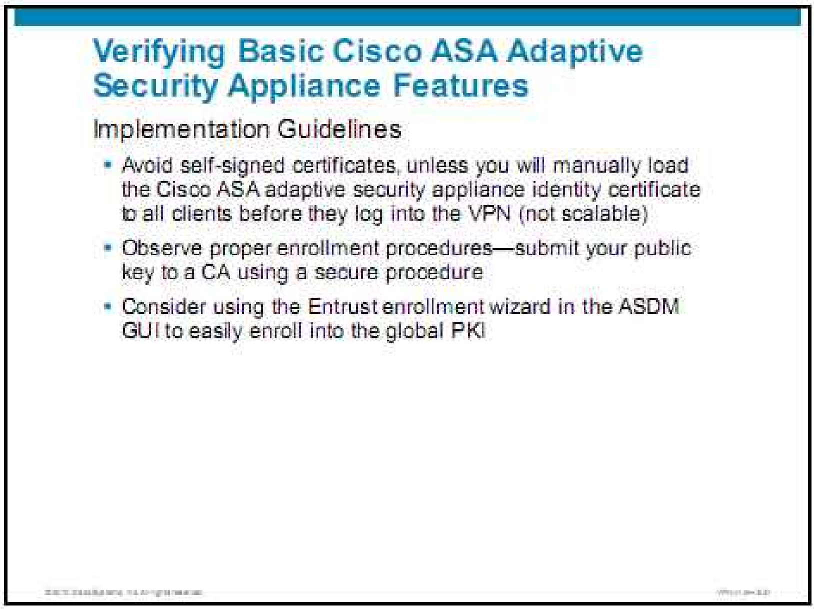
## show crypto ca certificates

To display the certificates that are associated with a specific trustpoint or to display all the certificates that are installed on the system, use the **show crypto ca certificates** command in global configuration or privileged EXEC mode.

**show crypto ca certificates** [*trustpointname*]

### show crypto ca certificates Parameters

| Parameter | Description |
|---|---|
| `trustpointname` | (Optional) The name of a trustpoint. If you do not specify a name, this command displays all certificates that are installed on the system. |



## Verifying Basic Cisco ASA Adaptive Security Appliance Features

Implementation Guidelines

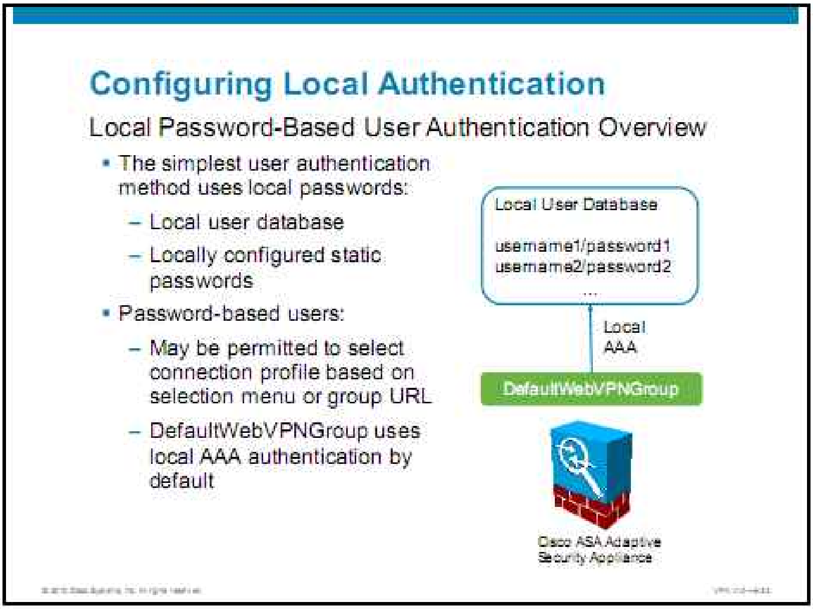
- Avoid self-signed certificates, unless you will manually load the Cisco ASA adaptive security appliance identity certificate to all clients before they log into the VPN (not scalable)
- Observe proper enrollment procedures—submit your public key to a CA using a secure procedure
- Consider using the Entrust enrollment wizard in the ASDM GUI to easily enroll into the global PKI

When implementing basic Cisco ASA adaptive security appliance SSL VPN gateway features, consider the following implementation guidelines:

- Generally, avoid using self-signed certificates, except in very small deployments where you can manually load the identity certificate of the Cisco ASA adaptive security appliance to all the remote clients before they log into the VPN. The remote users can also install the self-signed certificate themselves if they initially log in over a trusted network, which is often not the case.
- When enrolling into a PKI over an untrusted network, observe proper enrollment procedures and make sure that the PKI administrator properly verifies the appliance name and public key before issuing a certificate, in order to avoid issuing the certificate to a malicious entity.
- The Cisco ASDM includes an Entrust enrollment wizard, which simplifies the enrollment into the global PKI by providing you with step-by-step instructions for obtaining an Entrust-provisioned certificate. Consider using this wizard if you are unsure how to enroll into the global PKI. The wizard can be started by clicking the Enroll ASA SSL VPN with Entrust button in the Configuration > Device Management > Certificate Management > Identity Certificates pane.

# Configuring Local Password-Based User Authentication

This topic enables you to configure and verify password-based local user authentication in a Cisco AnyConnect full tunnel SSL VPN.



## Configuring Local Authentication

Local Password-Based User Authentication Overview

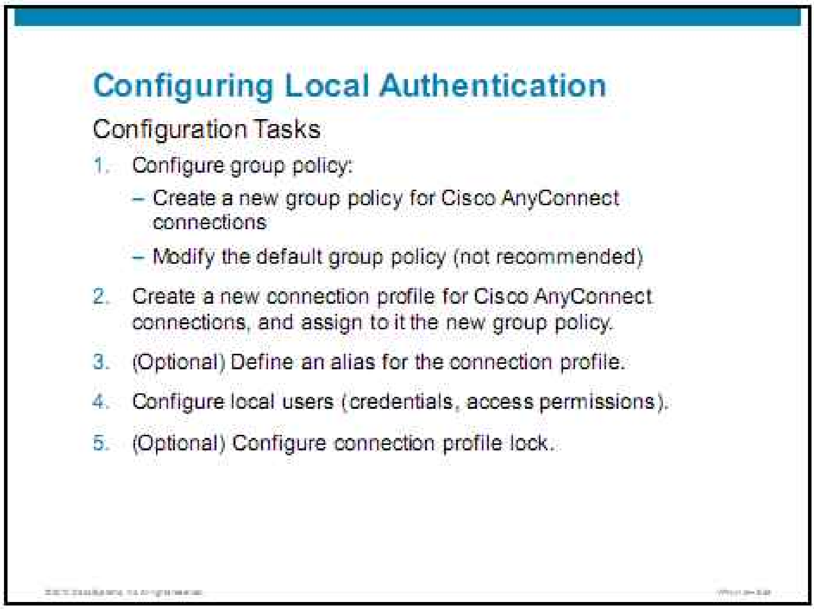
- The simplest user authentication method uses local passwords:
  - Local user database
  - Locally configured static passwords
- Password-based users:
  - May be permitted to select connection profile based on selection menu or group URL
  - DefaultWebVPNGroup uses local AAA authentication by default

Local User Database

username1/password1
username2/password2
...

After configuring basic Cisco ASA adaptive security appliance SSL VPN gateway parameters, the next deployment task is to configure a user authentication method, and prepare the Cisco ASA adaptive security appliance with all necessary configuration objects to enable later assignment of VPN policies. In this basic SSL VPN full tunnel solution, you will deploy simple password-based user authentication, using the local user database on the adaptive security appliance.

When SSL VPN full tunnel users connect to the Cisco ASA adaptive security appliance, the users may be permitted to select their connection profile by either choosing the desired profile from a drop-down list or connecting to the group URL. If no specific connection profile has been chosen, the security appliance will assign users to the default WebVPN group (DefaultWebVPNGroup) connection profile. This profile is, by default, configured to use user authentication by leveraging the local user of the Cisco ASA adaptive security appliance database. In this topic, you will configure a custom connection profile, and lock users into this custom connection profile after they authenticate to the security appliance.



## Configuring Local Authentication

Configuration Tasks

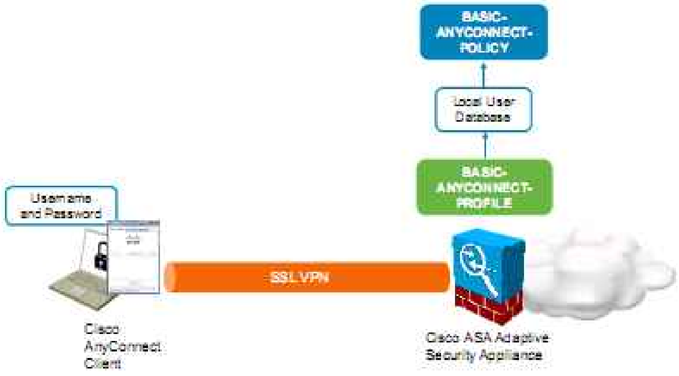
1. Configure group policy:
   - Create a new group policy for Cisco AnyConnect connections
   - Modify the default group policy (not recommended)
2. Create a new connection profile for Cisco AnyConnect connections, and assign to it the new group policy.
3. (Optional) Define an alias for the connection profile.
4. Configure local users (credentials, access permissions).
5. (Optional) Configure connection profile lock.

To configure basic user authentication in the basic Cisco ASA adaptive security appliance full tunnel SSL VPN solution, perform the following configuration tasks:

1. Configure a group policy. You can use one of two methods:
   - Create a new, custom group policy for your Cisco AnyConnect users. In this topic, you will create a single custom group policy for all users. Based on your requirements, you may need to create multiple group policies to differentiate users based on their access needs. This method is recommended in favor of tuning the default group policy.
   - Modify the default group policy to allow SSL VPN connections. The default group policy is the root policy from which all other connection or user profiles inherit settings. By default, full tunnel SSL VPN connections are not allowed. This approach is not recommended.
2. Create a new, custom connection profile into which you can assign users, and, based on this connection profile, assign the custom group policy to the users. As with the group policy, based on your requirements, you may need to create multiple connection profiles to differentiate users based on their access needs, and assign each connection profile a different group policy.
3. Optionally, define an alias for the connection profile. This approach is required to allow users to select the connection profile using the drop-down menu.
4. Configure users and their credentials in the Cisco ASA adaptive security appliance local user database.
5. Optionally, configure the connection profile lock feature for the created user account.

## Configuring Local Authentication

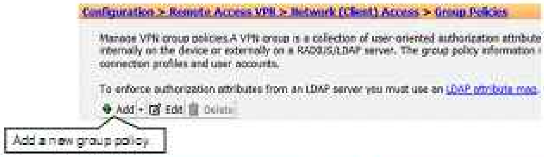
### Configuration Scenario



This figure presents the configuration scenario that is used in upcoming configuration tasks. On the Cisco ASA adaptive security appliance, you will create a custom connection profile named BASIC-ANYCONNECT-PROFILE, and a related group policy named BASIC-ANYCONNECT-POLICY. Then, you will create one user named "vpnuser" in the local user database.

## Configuring Local Authentication

### Task 1A: Create a Custom Group Policy

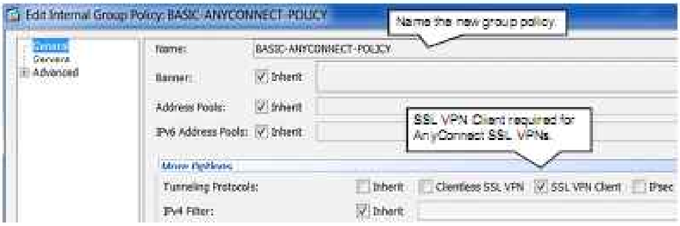


Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute internally on the device or externally on a RADIUS/LDAP server. The group policy information connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Add a new group policy.



Edit Internal Group Policy: BASIC-ANYCONNECT-POLICY

Name: BASIC-ANYCONNECT-POLICY

Banner: ☑ Inherit

Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: ☐ Inherit ☐ Clientless SSL VPN ☑ SSL VPN Client ☐ IPsec

IPv4 Filter: ☑ Inherit

Name the new group policy.

SSL VPN Client required for AnyConnect SSL VPNs.

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

First, you will create a custom group policy that you will apply to the full tunnel VPN users via their connection profile. Perform the following steps:

**Step 1** In Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Click **Add** to add a new policy.

**Step 2** Provide a name for the new group policy (BASIC-ANYCONNECT-POLICY, in this example).

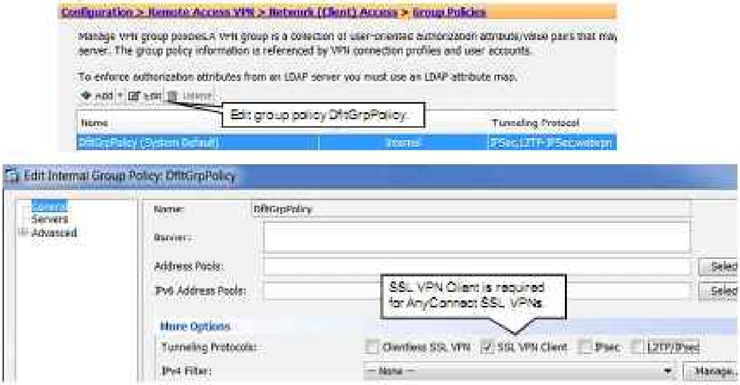
**Step 3** Expand the **More Options** pane, and check the **SSL VPN Client** check box in the Tunneling Protocols section. This protocol is needed to support Cisco AnyConnect SSL VPNs. You should uncheck all other tunneling protocols, if they are not used in your particular environment.

**Step 4** Click **OK**.

**Step 5** Click **Apply** to apply the configuration.

## Configuring Local Authentication

### Task 1B: Modify the Default Group Policy



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

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may ... server. The group policy information is referenced by VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Edit group policy DfltGrpPolicy.

| Name | | Tunneling Protocol |
|---|---|---|
| DfltGrpPolicy (System Default) | Internal | IPSec,L2TP-IPSec,webvpn |

Edit Internal Group Policy: DfltGrpPolicy

Name: DfltGrpPolicy

Banner:

Address Pools:

IPv6 Address Pools:

SSL VPN Client is required for AnyConnect SSL VPNs.

More Options

Tunneling Protocols: ☐ Clientless SSL VPN ☑ SSL VPN Client ☐ IPsec ☐ L2TP/IPsec

IPv4 Filter: -- None --

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

Alternatively, you may modify the default group policy. This approach is recommended only in two situations:

- In small environments with a single group policy
- When a certain parameter is identical in all custom group policies and can be inherited from the default policy

Perform the following steps to tune the default group policy:

**Step 1** In Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Choose **DfltGrpPolicy**, and click **Edit** to edit it.

**Step 2** Expand the **More Options** pane, and check the **SSL VPN Client** check box in the Tunneling Protocols section to support SSL VPN full tunnel connections.

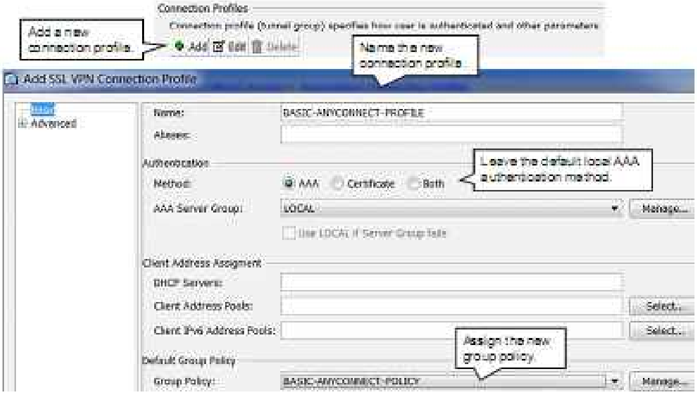
---

**Note** If your Cisco ASA adaptive security appliance will support other VPN access options, you may need to leave some of the other tunneling protocols enabled.

---

## Configuring Local Authentication

### Task 2: Create a Custom Connection Profile



Add a new connection profile.

Name the new connection profile.

Leave the default local AAA authentication method.

Assign the new group policy.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters

Add SSL VPN Connection Profile

Name: BASIC-ANYCONNECT-PROFILE

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: BASIC-ANYCONNECT-POLICY

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

Next, you will create a custom connection profile to which you will assign the full tunnel VPN users. Perform the following steps:

**Step 1** In Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. In the Connection Profiles section, click **Add** to add a new connection profile.

**Step 2** Provide a name for the new connection profile (BASIC-ANYCONNECT-PROFILE, in this example).

**Step 3** In the Authentication section, leave the authentication method at its default settings (LOCAL AAA authentication).

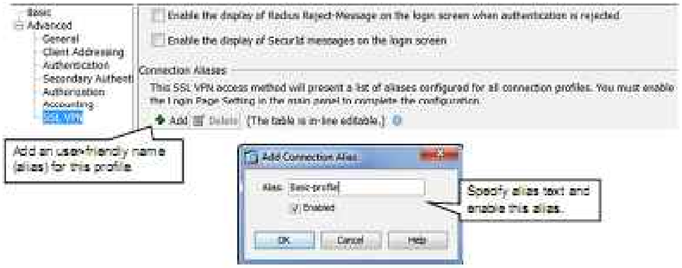
**Step 4** In the Default Group Policy section, choose the custom group policy (BASIC-ANYCONNECT-POLICY that was configured in the previous set of tasks) from the drop-down list.

## Configuring Local Authentication

Task 3: (Optional) Define Connection Profile Alias

Aliases are displayed to the user upon login.

- Enable users to choose desired connection profile



□ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

□ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

Alias: Basic-profile

☑ Enabled

Add an user-friendly name (alias) for this profile

Specify alias text and enable this alias.

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

Next, you may define an alias for the connection profile. Once the alias is defined, users may be permitted to select the desired connection profile when connecting to the SSL VPN. Perform the following steps:

**Step 1** In the connection profile edit window, choose **Advanced > SSL VPN**. Click **Add** in the Connection Aliases section.

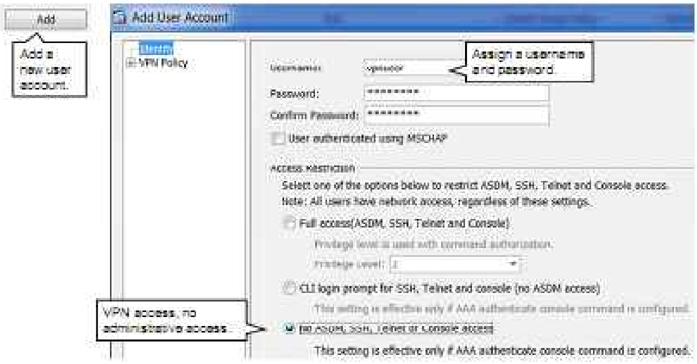
**Step 2** Assign an alias name to this connection profile. Use a user-friendly name, as this alias will be visible to your VPN users in their Cisco AnyConnect client (**Basic-profile** in this example). Check the **Enable** check box. You can use spaces in alias text, but if you do, you must provide the alias name inside quotes.

**Step 3** Click **OK** in the Add Connection Alias window. Click **OK** in the Connection Profile window.

**Step 4** Click **Apply**, and then click **Save** to save your configuration.

## Configuring Local Authentication

Task 4: Configure Local Users and Credentials



Add

Add a new user account.

Add User Account

Identity
VPN Policy

Username: vpnuser

Assign a username and password.

Password: ********

Confirm Password: ********

□ User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

○ Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 2

○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if AAA authenticate console command is configured.

VPN access, no administrative access.

● No ASDM, SSH, Telnet or Console access

This setting is effective only if AAA authenticate console command is configured.

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

Configuration > Device Management > Users/AAA > User Accounts

Finally, you will create user accounts in the Cisco ASA adaptive security appliance local database. These user accounts must only be able to log into the VPN, and not to the security appliance management user interfaces (the Cisco ASDM and the CLI). Perform the following tasks:

**Step 1** In Cisco ASDM, choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users**. Click **Add** to add a new user account.

**Step 2** Provide a name for the new user account (**vpnuser**, in this example).

**Step 3** Create a password for the new user account.

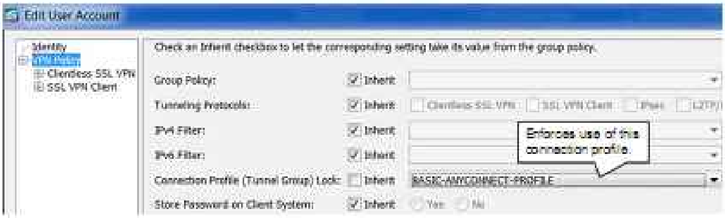
**Step 4** In the Access Restriction section, select the **No ASDM, SSH, Telnet or Console Access** option. This selection will restrict the user to prevent these credentials from being accepted for device management functions.

## Configuring Local Authentication

### Task 5: (Optional) Configure Connection Profile Lock

Lock user to connection profile

- Enforces use of connection profile
- Access denied if user attempts to connect to other profile



Edit User Account

- Identity
- VPN Policy
  - Clientless SSL VPN
  - SSL VPN Client

Check an Inherit checkbox to let the corresponding setting take its value from the group policy.

| | | |
|---|---|---|
| Group Policy: | ☑ Inherit | |
| Tunneling Protocols: | ☑ Inherit | □ Clientless SSL VPN □ SSL VPN Client □ IPsec □ L2TP/ |
| IPv4 Filter: | ☑ Inherit | |
| IPv6 Filter: | ☑ Inherit | |
| Connection Profile (Tunnel Group) Lock: | □ Inherit | BASIC-ANYCONNECT-PROFILE |
| Store Password on Client System: | ☑ Inherit | ○ Yes ○ No |

Enforces use of this connection profile.

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

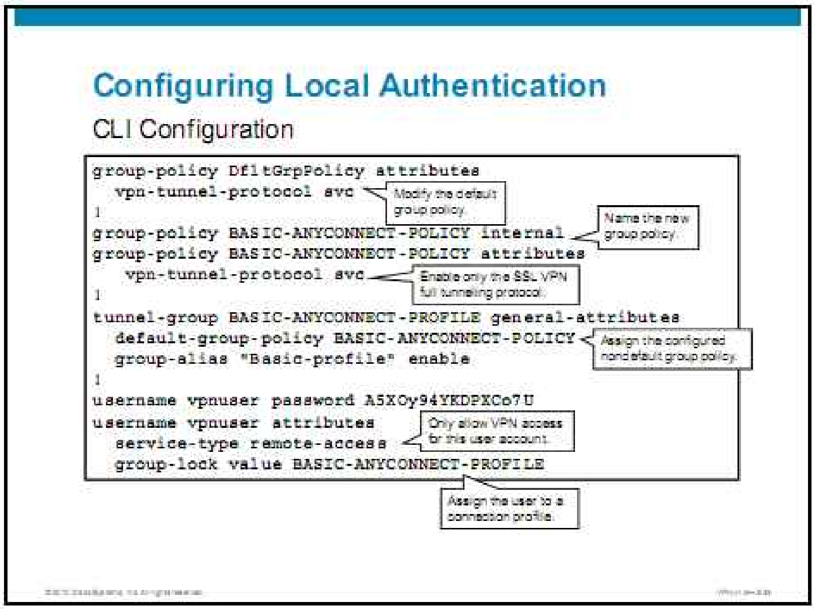
To configure the connection profile lock feature, perform the following tasks:

**Step 1** In the user account edit window, choose **VPN Policy**.

**Step 2** Uncheck the **Inherit** check box next to the Connection Profile (Tunnel Group) Lock field. Assign this user account to the custom connection profile by using the drop-down menu to select the custom connection profile (BASIC-ANYCONNECT-PROFILE, in this example).

**Step 3** Click **OK** in the Edit User Account window.

**Step 4** Click **Apply**, and then click **Save** to save your configuration.



## Configuring Local Authentication

CLI Configuration

```
group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol svc
!
group-policy BASIC-ANYCONNECT-POLICY internal
group-policy BASIC-ANYCONNECT-POLICY attributes
   vpn-tunnel-protocol svc
!
tunnel-group BASIC-ANYCONNECT-PROFILE general-attributes
  default-group-policy BASIC-ANYCONNECT-POLICY
  group-alias "Basic-profile" enable
!
username vpnuser password A5XOy94YKDPXCo7U
username vpnuser attributes
  service-type remote-access
  group-lock value BASIC-ANYCONNECT-PROFILE
```

Modify the default group policy.

Name the new group policy.

Enable only the SSL VPN full tunneling protocol.

Assign the configured nondefault group policy.

Only allow VPN access for this user account.

Assign the user to a connection profile.

The output shows the CLI commands that are required to configure basic Cisco ASA adaptive security appliance SSL VPN user authentication. In the CLI, use the **vpn-tunnel-protocol svc** command in the group-policy DfltGrpPolicy attributes mode to enable the SSL VPN full tunnel functionality in the default group policy.

Next, create a new, custom group policy by using the **group-policy** command, and specify the group policy as internal. In the new group-policy attributes mode, enable the SSL VPN full tunnel functionality for this group policy by using the **vpn-tunnel-protocol** command.

Next, create a new, custom connection profile by using the **tunnel-group** command, and attach the custom BASIC-ANYCONNECT-POLICY to this connection profile by using the **default-group-policy** command. Also, assign a user-friendly connection profile alias name to this connection profile by using the **group-alias** command, and enable it.

Finally, create a user account in the local database by using the **username** command, and assign to it a password. In the username attributes mode, restrict this user to VPN access (without the possibility of management access) by using the **service-type remote-access** command. Also, assign this user into the BASIC-ANYCONNECT-PROFILE connection profile by using the **group-lock value** 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 |
|---|---|
| **external server-group** *server_group* | Specifies the group policy as external and identifies the AAA server group for the adaptive security appliance to query for attributes. |
| **from** *group-policy_name* | Initializes the attributes of this internal group policy to the values of a pre-existing group policy. |
| **internal** | Identifies the group policy as internal. |
| *name* | Specifies the name of the group policy. The name can be up to 64 characters long and cannot contain spaces. |
| **password** *server_password* | 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 |
|---|---|
| *name* | Specifies the name of the group policy |

## vpn-tunnel-protocol

To configure a VPN tunnel type (IP Security [IPsec], Layer 2 Tunneling Protocol [L2TP] over IPsec, Cisco VPN Client, 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 |
|---|---|
| **ipsec** | 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. |
| **l2tp-ipsec** | Negotiates an IPsec tunnel for an L2TP connection. |
| **svc** | Negotiates an SSL VPN tunnel with an SSL VPN client. |
| **webvpn** | Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client. |

## tunnel-group general-attributes

To enter 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 |
|---|---|
| `general-attributes` | Specifies attributes for this tunnel group |
| *name* | 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 |
|---|---|
| *group-name* | Specifies the name of the default 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 |
|---|---|
| `disable` | Disables the group alias. |
| `enable` | Enables a previously disabled group alias. |
| *name* | Specifies the name of a tunnel group alias. This name can be any string that you choose, except that the string cannot contain spaces. |

## username

To add a user to the adaptive security appliance database, enter the **username** command in global configuration mode. To remove a user, use the **no** version of this command with the username you want to remove. To remove all usernames, use the **no** version of this command without appending a username.

**username** *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

### username Parameters

| Parameter | Description |
|---|---|
| **encrypted** | Indicates that the password is encrypted (if you did not specify **mschap**). When you define a password in the **username** command, the adaptive security appliance encrypts it when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password, which is followed by the **encrypted** keyword. For example, if you enter the password "test," the **show running-config** display would appear as something like the following:<br>`username pat password rvEdRh0xPC8bel7s encrypted`<br>The only time that you would actually enter the **encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another adaptive security appliance and you are using the same password. |
| **mschap** | Specifies that the password will be converted to Unicode and hashed using Message Digest 4 (MD4) after you enter it. Use this keyword if users are authenticated using Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1) or MS-CHAP version 2 (MS-CHAPv2). |
| *name* | Specifies the name of the user as a string from 4 to 15 characters in length. |
| **nopassword** | Indicates that this user needs no password. |
| **nt-encrypted** | Indicates that the password is encrypted for use with MS-CHAPv1 or MS-CHAPv2. If you specified the **mschap** keyword when you added the user, then this keyword is displayed instead of the **encrypted** keyword when you view the configuration using the **show running-config** command. |
| **password** *password* | Sets the password as a string from 3 to 16 characters in length. |
| **privilege** *priv_level* | Sets a privilege level for this use from 0 to 15 (lowest to highest). The default privilege level is 2. This privilege level is used with command authorization. |

## 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 |

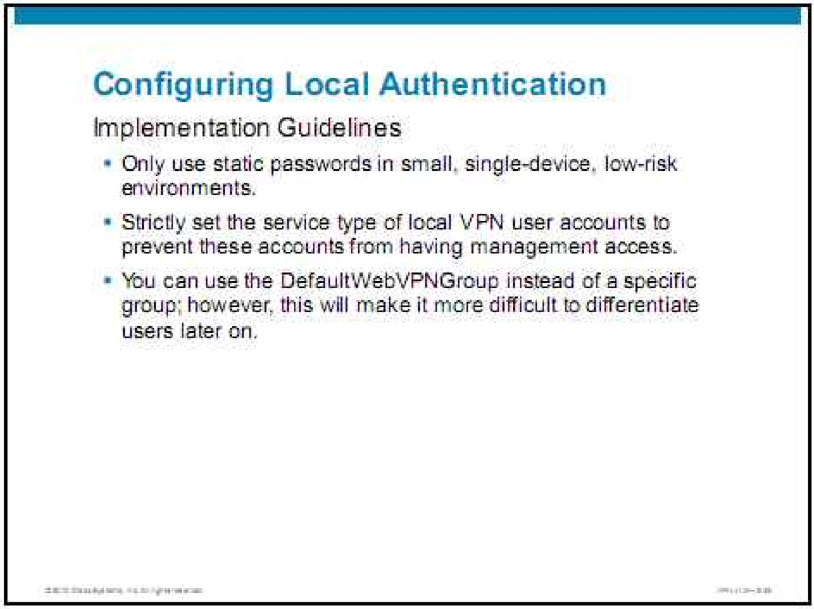
## group-lock

To restrict remote users to access through the tunnel group only, issue the **group-lock** command in group-policy configuration mode or username configuration mode. To remove the group-lock attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value from another group policy.

**group-lock** {**value** *tunnel-grp-name* | **none**}

### group-lock Parameters

| Parameter | Description |
|---|---|
| `none` | Sets group lock to a null value, thus allowing no group-lock restriction. Prevents inheriting a group-lock value from a default or specified group policy. |
| `value` *`tunnel-grp-name`* | Specifies the name of an existing tunnel group that the adaptive security appliance requires for the user to connect. |



## Configuring Local Authentication

Implementation Guidelines

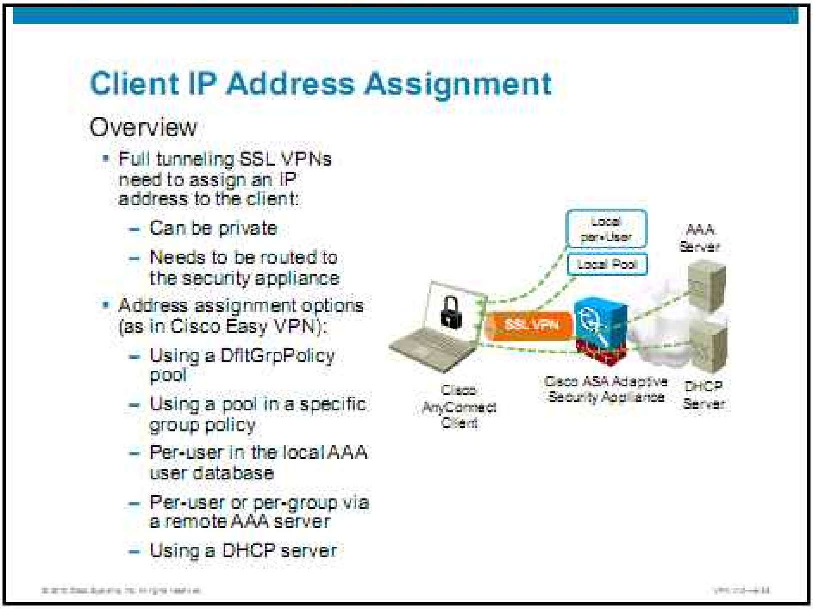
- Only use static passwords in small, single-device, low-risk environments.
- Strictly set the service type of local VPN user accounts to prevent these accounts from having management access.
- You can use the DefaultWebVPNGroup instead of a specific group; however, this will make it more difficult to differentiate users later on.

When implementing local password-based user authentication in an SSL VPN full tunnel solution, consider the following implementation guidelines:

- Only use user authentication with static passwords and the local database in small, single gateway, low-risk environments, as these passwords are reusable and typically easy to guess.
- Always strictly set the service type of the users to only allow VPN access. This setting is extremely important to prevent unauthorized access to Cisco ASA adaptive security appliance management functions.
- In this topic, all examples used a custom connection profile and a custom group policy. If all of your users share the same authentication method and access policies, you could also implement this by using only the DefaultWebVPNGroup connection profile and the default group policy. Note, however, that the approach that is taken in this topic makes it very easy to differentiate users later on, if needed.

# Configuring Client IP Address Management, Basic Access Control, and Split Tunneling

This topic enables you to configure IP address management, basic access control, and split tunneling in a Cisco AnyConnect full tunnel SSL VPN.



## Client IP Address Assignment

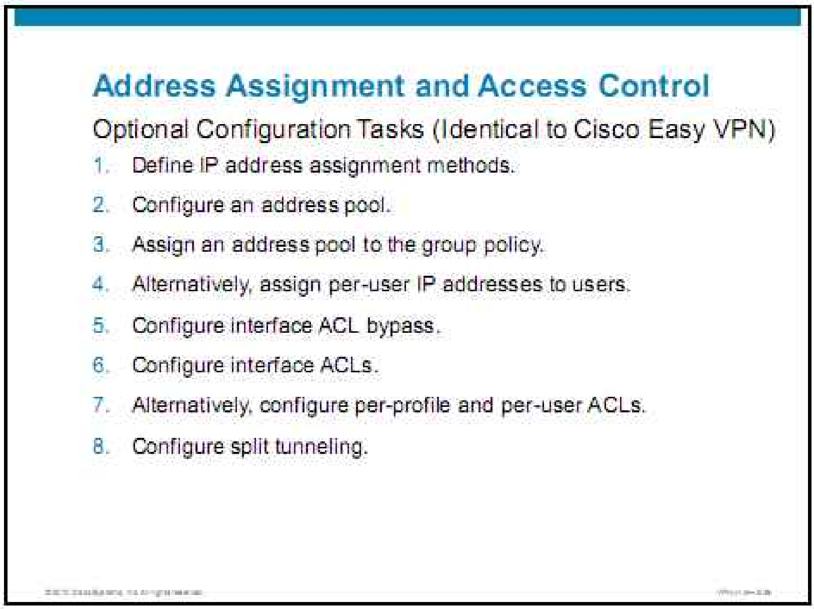
Overview

- Full tunneling SSL VPNs need to assign an IP address to the client:
  - Can be private
  - Needs to be routed to the security appliance
- Address assignment options (as in Cisco Easy VPN):
  - Using a DfltGrpPolicy pool
  - Using a pool in a specific group policy
  - Per-user in the local AAA user database
  - Per-user or per-group via a remote AAA server
  - Using a DHCP server

When clients connect using the full tunnel VPN methods, the VPN gateway will assign them an IP address on their virtual network interface (adapter), and the clients will use this IP address as their source IP address to access resources beyond the VPN gateway. These addresses can be from the private address space, but they need to be routed to the gateway (Cisco ASA adaptive security appliance) in the internal network.

There are five different IP address assignment options available in the Cisco ASA security appliance SSL VPN full tunnel solution. They are identical to the Cisco Easy VPN deployment methods and include the following:

- Use a pool of IP addresses, which are configured on the Cisco ASA adaptive security appliance, and assign the pool to the default group policy. By default these addresses are leased to all users (if their more specific policies do not provide other IP assignment methods).
- Use a pool of IP addresses, which are configured on the Cisco ASA adaptive security appliance, and assign the pool to a specific custom group policy, and therefore to specific connection profiles that use the specific group policy.
- Configure the addresses as part of the user account in the local user database, enabling per-user IP addresses.
- Configure the addresses as part of the user account in a remote (AAA) user database, enabling per-user IP addresses.
- Use a DHCP server, which the Cisco ASA adaptive security appliance will query to obtain an IP address for remote clients.



## Address Assignment and Access Control

Optional Configuration Tasks (Identical to Cisco Easy VPN)

1. Define IP address assignment methods.
2. Configure an address pool.
3. Assign an address pool to the group policy.
4. Alternatively, assign per-user IP addresses to users.
5. Configure interface ACL bypass.
6. Configure interface ACLs.
7. Alternatively, configure per-profile and per-user ACLs.
8. Configure split tunneling.

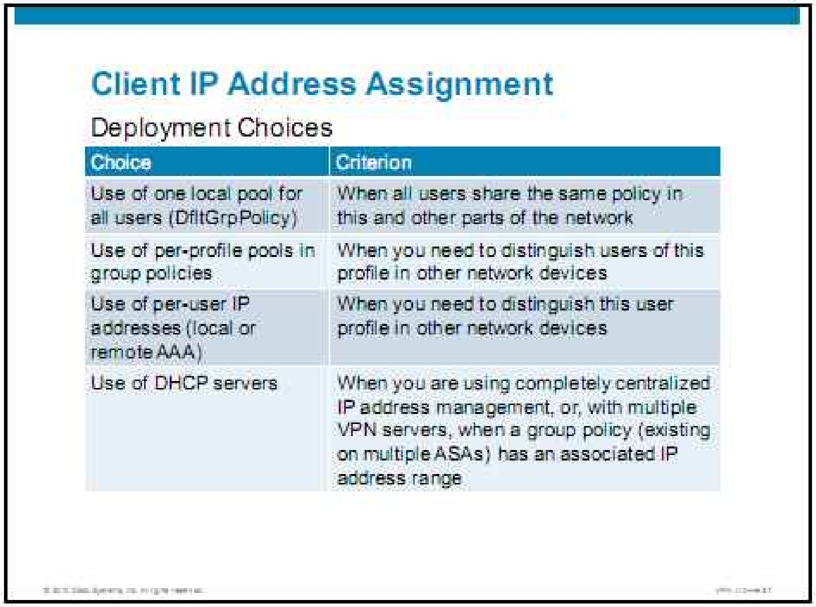
To configure client IP address assignment, basic access control, and split tunneling, you may need to perform some of the optional configuration tasks that have been explained in the lesson on Cisco Easy VPN. The procedures surrounding Cisco Easy VPN will not be further discussed in this lesson. The optional tasks are as follows:

1. Globally configure the allowed IP address assignment methods on the Cisco ASA adaptive security appliance.
2. Configure IP address pools, if you decide to use pools from which users can lease client IP addresses.
3. A) Assign the configured IP address pool to the default or specific custom group policy.

   B) Optionally, assign IP addresses to individual users, if you require per-user IP addresses, where each user "owns" a particular IP address.
4. Configure interface access control list (ACL) bypass.
5. A) Configure interface ACLs.

   B) Configure per-profile and per-user ACLs.
6. Configure split tunneling.

**Note** You need to configure either per-group-policy, or per-user IP addresses. If you configure no address assignment, SSL VPN full tunnel connections to the Cisco ASA adaptive security appliance will fail.



## Client IP Address Assignment

### Deployment Choices

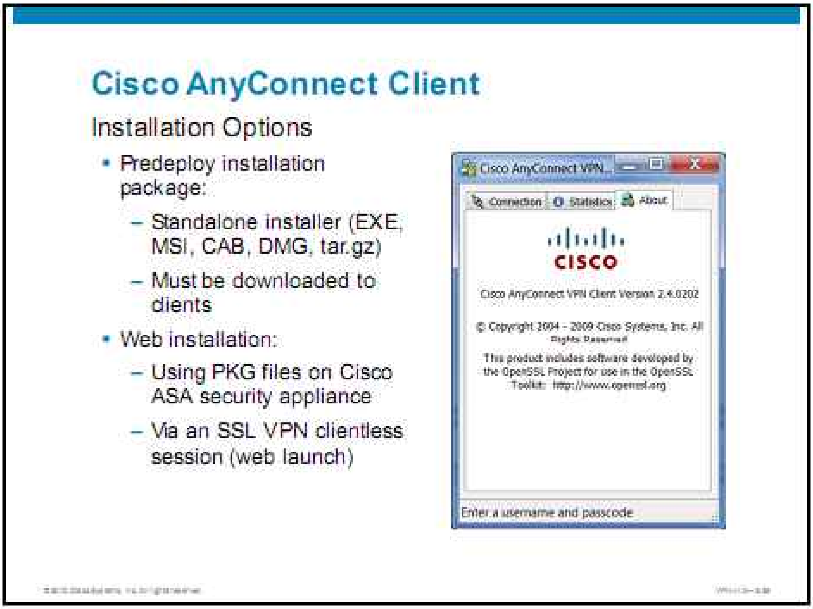
| Choice | Criterion |
|---|---|
| Use of one local pool for all users (DfltGrpPolicy) | When all users share the same policy in this and other parts of the network |
| Use of per-profile pools in group policies | When you need to distinguish users of this profile in other network devices |
| Use of per-user IP addresses (local or remote AAA) | When you need to distinguish this user profile in other network devices |
| Use of DHCP servers | When you are using completely centralized IP address management, or, with multiple VPN servers, when a group policy (existing on multiple ASAs) has an associated IP address range |

The selection of the IP assignment method should be based on the following criteria:

- If all of your users will share a common VPN policy on the Cisco ASA adaptive security appliance, and also in other parts of the protected network, where you may use other IP-address-based access controls, you can consider using a local pool of IP addresses that are assigned to the default group policy.
- If you want to differentiate between multiple groups of users on the Cisco ASA adaptive security appliance, and also in other parts of the protected network, you should consider using a local pool of IP addresses that are assigned to the specific group policies and, as a consequence, to specific connection profiles.
- If you want to assign specific, per-user policies on the Cisco ASA adaptive security appliance, and especially in other parts of the protected network, you should consider using assigned per-user IP addresses. This approach also simplifies user auditing and tracking, as each user is always uniquely identified by a particular IP address when connected to the VPN.
- If your IP address assignment is completely centralized, using a DHCP server, you can consider reusing the DHCP server to also assign VPN IP addresses. The DHCP server must assign addresses in a VPN with multiple VPN servers, when a group policy (existing on multiple Cisco ASA adaptive security appliances) has an associated IP address range.

# Installing and Configuring the Cisco AnyConnect Client

This topic enables you to install, configure, and verify the predeploy version of the Cisco AnyConnect client.



## Cisco AnyConnect Client

### Installation Options

- Predeploy installation package:
  - Standalone installer (EXE, MSI, CAB, DMG, tar.gz)
  - Must be downloaded to clients
- Web installation:
  - Using PKG files on Cisco ASA security appliance
  - Via an SSL VPN clientless session (web launch)

Cisco AnyConnect VPN Client Version 2.4.0202

© Copyright 2004 - 2009 Cisco Systems, Inc. All Rights Reserved

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit: http://www.openssl.org

Enter a username and passcode

The Cisco AnyConnect VPN Client is the next-generation VPN client, providing remote users with secure VPN connections to the Cisco ASA 5500 Series Adaptive Security Appliance running Cisco ASA Software Release 8.0 and higher. It does not work with a Cisco PIX device or with Cisco VPN 3000 Series Concentrator Software.

As the network administrator, you configure the Cisco AnyConnect client features on the Cisco ASA adaptive security appliance. Then, you can load the client software on the Cisco ASA adaptive security appliance and have it automatically download to remote users when they log in using web launch, or you can manually install the Cisco AnyConnect client software as an application on the client PCs. The Cisco AnyConnect client allows user profiles to be displayed in the user interface that defines the names and addresses of VPN gateways. The network administrator can assign particular features to individual users or groups.

**Note** Initial installation of the Cisco AnyConnect client requires administrator privileges.

The Cisco AnyConnect VPN Client packages can be downloaded from the Cisco website and uploaded to the Cisco ASA adaptive security appliance so that clients can download the software as needed.

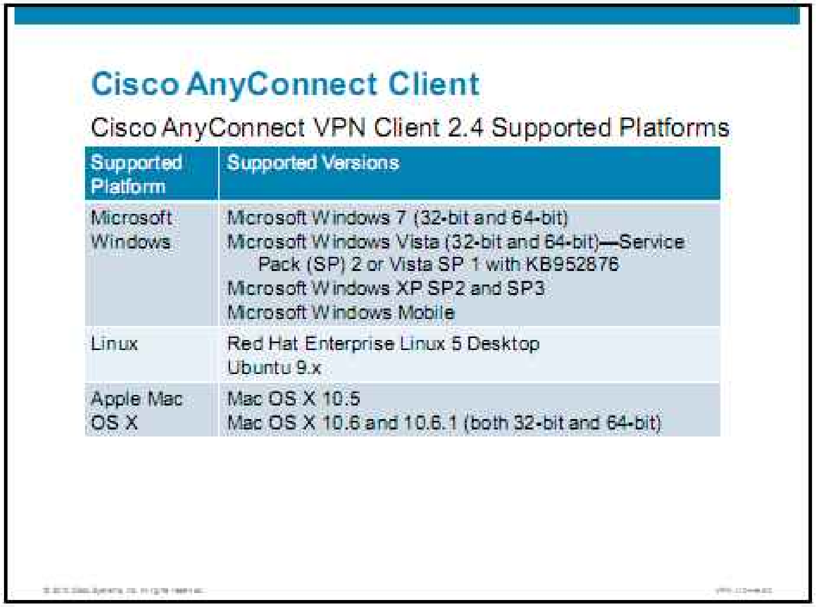
## Web Launch (Via SSL VPN Clientless Session)

The web launch installation method requires that the client system connect to the Cisco ASA adaptive security appliance by using a compliant web browser over an SSL connection. After being connected and authenticated, the user will be redirected by the security appliance to the Cisco AnyConnect VPN Client installation through ActiveX or Java. After the remote device has successfully installed the new software, the Cisco AnyConnect VPN Client will automatically log the user onto the network using the credentials that were originally supplied during the web session.

## Manual Installation

In addition to the autodownload packages that are available from the Cisco ASA adaptive security appliance, the remote device can also install the Cisco AnyConnect VPN Client manually by using an MSI installer on Windows-based systems. This installer is not a downloaded package from the security appliance, and the client will not be required to use a web browser for initial access to the network. After it is installed, the VPN client can be used to access the desired network resources.

**Note** In this topic, you will learn to use the manual installation of the predeploy Cisco AnyConnect client.



### Cisco AnyConnect Client

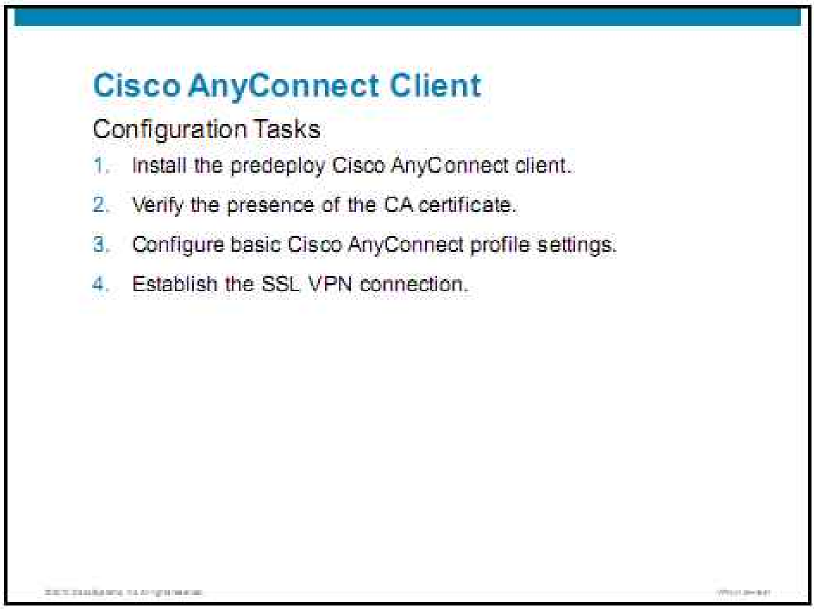
Cisco AnyConnect VPN Client 2.4 Supported Platforms

| Supported Platform | Supported Versions |
|---|---|
| Microsoft Windows | Microsoft Windows 7 (32-bit and 64-bit)<br>Microsoft Windows Vista (32-bit and 64-bit)—Service Pack (SP) 2 or Vista SP 1 with KB952876<br>Microsoft Windows XP SP2 and SP3<br>Microsoft Windows Mobile |
| Linux | Red Hat Enterprise Linux 5 Desktop<br>Ubuntu 9.x |
| Apple Mac OS X | Mac OS X 10.5<br>Mac OS X 10.6 and 10.6.1 (both 32-bit and 64-bit) |

The Cisco AnyConnect client supports the following operating systems:

- Microsoft Windows 7, Windows Vista, Windows XP, and Windows Mobile
- Mac OS X (version 10.5 or later) on either Intel or PowerPC
- Red Hat Linux (version 9 or later)
- Ubuntu 9 or later

See the Release Notes on Cisco.com for the full set of platform requirements and supported versions.



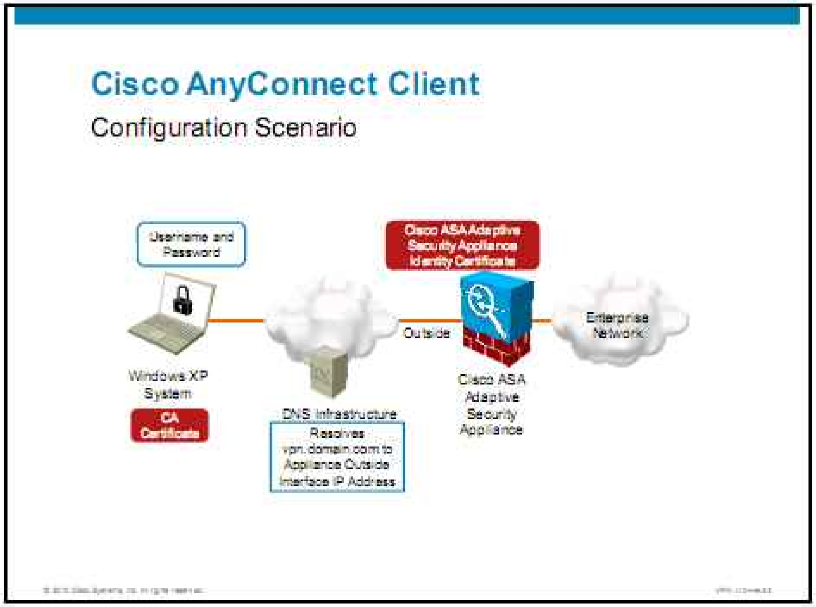
## Cisco AnyConnect Client

Configuration Tasks

1. Install the predeploy Cisco AnyConnect client.
2. Verify the presence of the CA certificate.
3. Configure basic Cisco AnyConnect profile settings.
4. Establish the SSL VPN connection.

In order to install and configure the AnyConnect client in a basic Cisco AnyConnect full tunnel solution, you will perform the following configuration tasks:

1. Manually install the Cisco AnyConnect client on the remote user PC.
2. Verify that the client has the necessary root CA certificates installed. The client should have a local, authentic copy of the CA certificate that was used to issue the Cisco ASA adaptive security appliance identity certificate.
3. Configure basic Cisco AnyConnect profile settings (the fully qualified domain name of the Cisco ASA adaptive security appliance).
4. Establish the SSL VPN full tunnel connection.



## Cisco AnyConnect Client

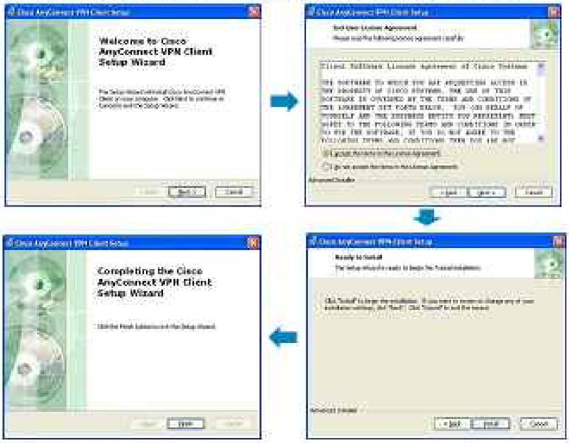
Configuration Scenario

Username and Password
Cisco ASA Adaptive Security Appliance Identity Certificate
Outside
Enterprise Network
Windows XP System
CA Certificate
DNS Infrastructure
Resolves vpn.domain.com to Appliance Outside Interface IP Address
Cisco ASA Adaptive Security Appliance

The figure presents the configuration scenario that is used in upcoming configuration tasks. The Cisco AnyConnect client will be installed on a Microsoft Windows XP system, and the Cisco ASA adaptive security appliance will use an identity certificate that was issued by the global PKI. The name vpn.domain.com will resolve to the security appliance outside interface IP address. This name will also be the identifier of the appliance in its identity certificate. The Cisco ASA adaptive security appliance will authenticate the remote users by using the username and password method.

## Cisco AnyConnect Client

### Task 1: Install the Predeploy AnyConnect Client


Cisco AnyConnect VPN Client Setup
Welcome to Cisco AnyConnect VPN Client Setup Wizard
End-User License Agreement
Ready to Install
Completing the Cisco AnyConnect VPN Client Setup Wizard

In the first task, you will install the predeploy version of the Cisco AnyConnect client. Perform the following steps on your client system:

**Step 1** Obtain the MSI installation package of the Cisco AnyConnect client from Cisco.com, and transfer it to the client.

**Step 2** Double-click the MSI installation package to start the installation process.

**Step 3** Click **Next** to start the installation dialog.

**Step 4** Examine the license agreement, check the **I Accept the Terms of the License Agreement** check box, and click **Next**.

**Step 5** Click **Install** to start the installation process.

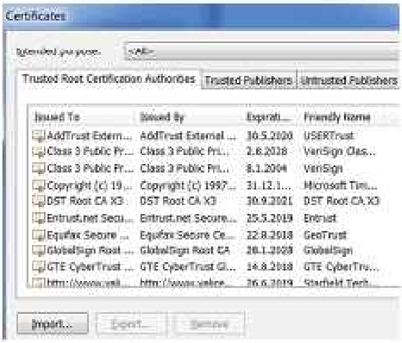
**Step 6** Click **Finish** to close the installer.

## Cisco AnyConnect Client

Task 2: Verify Server Certificate

The client certificate store must include the correct CA certificate:

- Cisco AnyConnect uses certificate store and preinstalled global CAs.
- This certificate must be obtained via a secure channel.
- If using an internal CA, import an authentic copy of your CA certificate.



| Issued To | Issued By | Expirati... | Friendly Name |
|---|---|---|---|
| AddTrust Extern... | AddTrust External ... | 30.5.2020 | USERTrust |
| Class 3 Public Pr... | Class 3 Public Pri... | 2.8.2028 | VeriSign Clas... |
| Class 3 Public Pr... | Class 3 Public Pri... | 8.1.2004 | VeriSign |
| Copyright (c) 19... | Copyright (c) 1997... | 31.12.1... | Microsoft Tim... |
| DST Root CA X3 | DST Root CA X3 | 30.9.2021 | DST Root CA X3 |
| Entrust.net Secu... | Entrust.net Secure... | 25.5.2019 | Entrust |
| Equifax Secure ... | Equifax Secure Ce... | 22.8.2018 | GeoTrust |
| GlobalSign Root ... | GlobalSign Root CA | 28.1.2028 | GlobalSign |
| GTE CyberTrust ... | GTE CyberTrust Gl... | 14.8.2018 | GTE CyberTru... |
| http://www.vali... | http://www.valice... | 26.6.2019 | Starfield Tech... |

Web Browser > Tools > Internet Options > Content > Certificates > Trusted Root Certification Authorities

In Task 2, on the client PC, examine the installed root CA certificates to determine that the CA that issued the Cisco ASA security appliance identity certificate is present. This verification will prevent certificate warnings from being displayed at SSL/TLS session establishment, and allow you to authenticate the appliance VPN gateway.

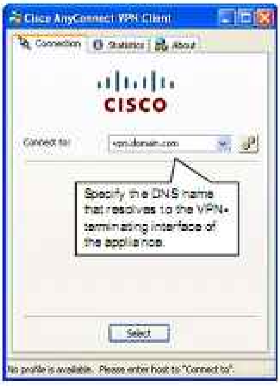
Typically, with global CAs, this verification will not be an issue as their CA certificates are embedded in the default operating system install or operating system updates. If you are using a nonglobal PKI, install the CA certificate to all client PCs.

## Cisco AnyConnect Client

### Task 3: Configure Basic Cisco AnyConnect Profile Settings

Start the Cisco AnyConnect client and specify gateway information:

- DNS name must match the name of the security appliance in the certificate canonical name field
- By clicking Select, the client will connect to the gateway



Connect to: vpn.domain.com

Specify the DNS name that resolves to the VPN-terminating interface of the appliance.

No profile is available. Please enter host to "Connect to".

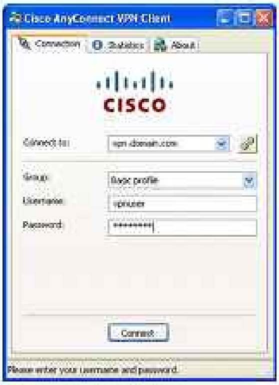
In Task 3, start the Cisco AnyConnect client and configure it with Cisco ASA adaptive security appliance VPN gateway information. In the Connect To field, enter the fully qualified domain name that resolves to the SSL-VPN-terminating interface of the security appliance. In the example, the **vpn.domain.com** fully qualified domain name (FQDN) has been used. This name must match the canonical name in the identity certificate of the Cisco ASA adaptive security appliance; otherwise, you will receive certificate name mismatch warnings. Click **Select** to make the Cisco AnyConnect client connect to the Cisco ASA adaptive security appliance using an SSL/TLS session.

## Cisco AnyConnect Client

Task 4: Establish the SSL VPN Connection

The client will download instructions for its next action from the gateway:

- Prompt for user authentication
- Enter your VPN username and password
- Click **Connect** to establish the SSL VPN tunnel



Cisco AnyConnect VPN Client

Connect to: vpn.domain.com

Group: Basic profile

Username: vpnuser

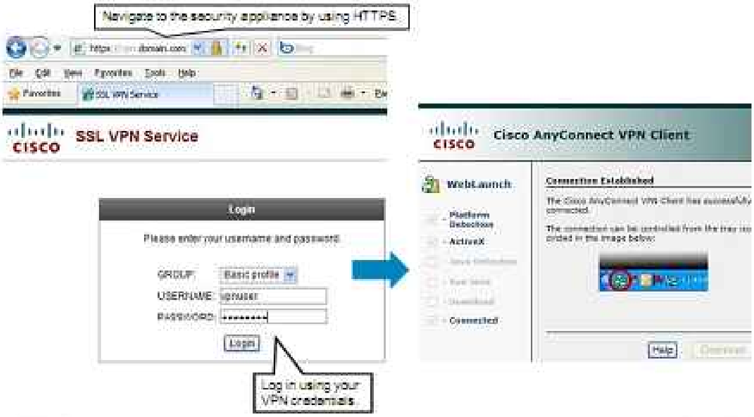
Password: *********

Please enter your username and password.

After the initial connection, the Cisco ASA adaptive security appliance will push instructions for the next step of VPN establishment to the Cisco AnyConnect client. In the example, the AnyConnect client will display the list of configured connection profile aliases (in the example, **Basic profile**, referencing the BASIC-ANYCONNECT-PROFILE, is the only available alias) and prompt you for user authentication. Enter your credentials, and click **Connect** to establish the VPN connection.

## Cisco AnyConnect Client

### Tasks 3 and 4: Alternatively, Using Web Launch



Navigate to the security appliance by using HTTPS.

Log in using your VPN credentials.

File Edit View Favorites Tools Help
Favorites
SSL VPN Service
SSL VPN Service
Login
Please enter your username and password.
GROUP: Basic profile
USERNAME: vpnuser
PASSWORD: ••••••••
Login
Cisco AnyConnect VPN Client
WebLaunch
Platform Detection
ActiveX
Java Detection
Sun Java
Download
Connected
Connection Established
The Cisco AnyConnect VPN Client has successfully connected.
The connection can be controlled from the tray icon circled in the image below:
Help
Download

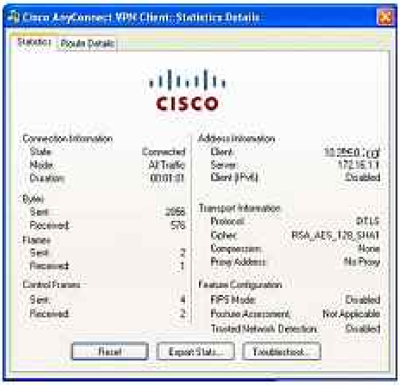
Alternatively, you can use the web launch feature to start the VPN connection by using a browser. If no web portal has been configured (for example, a clientless SSL VPN was not enabled on the security appliance interface), the security appliance will automatically start the Cisco AnyConnect client (using an ActiveX or Java applet, automatically selected depending on the user environment) after the user logs into the main page. The Cisco AnyConnect client will use the credentials that are supplied for the web page to attempt to log the user into the network.

## Verifying Cisco AnyConnect Session

Client-Side Verification

The AnyConnect client will automatically minimize by default.

- Open the AnyConnect GUI from the tray to examine session properties
- Nonzero sent and received bytes indicate proper routing to and from VPN addresses
- Details will reveal additional feature properties



Cisco AnyConnect VPN Client: Statistics Details

Connection Information
State: Connected
Mode: All Traffic
Duration: 00:01:01

Bytes
Sent: 2066
Received: 576

Frames
Sent: 2
Received: 1

Control Frames
Sent: 4
Received: 2

Address Information
Client: [illegible]
Server: 172.16.1.1
Client (IPv6): Disabled

Transport Information
Protocol: DTLS
Cipher: RSA_AES_128_SHA1
Compression: None
Proxy Address: No Proxy

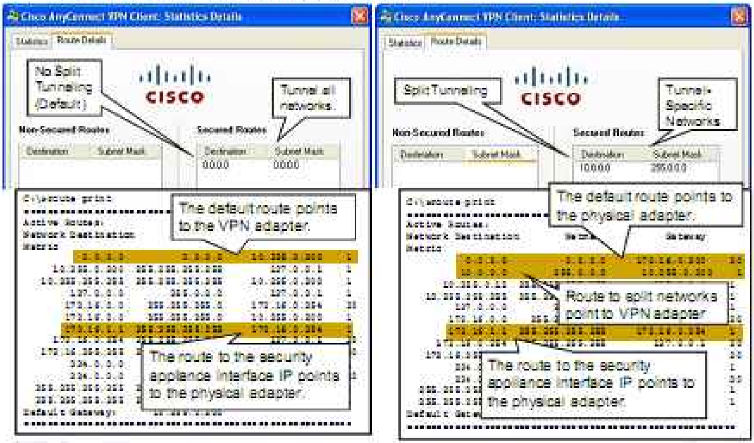
Feature Configuration
FIPS Mode: Disabled
Posture Assessment: Not Applicable
Trusted Network Detection: Disabled

The Cisco AnyConnect VPN Client will automatically minimize after a successful connection. You can verify connection properties by clicking the AnyConnect icon in the Windows icon tray. In its Statistics pane (not shown in the example), you can observe the state of the connection, the IP address that is assigned to the client, the bytes that are sent and received through the tunnel, and the connection time. By clicking the Details button, you can observe more detailed feature properties (shown in the example).

**Note** The client interface (Connection Pane > Disconnect) can also be used to log the user out.

## Verifying Cisco AnyConnect Session

Client-Side Verification (Cont.)


Cisco AnyConnect VPN Client: Statistics Details
Statistics
Route Details
No Split Tunneling (Default)
cisco
Tunnel all networks.
Non-Secured Routes
Secured Routes
Destination
Subnet Mask
0.0.0.0
0.0.0.0
The default route points to the VPN adapter.
The route to the security appliance interface IP points to the physical adapter.
Cisco AnyConnect VPN Client: Statistics Details
Statistics
Route Details
Split Tunneling
cisco
Tunnel- Specific Networks
Non-Secured Routes
Secured Routes
Destination
Subnet Mask
10.0.0.0
255.0.0.0
The default route points to the physical adapter.
Route to split networks point to VPN adapter
The route to the security appliance interface IP points to the physical adapter.

```
C:\>route print
===========================================
Active Routes:
Network Destination
Metric
          0.0.0.0          0.0.0.0     10.255.0.200   1
     10.255.0.200  255.255.255.255        127.0.0.1   1
   10.255.255.255  255.255.255.255     10.255.0.200   1
        127.0.0.0        255.0.0.0        127.0.0.1   1
       172.16.0.0    255.255.255.0     172.16.0.254  20
       172.16.0.0    255.255.255.0     10.255.0.200   1
       172.16.1.1  255.255.255.255     172.16.0.254   1
     172.16.0.254  255.255.255.255        127.0.0.1  20
   172.16.255.255
        224.0.0.0
        224.0.0.0
  255.255.255.255
  255.255.255.255
Default Gateway:
===========================================
```

```
C:\>route print
===========================================
Active Routes:
Network Destination          Netmask          Gateway
Metric
          0.0.0.0          0.0.0.0     172.16.1.200  20
         10.0.0.0        255.0.0.0      10.255.0.11   1
      10.255.0.11                                     1
   10.255.255.255                                     1
        127.0.0.0                                     1
       172.16.0.0                                    20
       172.16.1.1  255.255.255.255     172.16.1.254   1
     172.16.1.200  255.255.255.255        127.0.0.1  20
      172.16.255.                                    20
             224.                                     1
             224.                                    20
      255.255.255                                     1
      255.255.255                                     1
Default Gateway
===========================================
```

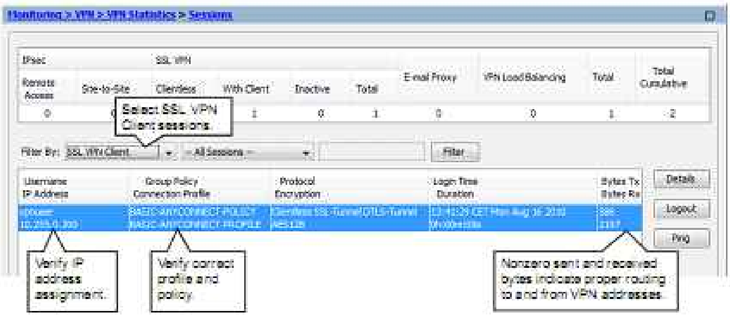
To verify the state of split tunneling and routing on the client, you can navigate to the Route Details tab of the Details window.

On the left side, you can see a client that is configured with no split tunneling (that is, the default setting). In the Secured Routes pane, you can see the default network 0.0.0.0/0 instructing all traffic to enter the tunnel. You can also verify this setting by using the **route print** Windows CMD command, where a default route should point to the VPN adapter (recognized by its assigned IP address).

On the right side, you can see a client that is configured for split tunneling. In the Secured Routes pane, you can see the default network 10.0.0.0/8 instructing only traffic to this specific network to enter the tunnel. You can also verify this setting by using the **route print** Windows CMD command, where a route to this network should point to the VPN adapter (recognized by its assigned IP address, 10.255.0.11). The default route should point to the physical interface of the client (172.16.1.200, in the example).

# Verifying Cisco AnyConnect Session

## Gateway-Side Verification



Monitoring > VPN > VPN Statistics > Sessions

| IPsec | | SSL VPN | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Remote Access | Site-to-Site | Clientless | With Client | Inactive | Total | E-mail Proxy | VPN Load Balancing | Total | Total Cumulative |
| 0 | 0 | | 1 | 0 | 1 | 0 | 0 | 1 | 2 |

Filter By: SSL VPN Client -- All Sessions -- Filter

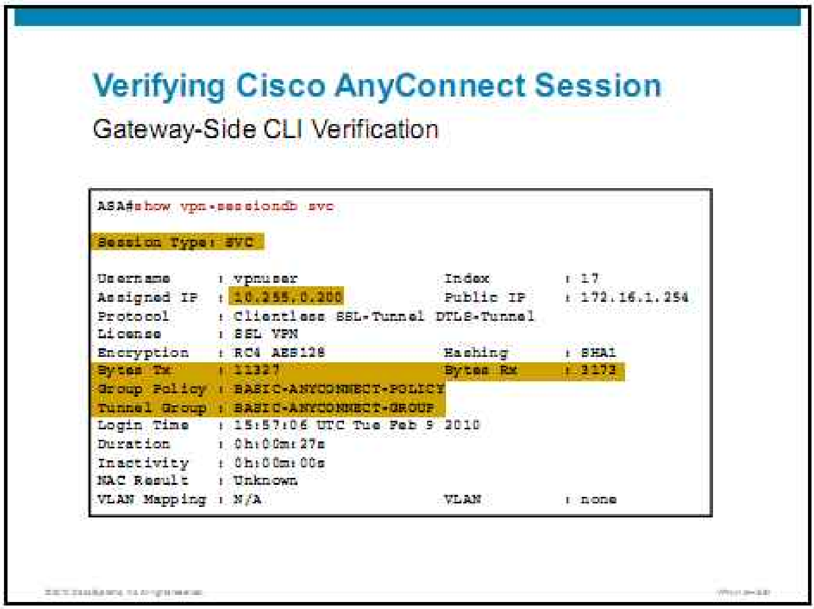
| Username<br>IP Address | Group Policy<br>Connection Profile | Protocol<br>Encryption | Login Time<br>Duration | Bytes Tx<br>Bytes Rx |
|---|---|---|---|---|
| vpnuser<br>10.255.0.200 | BASIC-ANYCONNECT-POLICY<br>BASIC-ANYCONNECT-PROFILE | Clientless SSL-Tunnel DTLS-Tunnel<br>AES128 | 12:41:29 CET Mon Aug 16 2010<br>0h:00m:[illegible] | 388<br>2317 |

Details
Logout
Ping
Select SSL VPN Client sessions.
Verify IP address assignment.
Verify correct profile and policy.
Nonzero sent and received bytes indicate proper routing to and from VPN addresses.

Monitoring > VPN > VPN Statistics > Sessions

To verify the connection of the client on the Cisco ASA adaptive security appliance, use Cisco ASDM to choose **Monitoring > VPN > VPN Statistics > Session**. From the drop-down menu, choose **SSL VPN Client** in the Filter By field. The VPN session should be displayed in the main pane.

In the example, you can see that the SSL VPN user with the vpnuser username has been assigned the 10.255.0.200 IP address. The group policy that is being used is BASIC-ANYCONNECT-POLICY, and the connection profile is BASIC-ANYCONNECT-PROFILE.



## Verifying Cisco AnyConnect Session

Gateway-Side CLI Verification

```
ASA#show vpn-sessiondb svc

Session Type: SVC

Username     : vpnuser                   Index        : 17
Assigned IP  : 10.255.0.200              Public IP    : 172.16.1.254
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : RC4 AES128                Hashing      : SHA1
Bytes Tx     : 11327                     Bytes Rx     : 3173
Group Policy : BASIC-ANYCONNECT-POLICY
Tunnel Group : BASIC-ANYCONNECT-GROUP
Login Time   : 15:57:06 UTC Tue Feb 9 2010
Duration     : 0h:00m:27s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                       VLAN         : none
```

In the CLI, use the **show vpn-sessiondb svc** command to obtain the same information.

## 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. It also lets you specify the type of sessions to display, and it 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**}]

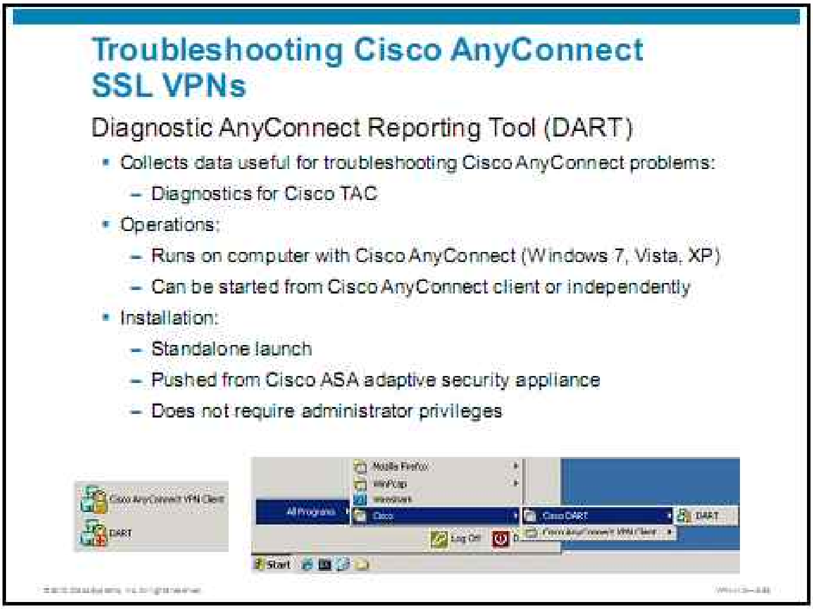
### show vpn-sessiondb Parameters

| Parameter | Description |
|---|---|
| `detail` | (Optional) Displays extended details about a session. For example, using the **detail** option for an IPsec session displays additional details such as the Internet Key Exchange (IKE) hashing algorithm, authentication mode, and rekey interval.<br>If you choose **detail** with the **full** option, the adaptive security appliance displays the detailed output in a machine-readable format. |
| `filter` *`filter_criteria`* | (Optional) Filters the output to display only the information you specify by using one or more of the filter options. |
| `full` | (Optional) Displays streamed, untruncated output. Output is delineated by horizontal bar ("\|") characters and a double horizontal bar ("\|\|") string between records. |

| Parameter | Description |
|---|---|
| *session_type* | (Optional) To show data for a specific session type, enter one of the following keywords:<br>■ **email-proxy:** Displays email-proxy sessions.<br>■ **index** *indexnumber*: Displays a single session by index number. Specify the index number for the session, 1–750.<br>■ **l2l:** Displays VPN LAN-to-LAN (L2L) session information.<br>■ **ratio:** Displays VPN session protocol or encryption ratios.<br>■ **remote:** Displays IPsec remote access sessions.<br>■ **summary:** Displays the VPN session summary.<br>■ **svc:** Displays Cisco VPN Client sessions.<br>■ **vpn-lb:** Displays VPN load-balancing management sessions.<br>■ **webvpn:** Displays information about clientless SSL VPN sessions. |
| **sort** *sort_criteria* | (Optional) Sorts the output according to the sort option that you specify. |

# Troubleshooting Basic Full Tunnel SSL VPN Operation

This topic explains how to deploy the Diagnostic AnyConnect Reporting Tool (DART) and troubleshoot full tunnel SSL VPN session establishment between a Cisco AnyConnect client and a Cisco ASA adaptive security appliance VPN gateway.



## Troubleshooting Cisco AnyConnect SSL VPNs

### Diagnostic AnyConnect Reporting Tool (DART)

- Collects data useful for troubleshooting Cisco AnyConnect problems:
  - Diagnostics for Cisco TAC
- Operations:
  - Runs on computer with Cisco AnyConnect (Windows 7, Vista, XP)
  - Can be started from Cisco AnyConnect client or independently
- Installation:
  - Standalone launch
  - Pushed from Cisco ASA adaptive security appliance
  - Does not require administrator privileges

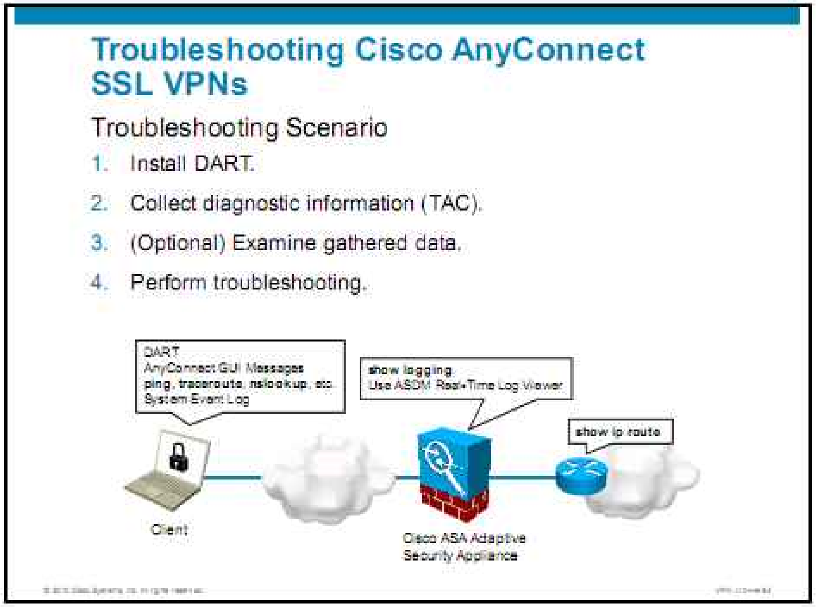
You can use DART to collect data that is useful for troubleshooting Cisco AnyConnect install and connection problems. DART supports Microsoft Windows XP, Microsoft Windows Vista, and Microsoft Windows 7.

The DART wizard runs on the computer that runs the Cisco AnyConnect client. Without requiring administrator privileges, DART assembles the log, status, and diagnostic information for Cisco Technical Assistance Center (TAC) analysis.

DART does not rely on any component of the Cisco AnyConnect software to run, though you can launch DART from AnyConnect, and DART does collect the Cisco AnyConnect log file, if it is available.

Any version of DART works with any version of Cisco AnyConnect; the version numbers of each are no longer synchronized. To optimize DART, it is recommend to download the most recent version that is available on the Cisco AnyConnect VPN Client Software Download site, regardless of the AnyConnect version you are using.

DART is currently available as a standalone installation, or the administrator can push this application to the client PC as part of the Cisco AnyConnect dynamic download infrastructure. Once installed, the DART wizard can be launched from the Cisco folder available through the Start button.



## Troubleshooting Cisco AnyConnect SSL VPNs

### Troubleshooting Scenario

1. Install DART.
2. Collect diagnostic information (TAC).
3. (Optional) Examine gathered data.
4. Perform troubleshooting.

DART
AnyConnect GUI Messages
**ping, traceroute, nslookup, etc.**
System Event Log

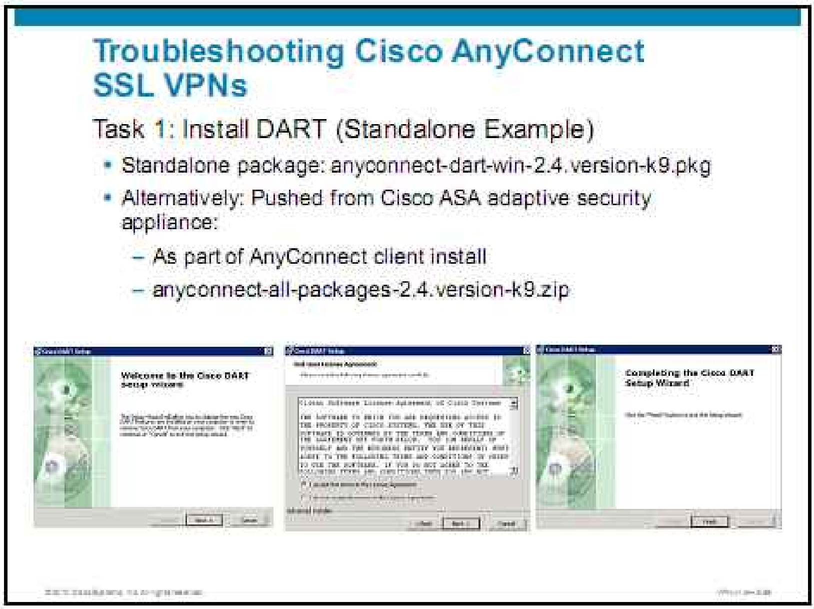
**show logging**
Use ASDM Real-Time Log Viewer

**show ip route**

When troubleshooting Cisco AnyConnect SSL VPNs, you will typically perform these tasks:

1. Install DART.
2. Collect diagnostic information (TAC).
3. Optionally, examine the gathered data.
4. Perform troubleshooting on both the client and the Cisco ASA adaptive security appliance. Sometimes, you may need to also resolve routing issues on adjacent network devices. The figure shows some of the most useful troubleshooting commands and actions that you can use on involved components.

**Note** The Cisco ASA adaptive 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.



## Troubleshooting Cisco AnyConnect SSL VPNs

Task 1: Install DART (Standalone Example)

- Standalone package: anyconnect-dart-win-2.4.version-k9.pkg
- Alternatively: Pushed from Cisco ASA adaptive security appliance:
  - As part of AnyConnect client install
  - anyconnect-all-packages-2.4.version-k9.zip

Welcome to the Cisco DART Setup Wizard
Cisco Software License Agreement
Completing the Cisco DART Setup Wizard

DART is available as part of the Cisco AnyConnect client download and installation package, or as a standalone .msi file.

Following are the AnyConnect downloads, containing DART, on Cisco.com. Refer to the Release Notes for the Cisco AnyConnect VPN Client for the latest version numbers:

- **anyconnect-all-packages-2.4.version-k9.zip:** Contains all Cisco AnyConnect packages. When the user downloads the AnyConnect client, a new version of DART, if available, is also automatically downloaded to the PC of the user. When a new version of the Cisco AnyConnect client is downloaded as part of an automatic upgrade, that download includes a new version of DART, if there is one.
- **anyconnect-dart-win-2.4.version-k9.pkg:** Contains only the DART installation package, not the Cisco AnyConnect or VPNGINA software. Use this download when installing DART as a standalone application.

## Installing DART with Cisco AnyConnect

Perform this procedure to download DART to the machine of the remote user the next time the user connects:

**Step 1** Load the Cisco AnyConnect package containing DART to the security appliance, just as you would any other Cisco software package.

**Step 2** After installing the Cisco AnyConnect .pkg file containing DART on the security appliance, you must specify DART in a group policy, in order for it to be installed with AnyConnect:

- Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** and add a new group policy or edit an existing group policy. In the group policy dialog box, expand the **Advanced** selection and click **SSL VPN Client**.

- In the SSL VPN Client dialog box, uncheck **Inherit** for the Optional Client Modules to Download check box. Choose the DART module in the option drop-down list.
- If the version of Cisco ASDM that you are using does not have the DART option check box, enter the keyword **dart**in the field. Click **OK**, and then click **Apply**.

## Manually Installing DART on the Host

Perform these steps to install DART using the standalone package:

**Step 1** Obtain the DART software from Cisco.com (http://www.cisco.com/pcgi-bin/tablebuild.pl/anyconnect). Store the anyconnect-dart-win-2.4.version-k9.pkg file locally.

**Step 2** Using a file compression utility, extract the contents of the anyconnect-dart-win-2.4.version-k9.pkg file and maintain the directory structure.

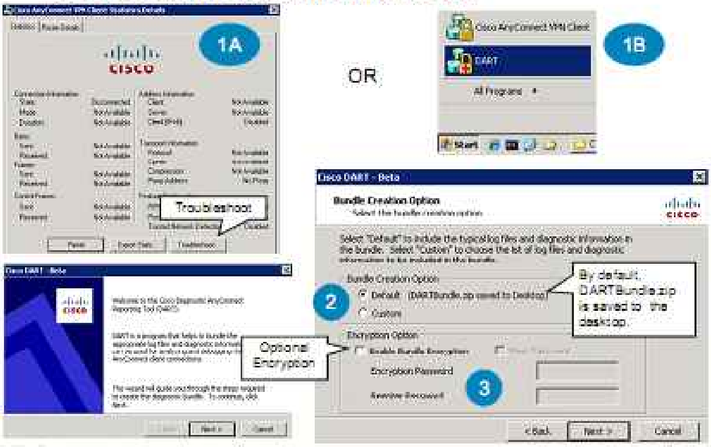
**Step 3** Open the binaries directory that is created from extracting the contents of the anyconnect-dart-win-2.4.version-k9.pkg file.

**Step 4** Double-click the **anyconnect-dart-win-2.4.version-k9.msi** file to launch the DART Setup Wizard.

**Step 5** Follow the wizard prompts. The installation wizard installs DartOffline.exe in the <System Drive>:\Program Files\Cisco\Cisco DART directory. Click **Finish** to complete the installation.

## Troubleshooting Cisco AnyConnect SSL VPNs

### Task 2: Collect Diagnostic Information



Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.

You must launch the DART wizard to collect diagnostic information. Follow these steps to create a DART bundle on a Windows PC:

**Step 1** Start the DART wizard by using one of the two options:

- From the Cisco AnyConnect client GUI, click the **Statistics** tab and then click the **Details** button at the bottom of the dialog box. This action opens the Statistics Details dialog box. Click **Troubleshoot** at the bottom of the Statistics Details window.
- From the Start menu, choose and launch the DART wizard.

Click **Next** at the Welcome screen. This brings you to the Bundle Creation Option dialog box.

**Step 2** In the Bundle Creation Option area, choose **Default** or **Custom**:

- The Default option includes the typical log files and diagnostic information, such as the Cisco AnyConnect and Cisco Secure Desktop log files, general information about the computer, and a summary of what DART did and did not do.
- When you choose **Default** and then click **Next** at the bottom of the dialog box, DART immediately begins creating the bundle. The default name for the bundle is DARTBundle.zip, and it is saved to the local desktop.
- If you choose **Custom**, the DART wizard will present you with more dialog boxes after you click **Next**. These boxes will allow you to specify which files you want to include in the bundle and where to store the bundle.

**Step 3** If you want to encrypt the DART bundle, in the Encryption Option area, check the **Enable Bundle Encryption** check box. Then, enter a password in the Encryption Password field. Optionally, check the **Mask Password** check box. This selection will cause the password that you enter in the Encryption Password and Reenter Password fields to be masked with asterisks (*).

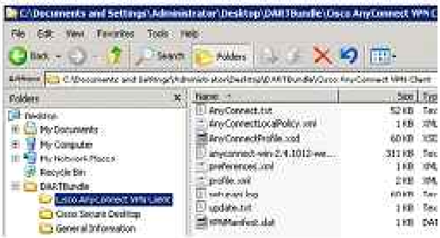
**Step 4** Follow the wizard to create the bundle.

## Troubleshooting Cisco AnyConnect SSL VPNs

### Task 3: (Optional) Examine Gathered Data

Three folders:

- Cisco AnyConnect VPN Client
- Cisco Secure Desktop
- General Information

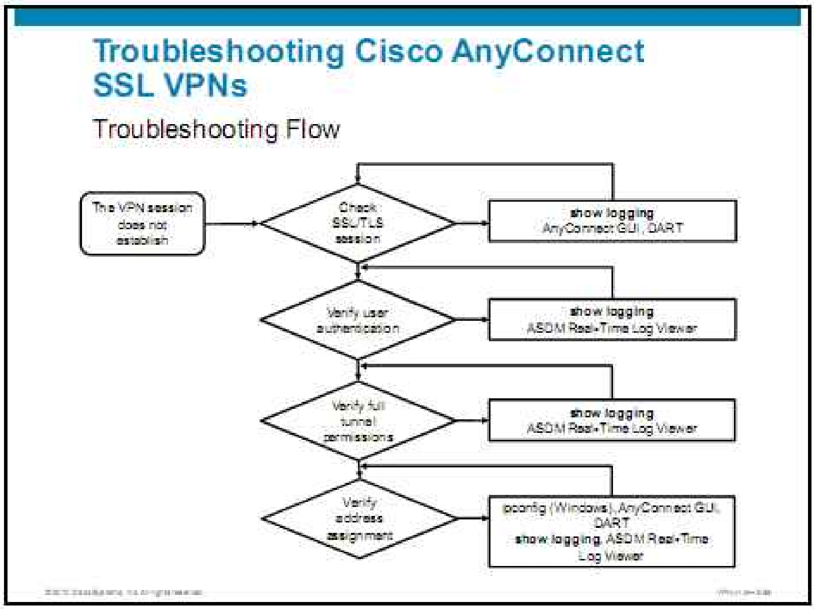

C:\Documents and Settings\Administrator\Desktop\DARTBundle\Cisco AnyConnect VPN C
File Edit View Favorites Tools Help
Back
Search
Folders
Address C:\Documents and Settings\Administrator\Desktop\DARTBundle\Cisco AnyConnect VPN Client
Folders
Desktop
My Documents
My Computer
My Network Places
Recycle Bin
DARTBundle
Cisco AnyConnect VPN Client
Cisco Secure Desktop
General Information
Name
Size
Typ

| Name | Size | Typ |
|---|---|---|
| AnyConnect.txt | 52 KB | Tex |
| AnyConnectLocalPolicy.xml | 1 KB | XML |
| AnyConnectProfile.xsd | 60 KB | XSD |
| anyconnect-win-2.4.1012-we... | 311 KB | Tex |
| preferences.xml | 1 KB | XML |
| profile.xml | 2 KB | XML |
| setupapi.log | 60 KB | Tex |
| update.txt | 1 KB | Tex |
| VPNManifest.dat | 1 KB | DAT |

Summary.txt:

```
DART BUNDLE SUMMARY
Username:              unknown (user is offline, or username was not specified in Request)
Time:                 07/07/2010 13:52:27 Central Europe Daylight Time
OS:                  WinXP : WinNT 5.1.2600 Service Pack 2
OS username:              Administrator
Upload URL:              None (offline mode)
DART Mode:               User-Initiated/Offline Mode
Bundle on client computer:   C:\Documents and Settings\Administrator\Desktop\DARTBundle
<text truncated>
```

DART generates a bundle that is useful when escalating the problem to Cisco TAC or another troubleshooting team. The bundle, when unpacked, contains three folders with diagnostic information: Cisco AnyConnect VPN Client, Cisco Secure Desktop, and General Information. You may examine the logs when you are troubleshooting AnyConnect problems.



## Troubleshooting Cisco AnyConnect SSL VPNs

### Troubleshooting Flow

The VPN session does not establish

Check SSL/TLS session

**show logging**
AnyConnect GUI , DART

Verify user authentication

**show logging**
ASDM Real-Time Log Viewer

Verify full tunnel permissions

**show logging**
ASDM Real-Time Log Viewer

Verify address assignment

ipconfig (Windows), AnyConnect GUI, DART
**show logging**, ASDM Real-Time Log Viewer

If you are encountering session establishment issues, you may follow these steps to troubleshoot the issues:

**Step 1** First, check that the SSL/TLS session initially establishes, and that there are no negotiation problems that are related to the use of incompatible protocol versions or cipher suites. You can observe these issues in the Cisco AnyConnect GUI, but you will obtain more-detailed and specific information by examining Cisco ASA adaptive security appliance syslog messages.

**Step 2** If the SSL/TLS negotiation completes with no errors, check whether user authentication works and whether the user is supplying the correct credentials. The Cisco ASA adaptive security appliance will clearly indicate these issues in its syslog messages.

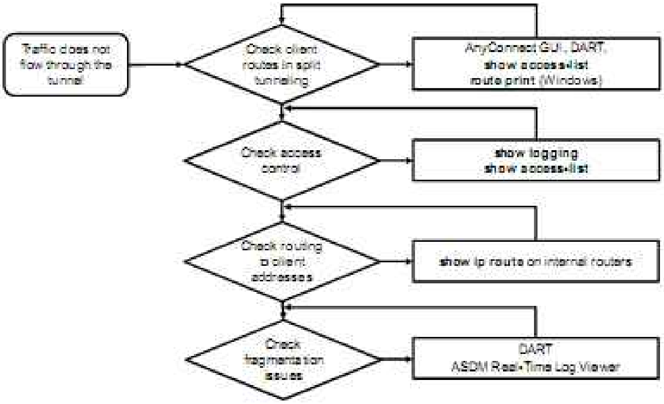
**Step 3** Next, check whether the connection profile and the associated group policy allow SSL VPN tunnels. The Cisco ASA adaptive security appliance will clearly indicate these issues in its syslog messages.

**Step 4** Finally, verify that the Cisco ASA adaptive security appliance is able to assign an IP address to the client. The IP Address Assignment (IPAA) subsystem will extensively log to the syslog subsystem to indicate any issues.

If all these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.

## Troubleshooting Cisco AnyConnect SSL VPNs

### Troubleshooting Flow (Cont.)



Traffic does not flow through the tunnel

Check client routes in split tunneling

AnyConnect GUI, DART, **show access-list** **route print** (Windows)

Check access control

**show logging**
**show access-list**

Check routing to client addresses

**show ip route** on internal routers

Check fragmentation issues

DART
ASDM Real-Time Log Viewer

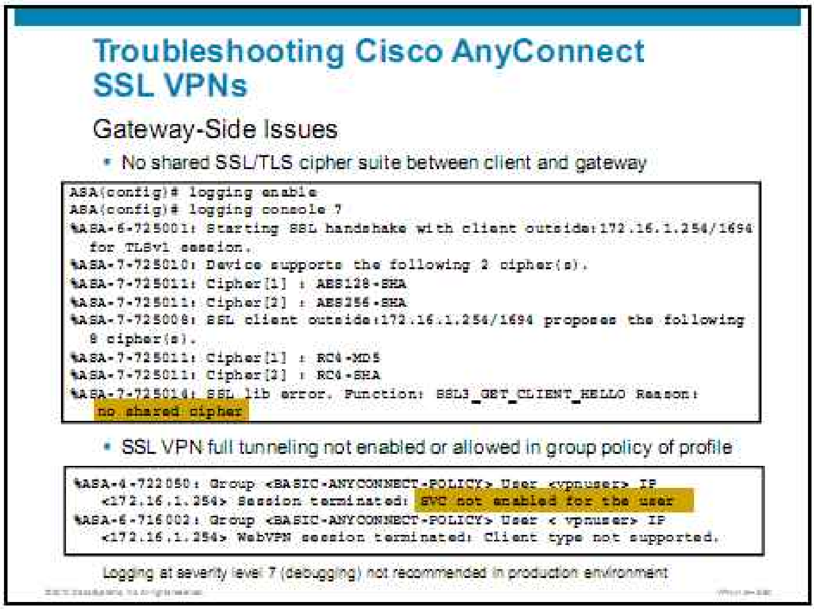
If your SSL VPN session establishes, but there is no connectivity over the tunnel, you may follow these steps to troubleshoot the issue:

**Step 1** First, if you are using split tunneling, check that the correct routes (networks) to the tunneled destination are present in the routing table of the client PC. You can observe this information in the Cisco AnyConnect GUI, or by examining the routing table of the client PC.

**Step 2** Next, verify that the Cisco ASA adaptive security appliance is not denying traffic from the VPN tunnel. Examine the Cisco ASA adaptive security appliance syslog to see messages regarding permitted or denied packets.

**Step 3** Finally, verify that the protected network has a route to the client-assigned addresses by examining routing tables in internal network routers along the path to the destination.

If all these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.



## Troubleshooting Cisco AnyConnect SSL VPNs

### Gateway-Side Issues

- No shared SSL/TLS cipher suite between client and gateway

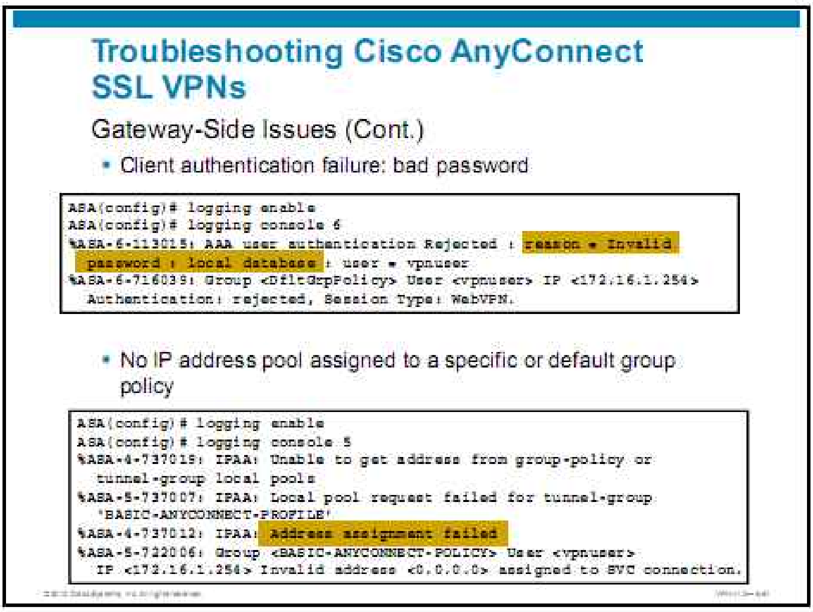
```
ASA(config)# logging enable
ASA(config)# logging console 7
%ASA-6-725001: Starting SSL handshake with client outside:172.16.1.254/1694
  for TLSv1 session.
%ASA-7-725010: Device supports the following 2 cipher(s).
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725011: Cipher[2] : AES256-SHA
%ASA-7-725008: SSL client outside:172.16.1.254/1694 proposes the following
  8 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-MD5
%ASA-7-725011: Cipher[2] : RC4-SHA
%ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason:
  no shared cipher
```

- SSL VPN full tunneling not enabled or allowed in group policy of profile

```
%ASA-4-722050: Group <BASIC-ANYCONNECT-POLICY> User <vpnuser> IP
   <172.16.1.254> Session terminated: SVC not enabled for the user
%ASA-6-716002: Group <BASIC-ANYCONNECT-POLICY> User < vpnuser> IP
   <172.16.1.254> WebVPN session terminated: Client type not supported.
```

Logging at severity level 7 (debugging) not recommended in production environment

The outputs in this figure list the Cisco ASA adaptive security appliance syslog messages that indicate two common session establishment issues: a failed SSL/TLS negotiation due to incompatible cipher suites, and a session teardown due to the SSL VPN full tunnel function not being enabled for a user, a connection profile, or a group policy.



## Troubleshooting Cisco AnyConnect SSL VPNs

### Gateway-Side Issues (Cont.)

- Client authentication failure: bad password

```
ASA(config)# logging enable
ASA(config)# logging console 6
%ASA-6-113015: AAA user authentication Rejected : reason = Invalid
  password : local database : user = vpnuser
%ASA-6-716039: Group <DfltGrpPolicy> User <vpnuser> IP <172.16.1.254>
  Authentication: rejected, Session Type: WebVPN.
```

- No IP address pool assigned to a specific or default group policy

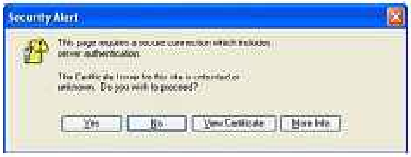
```
ASA(config)# logging enable
ASA(config)# logging console 5
%ASA-4-737019: IPAA: Unable to get address from group-policy or
  tunnel-group local pools
%ASA-5-737007: IPAA: Local pool request failed for tunnel-group
  'BASIC-ANYCONNECT-PROFILE'
%ASA-4-737012: IPAA: Address assignment failed
%ASA-5-722006: Group <BASIC-ANYCONNECT-POLICY> User <vpnuser>
  IP <172.16.1.254> Invalid address <0.0.0.0> assigned to SVC connection.
```

The outputs in this figure list the Cisco ASA adaptive security appliance syslog messages that indicate failed user authentication due to a bad password, and a failed IP address assignment due to a lack of IP address pools configured on the Cisco ASA adaptive security appliance.

## Troubleshooting Cisco AnyConnect SSL VPNs

### Client-Side Issues: Certificates

- A certificate warning can appear because of:
  - Unverifiable security appliance identity certificate
  - A name mismatch between certificate canonical name and AnyConnect profile hostname
  - An expired security appliance identity certificate
- You should *never* see this issue in production use:
  - This message indicates a man-in-the-middle attack
  - If users are conditioned to accept, they negate all SSL/TLS protection



Security Alert

This page requires a secure connection which includes server authentication.

The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?

[illegible]

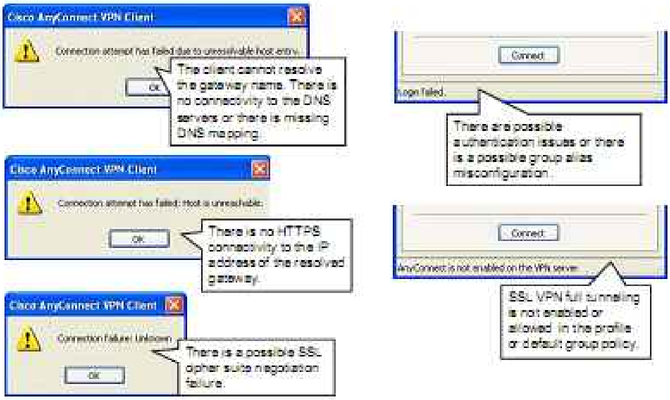
On the client, the most common issue that you may observe is a certificate warning at VPN session establishment. There are three main reasons for this message to appear:

- The Cisco ASA adaptive security appliance identity certificate is not verifiable, due to a missing CA certificate on the client that should be used to verify the signature of the appliance identity certificate. To resolve this issue, install an authentic copy of the CA certificate on the client.
- A name mismatch between the name that is specified in the Cisco AnyConnect profile (in the Connect To field), and the canonical name field in the security appliance identity certificate. To resolve this issue, fix either of these values to match the other.
- An expired Cisco ASA adaptive security appliance identity certificate. To resolve this issue, renew the security appliance identity certificate.

You should never see these issues occurring during production use of the network. If users are conditioned to proceed with the VPN connection despite these warnings, their VPN connection will be vulnerable to man-in-the-middle interception attacks, where the attacker poses as the Cisco ASA security appliance and terminates VPN connections from legitimate users. This message is the only message that indicates such an attack.

## Troubleshooting Cisco AnyConnect SSL VPNs

### Client-Side Notifications



Cisco AnyConnect VPN Client

Connection attempt has failed due to unresolvable host entry.

The client cannot resolve the gateway name. There is no connectivity to the DNS servers or there is missing DNS mapping.

Cisco AnyConnect VPN Client

Connection attempt has failed: Host is unreachable.

There is no HTTPS connectivity to the IP address of the resolved gateway.

Cisco AnyConnect VPN Client

Connection failure: Unknown

There is a possible SSL cipher suite negotiation failure.

Login failed.

There are possible authentication issues or there is a possible group alias misconfiguration.

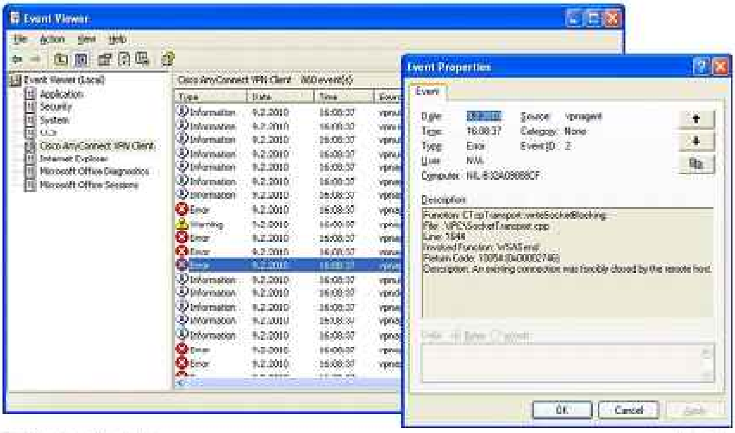
AnyConnect is not enabled on the VPN server.

SSL VPN full tunneling is not enabled or allowed in the profile or default group policy.

During session establishment, the client will display informative messages that you can use to pinpoint the cause of an issue. The figure shows the five common scenarios and the messages that they produce inside the Cisco AnyConnect GUI.

## Troubleshooting Cisco AnyConnect SSL VPNs

### Client-Side Notifications: Windows Event Viewer



Date:
Time: 16:08:37
Type: Error
User: N/A
Computer: NIL-B32A09089CF
Source: vpnagent
Category: None
Event ID: 2

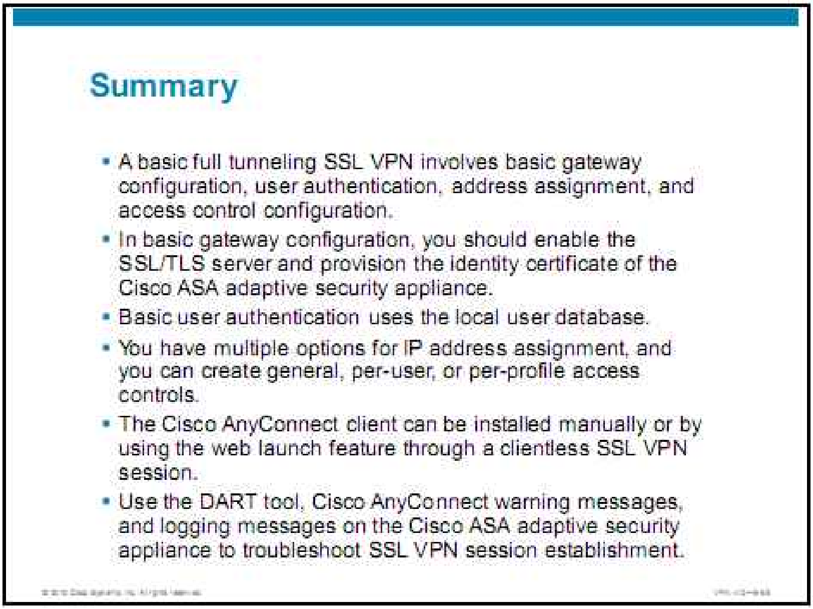
Description:

Function: CTcpTransport::writeSocketBlocking
File: .\IPC\SocketTransport.cpp
Line: 1544
Invoked Function: WSASend
Return Code: 10054 (0x00002746)
Description: An existing connection was forcibly closed by the remote host.

The Cisco AnyConnect client will also use the Windows Event Log to store all error messages, as well as informational messages about client operation. You can use the Windows Event Viewer to examine this log for past and current issues with client operation.

# Summary

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



## Summary

- A basic full tunneling SSL VPN involves basic gateway configuration, user authentication, address assignment, and access control configuration.
- In basic gateway configuration, you should enable the SSL/TLS server and provision the identity certificate of the Cisco ASA adaptive security appliance.
- Basic user authentication uses the local user database.
- You have multiple options for IP address assignment, and you can create general, per-user, or per-profile access controls.
- The Cisco AnyConnect client can be installed manually or by using the web launch feature through a clientless SSL VPN session.
- Use the DART tool, Cisco AnyConnect warning messages, and logging messages on the Cisco ASA adaptive security appliance to troubleshoot SSL VPN session establishment.

## Lesson 2

# Deploying Advanced Cisco AnyConnect VPN Client

## Overview

Different deployment objectives require a scalable and flexible solution. This lesson enables you to deploy and manage advanced deployment functionality of the Cisco AnyConnect VPN Client.

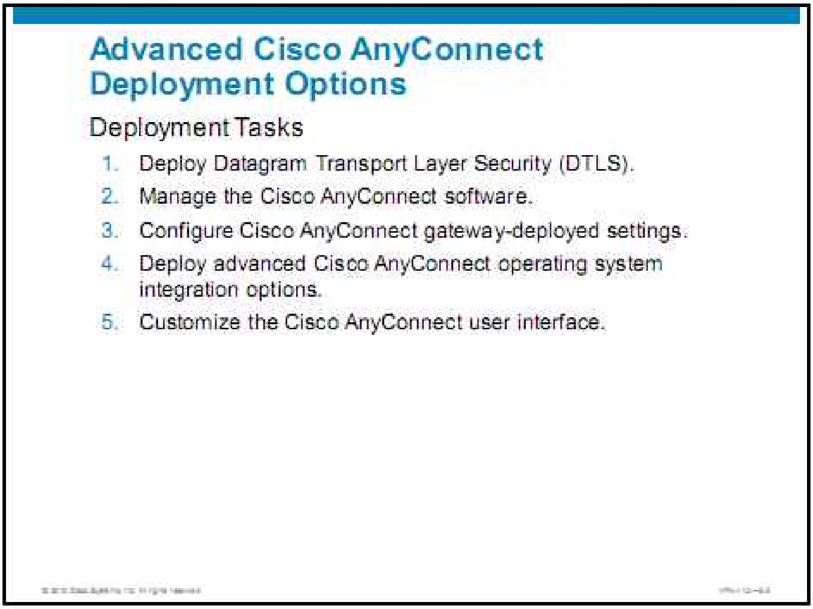
## Objectives

Upon completing this lesson, you will be able to deploy and manage the advanced centrally configured features of the Cisco AnyConnect VPN Client. This ability includes being able to meet these objectives:

- Configure and verify DTLS encapsulation in Cisco ASA adaptive security appliance Cisco AnyConnect full tunnel VPNs
- Choose centrally controlled client functions in Cisco AnyConnect full tunnel SSL VPNs
- Manage Cisco AnyConnect software
- Configure and verify Cisco AnyConnect client profiles
- Deploy advanced Cisco AnyConnect operating system integration options
- Configure and verify Cisco AnyConnect user interface customization

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic provides an overview of how to choose centrally controlled client functions in Cisco AnyConnect full tunnel Secure Sockets Layer (SSL) virtual private networks (VPNs).



## Advanced Cisco AnyConnect Deployment Options

Deployment Tasks

1. Deploy Datagram Transport Layer Security (DTLS).
2. Manage the Cisco AnyConnect software.
3. Configure Cisco AnyConnect gateway-deployed settings.
4. Deploy advanced Cisco AnyConnect operating system integration options.
5. Customize the Cisco AnyConnect user interface.

The deployment tasks for centrally controlled client functions in the Cisco AnyConnect VPN Client include the following:

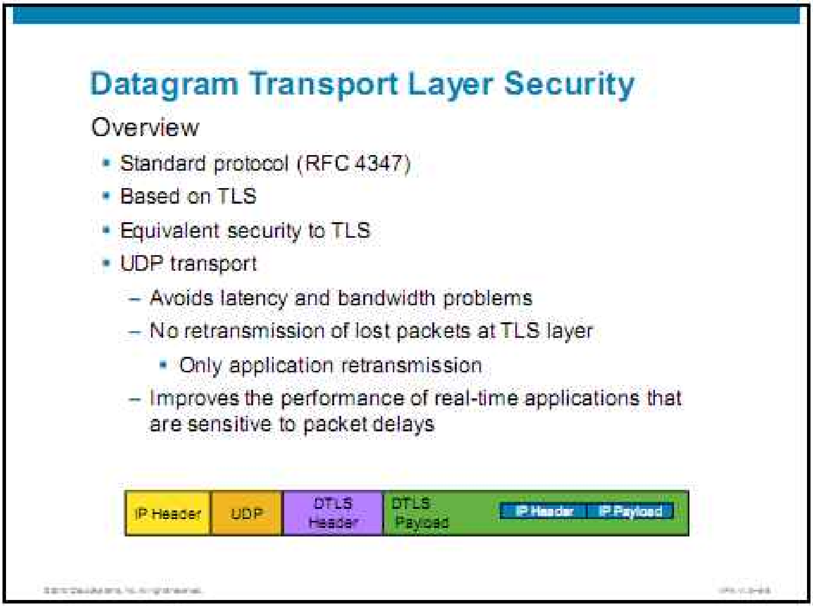
1. Deploy Datagram Transport Layer Security (DTLS).
2. Manage Cisco AnyConnect software.
3. Configure Cisco AnyConnect gateway-deployed settings.
4. Deploy advanced Cisco AnyConnect operating system integration options.
5. Customize the Cisco AnyConnect user interface.

Before you deploy the Cisco AnyConnect VPN Client, several input parameters need to be examined in order to ensure success:

- Ensure that the Cisco AnyConnect VPN Client exists for operating systems that are used by your clients.
- Determine the experience and environment integration needs of future VPN users in order to select the customization options that need to be deployed.
- Consult client security policy to determine software update requirements.
- Determine any requirements for Cisco AnyConnect user interface customization and localization needs. These needs can be different based on the country where the Cisco AnyConnect client is used, owing to different laws, different languages, and so on.

# Deploying DTLS

This topic describes how to improve Cisco AnyConnect VPN Client performance by using DTLS.



## Datagram Transport Layer Security

Overview

- Standard protocol (RFC 4347)
- Based on TLS
- Equivalent security to TLS
- UDP transport
  - Avoids latency and bandwidth problems
  - No retransmission of lost packets at TLS layer
    - Only application retransmission
  - Improves the performance of real-time applications that are sensitive to packet delays

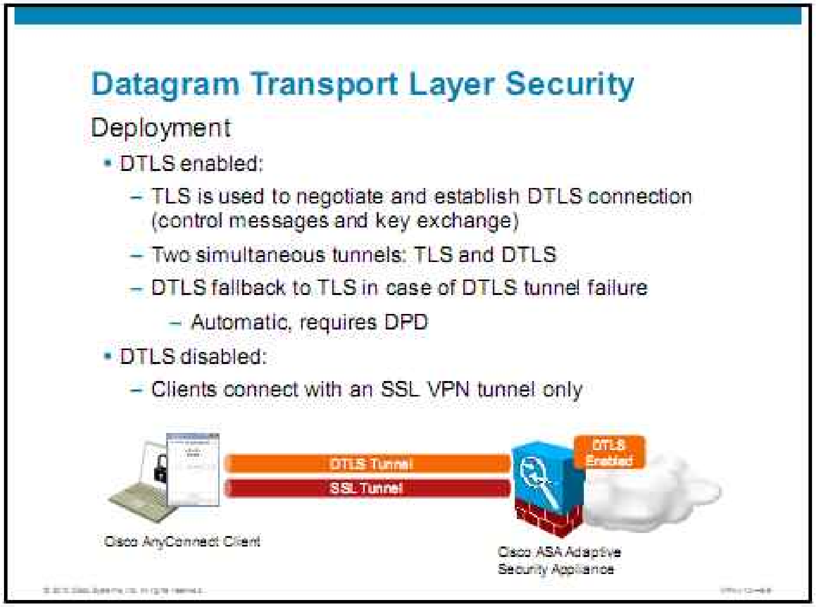
IP Header
UDP
DTLS Header
DTLS Payload
IP Header
IP Payload

Datagram Transport Layer Security (DTLS) is an alternative VPN transport protocol to Secure Sockets Layer (SSL)/Transport Layer Security (TLS). DTLS allows datagram-based applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the stream-oriented TLS protocol and is intended to provide similar security guarantees.

DTLS mitigates latency and bandwidth problems that are associated with some SSL-only connections, and improves the performance of real-time applications that are sensitive to packet delays. DTLS is a standards-based SSL protocol that provides a low-latency data path using UDP. It is defined in RFC 4347.

DTLS improves the application performance in two ways:

- User Datagram Protocol (UDP) transport does not stipulate any retransmissions on the VPN layer. If VPN packets are lost in transit, only the TCP stack of the application endpoints will retransmit the datagrams. In contrast, when VPN packets that are transported over an SSL session are lost, both the SSL VPN endpoint and the TCP stack of the application endpoint will retransmit the packet.
- UDP is simpler than TCP, creates less overhead, and consumes fewer resources.



## Datagram Transport Layer Security

### Deployment

- DTLS enabled:
  - TLS is used to negotiate and establish DTLS connection (control messages and key exchange)
  - Two simultaneous tunnels: TLS and DTLS
  - DTLS fallback to TLS in case of DTLS tunnel failure
    - Automatic, requires DPD
- DTLS disabled:
  - Clients connect with an SSL VPN tunnel only

Enabling DTLS allows the Cisco AnyConnect VPN Client that is establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel.

The SSL/TLS channel is used to negotiate and establish the DTLS tunnel by exchanging a series of secured control and key exchange messages.

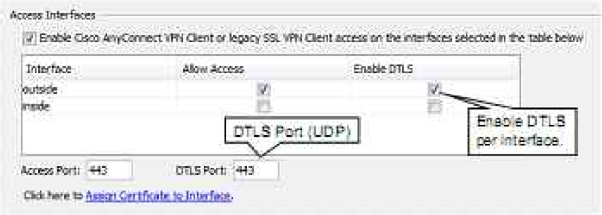
The security appliance supports an automatic fallback from DTLS to TLS if DTLS is no longer working. The DTLS-to-TLS fallback requires that dead peer detection (DPD) is enabled. DPD is described later in this lesson. If the DTLS tunnel does not work and DPD is not enabled, connectivity is broken.

If you do not enable DTLS, Cisco AnyConnect client users who are establishing SSL VPN connections connect with an SSL VPN tunnel only.

## Configuring DTLS

### Enable DTLS Globally

- DTLS takes precedence over SSL.
- DTLS is enabled by default.
- Default DTLS port is 443.



Access Interfaces

☑ Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below

| Interface | Allow Access | Enable DTLS |
|---|---|---|
| outside | ☑ | ☑ |
| inside | □ | □ |

Access Port: 443 DTLS Port: 443

Click here to Assign Certificate to Interface.

DTLS Port (UDP)

Enable DTLS per interface.

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

When configuring DTLS, you have to first make sure that DTLS is enabled globally. To configure DTLS globally, complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

**Step 2** Choose an interface that is configured for an SSL VPN.

**Step 3** Check the check box under the **Enable DTLS** column for the desired interface.

---

**Note** By default, the SSL VPN wizard will enable DTLS on the interface that is configured for Cisco AnyConnect SSL VPN service.

---

**Step 4** Enter the DTLS port number (UDP) in the DTLS port field. The default value is 443, the same as for SSL/TLS that uses TCP.

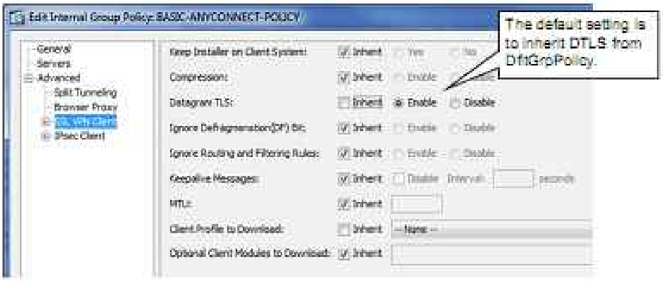
**Step 5** Click **Apply** to apply the configuration.

In this figure, the outside interface is configured to use DTLS with the Cisco AnyConnect SSL VPN.

## Configuring DTLS

### Configure DTLS in Group Policy

- DTLS can be activated on group or user policy level
  - Must be enabled on an interface
- DfltGrpPolicy has DTLS activated by default



Edit Internal Group Policy: BASIC-ANYCONNECT-POLICY

Keep Installer on Client System: ☑ Inherit ○ Yes ○ No
Compression: ☑ Inherit ○ Enable ○ Disable
Datagram TLS: □ Inherit ● Enable ○ Disable
Ignore Defragmentation(DF) Bit: ☑ Inherit ○ Enable ○ Disable
Ignore Routing and Filtering Rules: ☑ Inherit ○ Enable ○ Disable
Keepalive Messages: ☑ Inherit □ Disable Interval: seconds
MTU: ☑ Inherit
Client Profile to Download: □ Inherit --None--
Optional Client Modules to Download: ☑ Inherit

The default setting is to Inherit DTLS from DfltGrpPolicy.

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

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

Once enabled, DTLS can be activated in group policy or individual user settings. To configure DTLS at the group policy or user level, complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. Choose the policy that you want to edit, and then click the **Edit** button. If you want to activate DTLS for individual users, choose the **Configuration > Remote Access VPN > AAA / Local Users > Local Users** submenu and perform the same action.

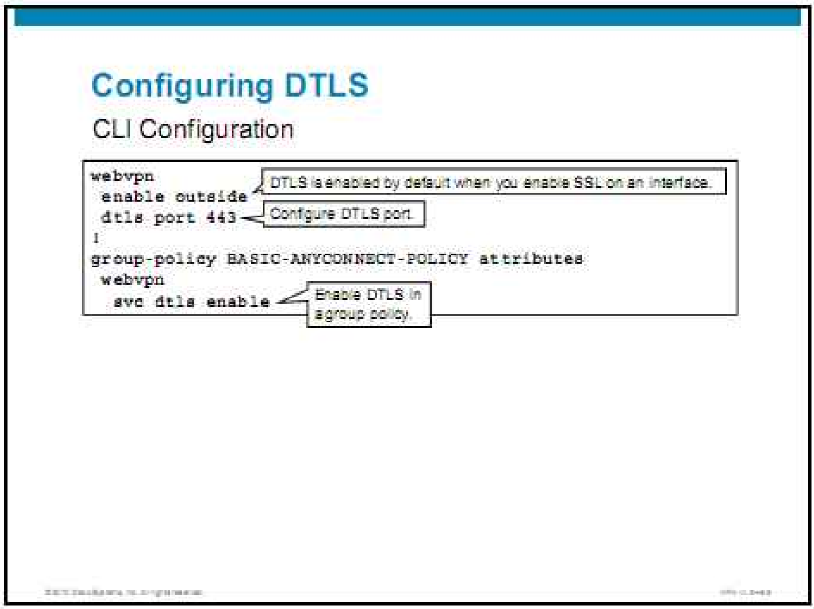
**Step 2** Inside the group policy or user configuration window, choose the **Advanced > SSL VPN Client** submenu, and choose the desired option (**Inherit**, **Enable**, or **Disable**) that is associated with DTLS.

**Note** DTLS is, by default, that is activated in the default group policy (DfltGrpPolicy). By default, all other group policies and users inherit from the DfltGrpPolicy. If you leave the Inherit check box selected, DTLS will effectively be activated for the group or user.

**Step 3** Click **OK**.

**Step 4** Click **Apply** to apply the configuration.

In this figure, DTLS is enabled in the SSL VPN group policy named SalesGroupPolicy.



## Configuring DTLS

CLI Configuration

```
webvpn
 enable outside
 dtls port 443
!
group-policy BASIC-ANYCONNECT-POLICY attributes
 webvpn
  svc dtls enable
```

DTLS is enabled by default when you enable SSL on an interface.

Configure DTLS port.

Enable DTLS in a group policy.

The figure illustrates the DTLS-related command-line interface (CLI) configuration that is applied to the Cisco Adaptive Security Appliance (ASA) adaptive security appliance in this procedure. Use the **dtls port** command in webvpn configuration mode to set the DTLS port number. The default port is 443 and will not be shown in the configuration. In the example, the SSL VPN is enabled on the outside interface, and DTLS is enabled by default. DTLS port is set to port 443.

To enable DTLs in a group policy, enter group-policy configuration mode, then enter webvpn mode and use the **svc dtls enable** command. In the example, DTLS is enabled in the SalesGroupPolicy group policy.

## webvpn

To enter webvpn mode, enter the **webvpn** command in global configuration mode. 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 authentication, authorization, and accounting (AAA) servers, default group policies, default idle timeout, HTTP and HTTPS proxies, and NetBIOS Name Service (NBNS) servers for WebVPN, as well as the appearance of WebVPN screens that end users see.

**webvpn**

## dtls port

To specify a port for DTLS connections, use the **dtls port** command from webvpn configuration mode. To remove the command from the configuration, use the **no** form of this command.

**dtls port** *number*

### dtls port Parameters

| Parameter | Description |
|---|---|
| *number* | The UDP port number, which can range from 1 to 65,535 |

## 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 |
|---|---|
| *name* | 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.

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**

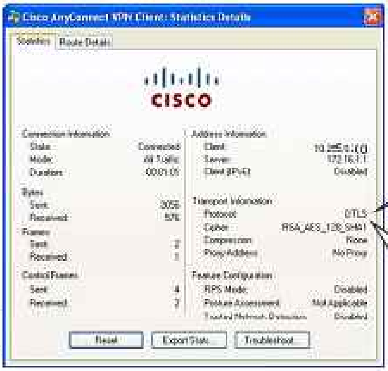
## svc dtls enable

To enable DTLS connections on an interface for specific groups or users who are establishing SSL VPN connections with the Cisco AnyConnect VPN Client, use the **dtls enable** command from group-policy webvpn or username attributes webvpn configuration mode.

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

**svc dtls enable** *interface*

## Verifying DTLS



Cisco AnyConnect VPN Client: Statistics Details

Connection Information
State: Connected
Mode: All Traffic
Duration: 00:01:01

Bytes
Sent: 3056
Received: 576

Frames
Sent: 2
Received: 1

Control Frames
Sent: 4
Received: 7

Address Information
Client: [illegible]
Server: 172.16.1.1
Client (IPv6): Disabled

Transport Information
Protocol: DTLS
Cipher: RSA_AES_128_SHA1
Compression: None
Proxy Address: No Proxy

Feature Configuration
FIPS Mode: Disabled
Posture Assessment: Not Applicable
Trusted Network Detection: Disabled

Primary VPN Protocol

When UDP path is broken, the protocol automatically changes to TLS.

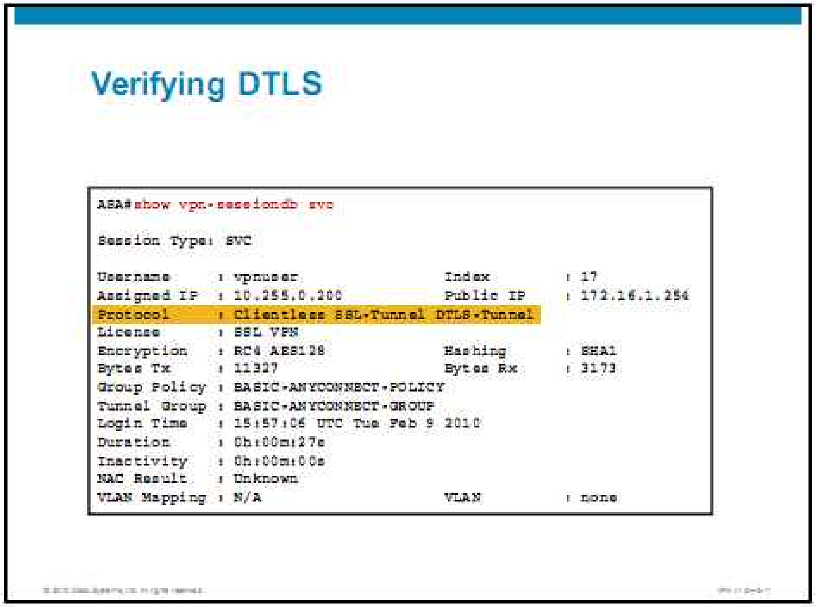
Connection Table on an Intermediate Appliance

```
ASA#show conn
UDP outside 172.16.0.1:443 inside 10.0.1.11:1210, idle 0:00:00, bytes 1292, flags -
TCP outside 172.16.0.1:443 inside 10.0.1.11:1209, idle 0:00:04, bytes 2648, flags UIO
```

In the example, DTLS has been enabled on the outside interface, and the group policy (BASIC-ANYCONNECT-POLICY) that is associated with the user who logged in was configured to have DTLS enabled.

The remote user can examine the selected transport protocol by choosing Statistics and then Details in the Cisco AnyConnect client GUI. The protocol is displays in the Transport Information section.

The **show conn** command output that is displayed is taken from a security appliance that resides in the VPN path. It shows a UDP connection that is established in addition to the SSL session.



## Verifying DTLS

```
ASA#show vpn-sessiondb svc

Session Type: SVC

Username      : vpnuser                    Index        : 17
Assigned IP   : 10.255.0.200               Public IP    : 172.16.1.254
Protocol      : Clientless SSL-Tunnel DTLS-Tunnel
License       : SSL VPN
Encryption    : RC4 AES128                 Hashing      : SHA1
Bytes Tx      : 11327                      Bytes Rx     : 3173
Group Policy  : BASIC-ANYCONNECT-POLICY
Tunnel Group  : BASIC-ANYCONNECT-GROUP
Login Time    : 15:57:06 UTC Tue Feb 9 2010
Duration      : 0h:00m:27s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                        VLAN         : none
```

To verify DTLS, you can use the **show vpn-sessiondb svc** command on the terminating full client SSL session of the security appliance. In the example, you can see that the SSL and DTLS tunnels are used for a connection.

### 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. It also lets you specify the type of sessions to display, and it 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**}]

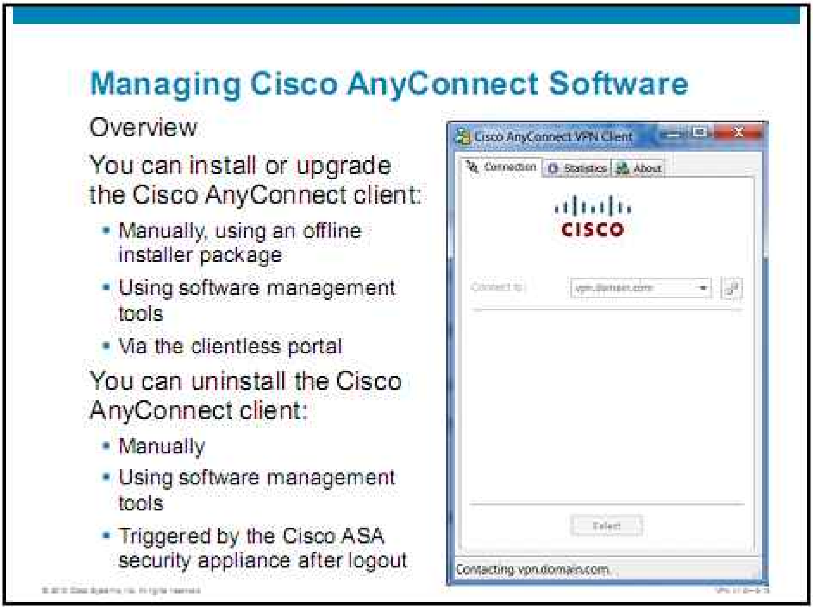
#### show vpn-sessiondb Parameters

| Parameter | Description |
|---|---|
| `detail` | (Optional) Displays extended details about a session. For example, using the **detail** option for an IP Security (IPsec) session displays additional details such as the Internet Key Exchange (IKE) hashing algorithm, authentication mode, and rekey interval.<br>If you choose **detail**, and the **full** option, the Cisco ASA adaptive security appliance displays the detailed output in a machine-readable format. |
| `filter` *`filter_criteria`* | (Optional) Filters the output to display only the information that you specify by using one or more of the filter options. |
| `full` | (Optional) Displays streamed, untruncated output. Output is delineated by horizontal line ("\|") characters and a double horizontal line ("\|\|") string between records. |

| Parameter | Description |
|---|---|
| *session_type* | (Optional) To show data for a specific session type, enter one of the following keywords:<br>■ **email-proxy:** Displays email-proxy sessions.<br>■ **index** *indexnumber*: Displays a single session by index number. Specify the index number for the session, between 1 and 750.<br>■ **l2l:** Displays VPN LAN-to-LAN (L2L) session information.<br>■ **ratio:** Displays VPN session protocol or encryption ratios.<br>■ **remote:** Displays IPsec remote access sessions.<br>■ **summary:** Displays the VPN session summary.<br>■ **svc:** Displays Cisco AnyConnect VPN Client sessions.<br>■ **vpn-lb:** Displays VPN load-balancing management sessions.<br>■ **webvpn:** Displays information about clientless SSL VPN sessions. |
| **sort** *sort_criteria* | (Optional) Sorts the output according to the sort option that you specify. |

# Managing Cisco AnyConnect Software

This topic describes how to manage Cisco AnyConnect software.



## Managing Cisco AnyConnect Software

Overview

You can install or upgrade the Cisco AnyConnect client:

- Manually, using an offline installer package
- Using software management tools
- Via the clientless portal

You can uninstall the Cisco AnyConnect client:

- Manually
- Using software management tools
- Triggered by the Cisco ASA security appliance after logout

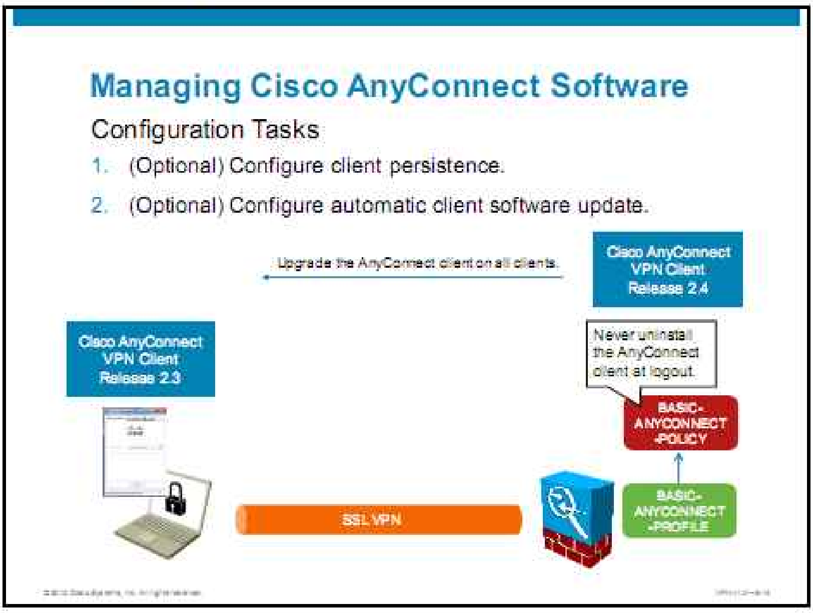
Contacting vpn.domain.com.

Depending on client experience and security policy, the Cisco AnyConnect VPN Client can be distributed and upgraded on workstations using several delivery methods:

- Manually, using an installation package that is downloaded from Cisco.com. This method is best suited for clients with a higher level of experience or for those with slower Internet connections.
- Installation of the Cisco AnyConnect VPN Client over different software management tools is the preferred method of installation in large organizations that have established infrastructure for software package deployment, such as Symantec Altiris or Microsoft Systems Management Server (SMS). Cisco AnyConnect installation is available in .msi format for the Windows platform, .pkg format for Linux and the Mac OS X Intel platform, and .dmg format for the Mac OS platform.
- Installation over the SSL VPN clientless portal can be initiated over the web. If a client has not been previously installed, a remote user can enter into a browser the IP address or Domain Name System (DNS) name of a security appliance interface that is configured to accept clientless SSL VPN connections. The users is then presented with a login screen, and, if the user satisfies the login and authentication, the security appliance identifies the user as requiring the Cisco AnyConnect client. It then uploads the AnyConnect client that matches the operating system of the remote computer. After loading, the Cisco AnyConnect client installs and configures itself and establishes a secure full tunnel SSL connection.

Uninstallation of the Cisco AnyConnect VPN Client can be performed using several methods:

- Manually, using a computer operating system program manager.
- Using software management tools.
- Triggered by the security appliance after logout. The Cisco AnyConnect client that is installed over a web portal can be configured to uninstall automatically after a client logs out from a security appliance.



## Managing Cisco AnyConnect Software

### Configuration Tasks

1. (Optional) Configure client persistence.
2. (Optional) Configure automatic client software update.

Upgrade the AnyConnect client on all clients.
Cisco AnyConnect VPN Client Release 2.4
Cisco AnyConnect VPN Client Release 2.3
Never uninstall the AnyConnect client at logout.
BASIC-ANYCONNECT-POLICY
BASIC-ANYCONNECT-PROFILE
SSL VPN

The following configuration tasks are required to manage the Cisco AnyConnect client:

1. Optionally, configure client persistence.
2. Optionally, configure automatic client software update.

If a client has already been installed, the Cisco ASA adaptive security appliance can be configured to examine the revision of the AnyConnect client with the user authenticates. The client can then upgrade the Cisco AnyConnect client on the remote computer if needed.

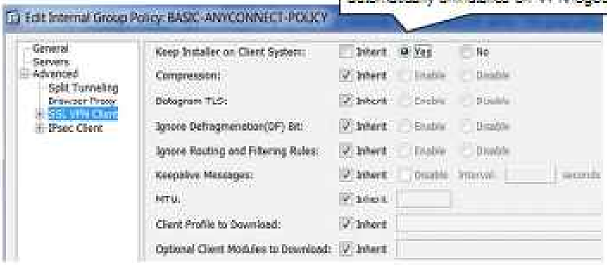
In the configuration scenario, the client that is connected to the Cisco ASA adaptive security appliance is using version 2.3 of the Cisco AnyConnect VPN Client software, but the Cisco ASA adaptive security appliance configuration requires the client to use version 2.4. Therefore, the security appliance will load the latest 2.4 version of the AnyConnect client to the PC. After the 2.4 AnyConnect client install, the software will establish the SSL tunnel to the Cisco ASA adaptive security appliance. After a user logs off, the adaptive security appliance will keep the Cisco AnyConnect client on the client PC.

## Managing Cisco AnyConnect Software

Task 1: (Optional) Configure Client Persistence

```
group-policy BASIC-ANYCONNECT-POLICY attributes
  webvpn
     svc keep-installer installed
```

Specify whether AnyConnect should be automatically uninstalled on VPN logout.



Edit Internal Group Policy: BASIC-ANYCONNECT-POLICY

Keep Installer on Client System: □ Inherit ● Yes ○ No

Compression: ☑ Inherit ○ Enable ○ Disable

Datagram TLS: ☑ Inherit ○ Enable ○ Disable

Ignore Defragmentation(DF) Bit: ☑ Inherit ○ Enable ○ Disable

Ignore Routing and Filtering Rules: ☑ Inherit ○ Enable ○ Disable

Keepalive Messages: ☑ Inherit □ Disable Interval: seconds

MTU: ☑ Inherit

Client Profile to Download: ☑ Inherit

Optional Client Modules to Download: ☑ Inherit

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

Optionally, the Cisco AnyConnect client can be configured in such a way that the client remains installed on a remote computer after client logout.

Using Cisco Adaptive Security Device Manager (ASDM), perform the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access** (not shown in the figure).

**Step 2** Select the group policy that you want to edit, and choose **Edit** (not shown in the figure).

**Step 3** Choose **Advanced > SSL VPN Client**.

**Step 4** Uncheck the **Inherit** check box next to the Keep Installer on Client System field, and choose **Yes** to allow permanent Cisco AnyConnect client installation on the remote computer. By choosing Yes, you disable the automatic uninstalling feature of the AnyConnect client, which allows the software to remain installed on the remote computer for subsequent connections.

**Step 5** Click **OK**, and click **Apply** to apply the changed policy to the security appliance.

Using the CLI, enter group-policy configuration mode using the **group-policy attributes** command. Enter the SSL VPN portion of the group policy configuration using the **webvpn** command, and use the **svc keep-installer installed** command to instruct the Cisco AnyConnect client to remain installed on the remote computer.

### svc keep-installer

To enable the permanent installation of an SSL VPN client on a remote PC, use the **svc keep-installer** command from group-policy webvpn or username webvpn configuration mode.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited.

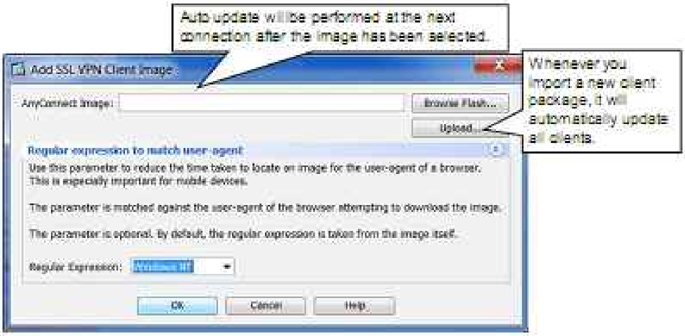
**svc keep-installer** {**installed** | **none**}

### svc keep-installer Parameters

| Parameter | Description |
|---|---|
| `installed` | Disables the automatic uninstalling feature of the client. The client remains installed on the remote PC for future connections. |
| `none` | Specifies that the client uninstalls from the remote computer after the active connection terminates. |

## Managing Cisco AnyConnect Software

Task 2: (Optional) Configure Automatic Client Software Update



Auto update will be performed at the next connection after the image has been selected.

Whenever you import a new client package, it will automatically update all clients.

Regular expression to match user-agent

Use this parameter to reduce the time taken to locate an image for the user-agent of a browser. This is especially important for mobile devices.

The parameter is matched against the user-agent of the browser attempting to download the image.

The parameter is optional. By default, the regular expression is taken from the image itself.

Regular Expression: Windows NT

Configuration > Remote Access VPN > Network (Client)Access > Advanced > SSL VPN > Client Settings

The security appliance can be configured to match a regular expression with a user agent string that is reported by the browser of a remote computer in order to upload the correct Cisco AnyConnect client version.

If a regular expression parameter is not entered, the security appliance will try to match the operating system that is reported in the user agent of the browser with the operating system string that is in the Cisco AnyConnect installation filename.

Using Cisco ASDM, perform the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings** (not shown in the figure).

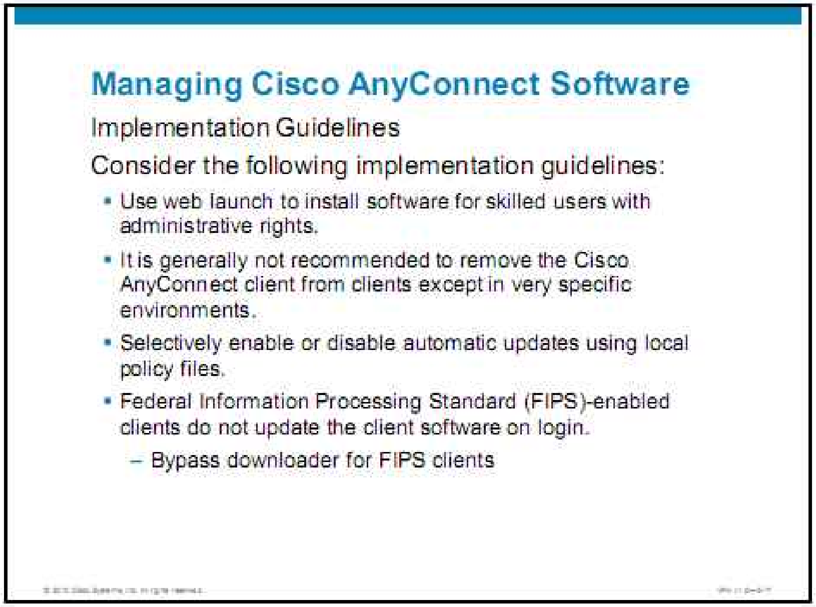
**Step 2** Choose **Add** to add the Cisco AnyConnect client installation image from the flash memory of the Cisco ASA adaptive security appliance (not shown in the figure).

**Step 3** Click **Browse Flash**. Locate the Cisco AnyConnect client installation image and select it. Click **OK**. (This step is not shown in the figure.)

If the file version that is listed here is higher than the one used by the remote computer, the Cisco AnyConnect client will be updated on the remote computer.

**Step 4** Optionally, enter a regular expression to match the user agent of a browser in order to reduce the time that is taken by the security appliance to locate the correct image.

**Step 5** Click **OK**, and click **Apply** to apply the changed policy to the security appliance.



## Managing Cisco AnyConnect Software

Implementation Guidelines

Consider the following implementation guidelines:

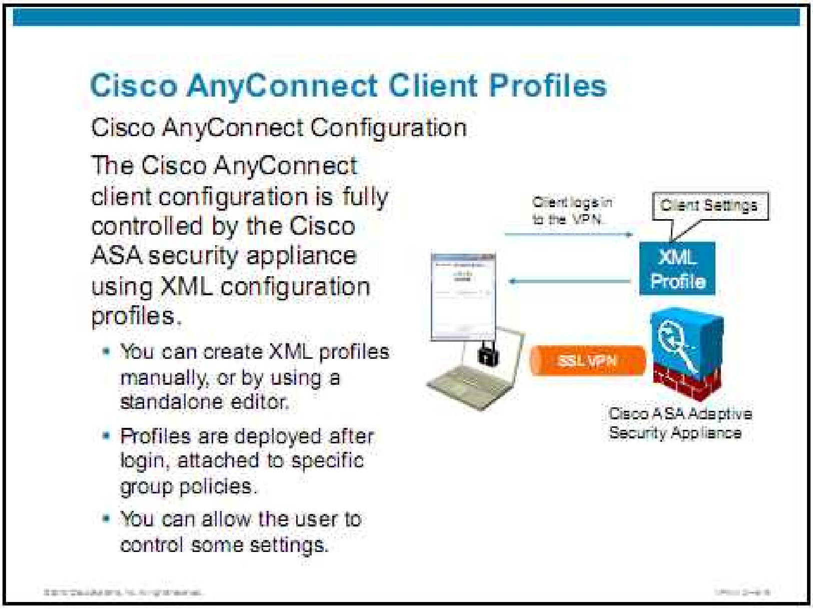
- Use web launch to install software for skilled users with administrative rights.
- It is generally not recommended to remove the Cisco AnyConnect client from clients except in very specific environments.
- Selectively enable or disable automatic updates using local policy files.
- Federal Information Processing Standard (FIPS)-enabled clients do not update the client software on login.
  - Bypass downloader for FIPS clients

When you are managing Cisco AnyConnect software, consider the following implementation guidelines:

- Use the web launch feature to install software for skilled users with administrative rights.
- It is generally not recommended to remove the Cisco AnyConnect client from clients except in very specific environments.
- Selectively enable or disable automatic updates using the Cisco AnyConnect client XML profiles (This topic is addressed later in this lesson).
- Be aware that FIPS-enabled clients do not update the client software on login.

# Configuring Cisco AnyConnect Client Profiles

This topic describes how to configure and verify Cisco AnyConnect client profiles.



## Cisco AnyConnect Client Profiles

Cisco AnyConnect Configuration

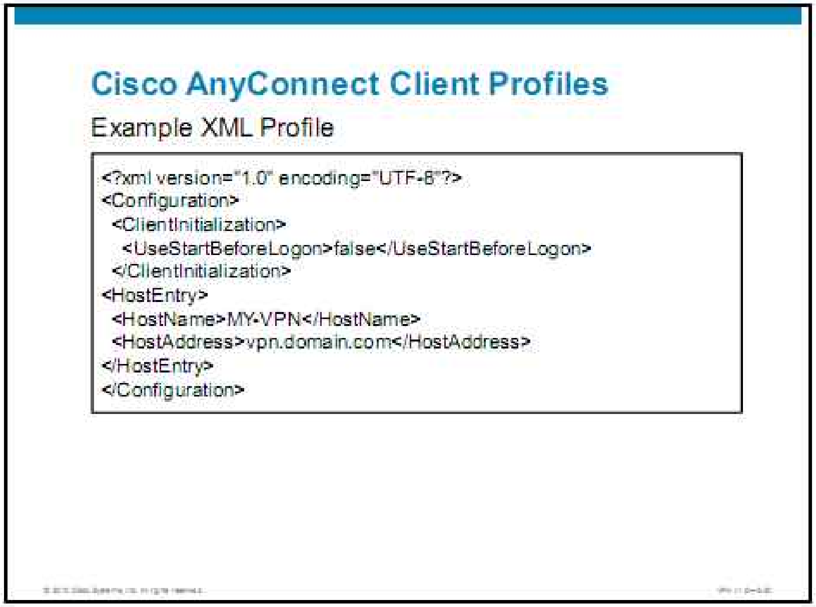
The Cisco AnyConnect client configuration is fully controlled by the Cisco ASA security appliance using XML configuration profiles.

- You can create XML profiles manually, or by using a standalone editor.
- Profiles are deployed after login, attached to specific group policies.
- You can allow the user to control some settings.

Client logs in to the VPN.
Client Settings
XML Profile
SSL VPN
Cisco ASA Adaptive Security Appliance

After the Cisco AnyConnect client connects to the Cisco ASA adaptive security appliance and a user successfully logs in, the AnyConnect client configuration that is defined in the XML configuration profile is uploaded to the remote computer.

XML profiles can be created and edited as regular text files on a computer, or the Cisco AnyConnect Profile Editor can be used. A Java-based standalone program, the Profile Editor can be run on any operating system that has Java software installed on it.



## Cisco AnyConnect Client Profiles

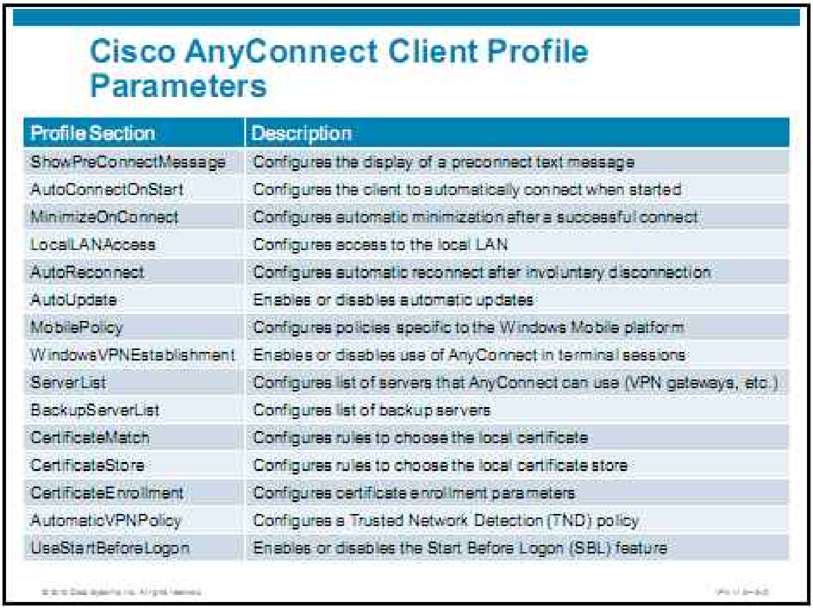
Example XML Profile

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration>
  <ClientInitialization>
    <UseStartBeforeLogon>false</UseStartBeforeLogon>
  </ClientInitialization>
<HostEntry>
  <HostName>MY-VPN</HostName>
  <HostAddress>vpn.domain.com</HostAddress>
</HostEntry>
</Configuration>
```

The Cisco AnyConnect client profile is XML formatted text that contains all configured AnyConnect client parameters. Standard XML format is a collection of beginning and ending tags with configuration values between them.

The recommended procedure is to initially create an XML profile by using the Cisco AnyConnect Profile Editor to correctly define the file structure. Later, you can edit the profile by using the text editor or by again using the Profile Editor.

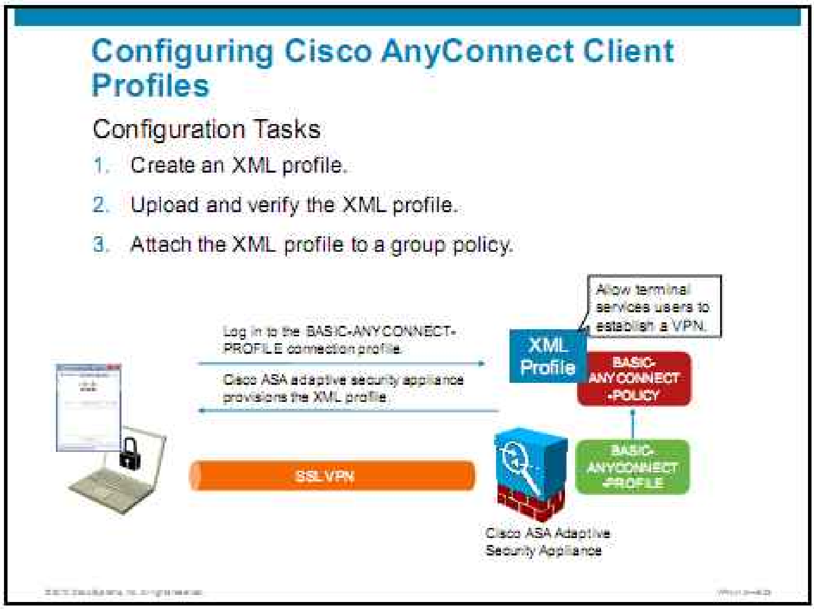
The figure shows a sample XML profile, which specifies the name and address of a VPN gateway.



## Cisco AnyConnect Client Profile Parameters

| Profile Section | Description |
|---|---|
| ShowPreConnectMessage | Configures the display of a preconnect text message |
| AutoConnectOnStart | Configures the client to automatically connect when started |
| MinimizeOnConnect | Configures automatic minimization after a successful connect |
| LocalLANAccess | Configures access to the local LAN |
| AutoReconnect | Configures automatic reconnect after involuntary disconnection |
| AutoUpdate | Enables or disables automatic updates |
| MobilePolicy | Configures policies specific to the Windows Mobile platform |
| WindowsVPNEstablishment | Enables or disables use of AnyConnect in terminal sessions |
| ServerList | Configures list of servers that AnyConnect can use (VPN gateways, etc.) |
| BackupServerList | Configures list of backup servers |
| CertificateMatch | Configures rules to choose the local certificate |
| CertificateStore | Configures rules to choose the local certificate store |
| CertificateEnrollment | Configures certificate enrollment parameters |
| AutomaticVPNPolicy | Configures a Trusted Network Detection (TND) policy |
| UseStartBeforeLogon | Enables or disables the Start Before Logon (SBL) feature |

The table describes the various XML profile settings.



## Configuring Cisco AnyConnect Client Profiles

Configuration Tasks

1. Create an XML profile.
2. Upload and verify the XML profile.
3. Attach the XML profile to a group policy.

Log in to the BASIC-ANYCONNECT-PROFILE connection profile.

Cisco ASA adaptive security appliance provisions the XML profile.

Allow terminal services users to establish a VPN.

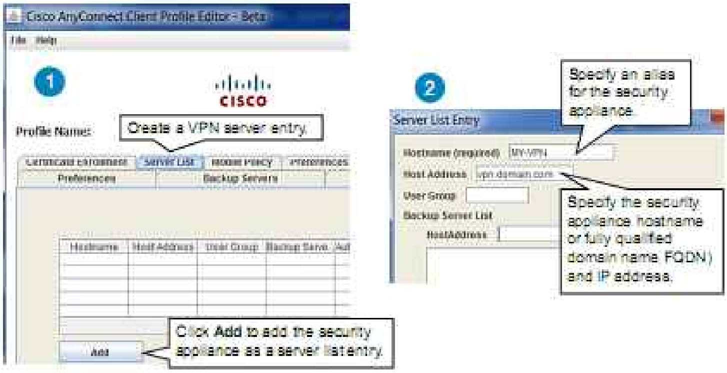
To create and use Cisco AnyConnect client profiles, perform the following configuration tasks:

1. Create an XML profile either by using the Cisco AnyConnect Profile Editor or the text editor on a computer.
2. Upload the XML profile to the security appliance. XML profile verification can be done online using Cisco ASDM or standalone XML verification tools.
3. Attach the uploaded XML profile to a group policy so that it can be uploaded and applied on the remote computers.

In the configuration scenario, after successful SSL VPN connection and user authentication, the group policy named BASIC-ANYCONNECT-POLICY is applied. During the Cisco AnyConnect client deployment, the XML AnyConnect client profile is also deployed. This XML profile will allow terminal services to establish the SSL VPN connection. The XML AnyConnect client profile is provisioned to the remote computer, and the Cisco AnyConnect client is configured accordingly.

## Configuring Cisco AnyConnect Client Profiles

### Task 1: Create an XML Profile



Create a VPN server entry.

Click **Add** to add the security appliance as a server list entry.

Hostname (required): MY-VPN

Host Address: vpn.domain.com

Specify an alias for the security appliance.

Specify the security appliance hostname or fully qualified domain name FQDN) and IP address.

To create the XML profile using the Cisco AnyConnect Profile Editor, follow these steps:

**Step 1** Run the Cisco AnyConnect Profile Editor on a PC.

**Step 2** Choose **File > New** (not shown in the figure).

**Step 3** Choose the **Server List** tab.

**Step 4** Click **Add** to add the security appliance as a server list entry. The client will be connecting to this appliance as a server.

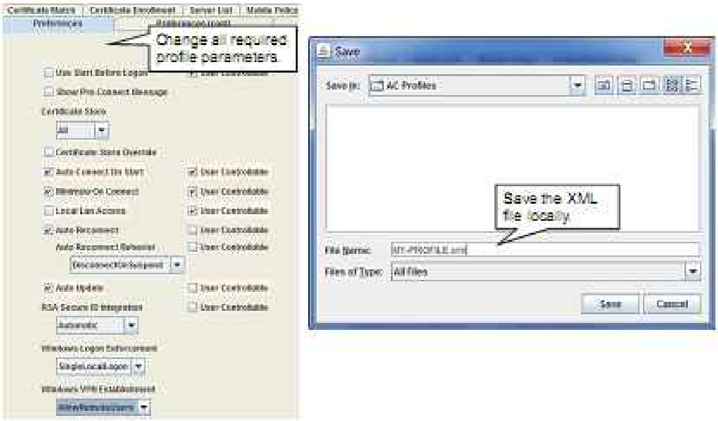
**Step 5** Specify the security appliance name in the **Hostname (Required)** field.

**Step 6** Click **OK**.

**Step 7** Repeat the previous steps for all the security appliances that will be used for terminating the SSL VPNs.

## Configuring Cisco AnyConnect Client Profiles

### Task 1: Create an XML Profile (Cont.)



Change all required profile parameters.

- ☐ Use Start Before Logon ☑ User Controllable
- ☐ Show Pre-Connect Message
- Certificate Store: All
- ☐ Certificate Store Override
- ☑ Auto Connect On Start ☑ User Controllable
- ☑ Minimize On Connect ☑ User Controllable
- ☐ Local Lan Access ☑ User Controllable
- ☑ Auto Reconnect ☐ User Controllable
- Auto Reconnect Behavior: DisconnectOnSuspend ☐ User Controllable
- ☑ Auto Update ☐ User Controllable
- RSA Secure ID Integration: Automatic ☐ User Controllable
- Windows Logon Enforcement: SingleLocalLogon
- Windows VPN Establishment: AllowRemoteUsers

Save in: AC Profiles

File Name: MY-PROFILE.xml

Files of Type: All Files

Save the XML file locally.

To allow terminal services to start a VPN connection, complete the following steps:

**Step 1** Click the **Preferences** tab.

**Step 2** Select **AllowRemoteUsers** from the Windows VPN Establishment drop-down menu.

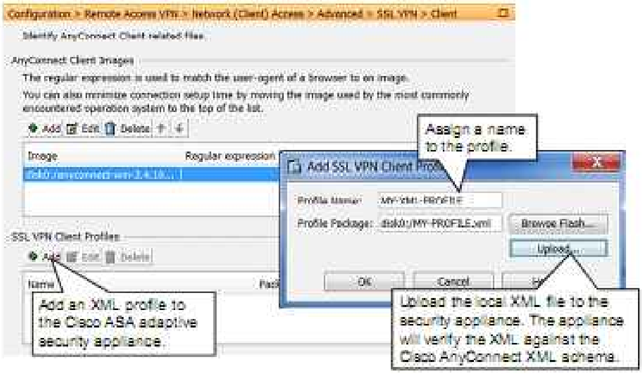
**Step 3** Optionally, change all other required profile parameters.

**Step 4** Choose **File > Save As**.

**Step 5** Save the newly created XML profile locally on the PC.

## Configuring Cisco AnyConnect Client Profiles

### Task 2: Upload and Verify the XML Profile



Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client

Identify AnyConnect Client related files.

AnyConnect Client Images

The regular expression is used to match the user-agent of a browser to an image.

You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Add SSL VPN Client Profile

Profile Name: MY-XML-PROFILE

Profile Package: disk0:/MY-PROFILE.xml

Assign a name to the profile.

Add an XML profile to the Cisco ASA adaptive security appliance.

Upload the local XML file to the security appliance. The appliance will verify the XML against the Cisco AnyConnect XML schema.

Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings

Upload and verify the newly created XML profile using Cisco ASDM by following these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings**.

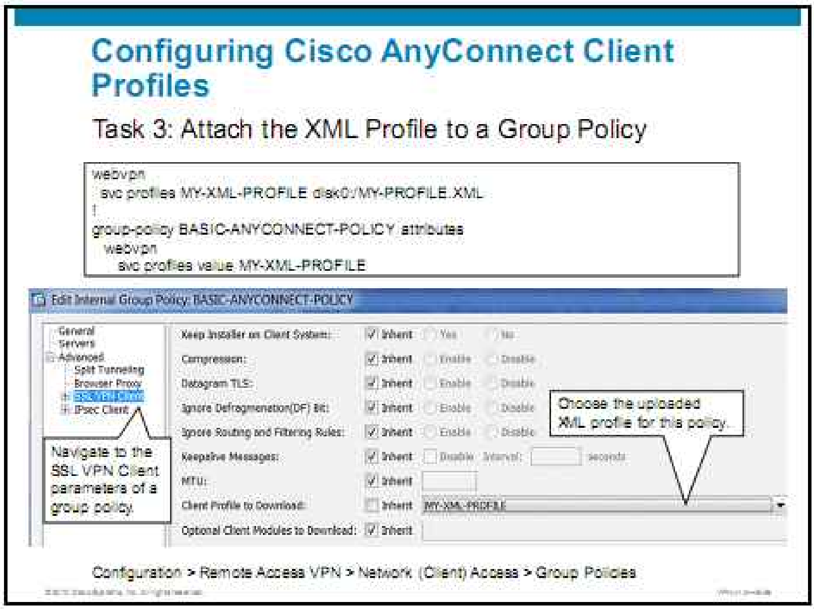
**Step 2** In the SSL VPN Client Profiles section, click **Add** to add the XML profile. The Add SSL VPN Client Profile window displays.

**Step 3** Assign a name to the profile (MY-XML-PROFILE, in the example).

**Step 4** Click the **Browse Flash** button to add an XML file that is already available on the flash memory of the Cisco ASA adaptive security appliance.

**Step 5** If the XML file is not resident in the Cisco ASA adaptive security appliance flash, click **Upload**, and then click **Browse Local Files** to locate the XML file on the PC that is running Cisco ASDM. Once the locally stored XML file is located, click **Upload File** to upload the file to the flash memory of the Cisco ASA adaptive security appliance (not shown in the example).

**Step 6** Click **OK**. The security appliance will verify the XML profile against the Cisco AnyConnect XML schema.



## Configuring Cisco AnyConnect Client Profiles

Task 3: Attach the XML Profile to a Group Policy

```
webvpn
 svc profiles MY-XML-PROFILE disk0:/MY-PROFILE.XML
!
group-policy BASIC-ANYCONNECT-POLICY attributes
  webvpn
    svc profiles value MY-XML-PROFILE
```

Edit Internal Group Policy: BASIC-ANYCONNECT-POLICY

Keep Installer on Client System: ☑ Inherit ○ Yes ○ No
Compression: ☑ Inherit ○ Enable ○ Disable
Datagram TLS: ☑ Inherit ○ Enable ○ Disable
Ignore Defragmentation(DF) Bit: ☑ Inherit ○ Enable ○ Disable
Ignore Routing and Filtering Rules: ☑ Inherit ○ Enable ○ Disable
Keepalive Messages: ☑ Inherit □ Disable Interval: seconds
MTU: ☑ Inherit
Client Profile to Download: □ Inherit MY-XML-PROFILE
Optional Client Modules to Download: ☑ Inherit

Navigate to the SSL VPN Client parameters of a group policy.

Choose the uploaded XML profile for this policy.

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

Attach the XML profile to a group policy using Cisco ASDM by following these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** (not shown in the figure).

**Step 2** Select a group policy in which you want to attach the XML profile, and click **Edit**. The Edit Internal Group Policy window displays.

**Step 3** Choose **SSL VPN Client** and uncheck the **Inherit** box next to the Client Profile to Download field. From the drop-down list, choose the uploaded XML profile to use for this group policy.

**Step 4** Click **OK**, and click **Apply** to save the configuration changes to the security appliance.

Using the CLI, the security appliance can be configured to use the custom XML profile.

Enter the SSL VPN portion of the group policy configuration by using the **webvpn** command. Use the **svc profiles** command to define the name of the XML profile and the location of the XML profile file.

Use the **group-policy attributes** command to edit the group-policy properties and use the **svc profiles value** command to associate the XML profile with the group policy.

### svc profiles (webvpn)

To specify a file as a profiles package that the Cisco ASA 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.

### svc profiles (group-policy and username modes)

To specify a Cisco AnyConnect client profiles package that is downloaded to AnyConnect VPN Client users, use the **svc profile** command from group-policy webvpn or username attributes webvpn configuration mode.

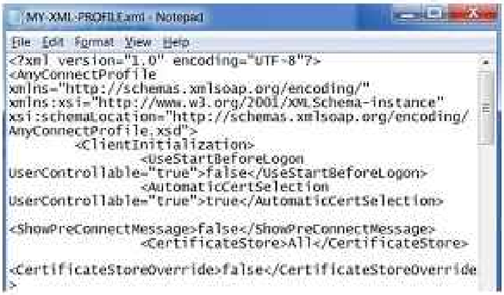
## Verify Cisco AnyConnect Client Profiles

### Client File Verification

Windows XP: C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile

Windows Vista/Windows 7: C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\Profile

Find the XML profile on the client (after the next VPN login).



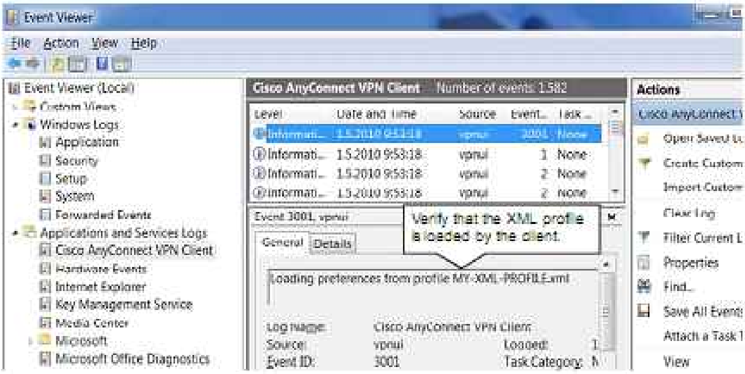
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile
xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
        <ClientInitialization>
                <UseStartBeforeLogon
UserControllable="true">false</UseStartBeforeLogon>
                <AutomaticCertSelection
UserControllable="true">true</AutomaticCertSelection>

<ShowPreConnectMessage>false</ShowPreConnectMessage>
                <CertificateStore>All</CertificateStore>

<CertificateStoreOverride>false</CertificateStoreOverride
>
```

After successful connection and authentication to the SSL VPN, the security appliance uploads the XML profile file to the remote computer.

Correct configuration and successful upload of the XML profile file can be checked by examining the location in which the XML profile file is stored based on the operating system of the client.

## Verify Cisco AnyConnect Client Profiles

Event Viewer Verification



Cisco AnyConnect VPN Client Number of events: 1582

| Level | Date and Time | Source | Event... | Task ... |
|---|---|---|---|---|
| Informati... | 1.5.2010 9:53:18 | vpnui | 3001 | None |
| Informati... | 1.5.2010 9:53:18 | vpnui | 1 | None |
| Informati... | 1.5.2010 9:53:18 | vpnui | 2 | None |
| Informati... | 1.5.2010 9:53:18 | vpnui | 2 | None |

Event 3001, vpnui

Loading preferences from profile MY-XML-PROFILE.xml

Log Name: Cisco AnyConnect VPN Client
Source: vpnui Logged: 1
Event ID: 3001 Task Category: N

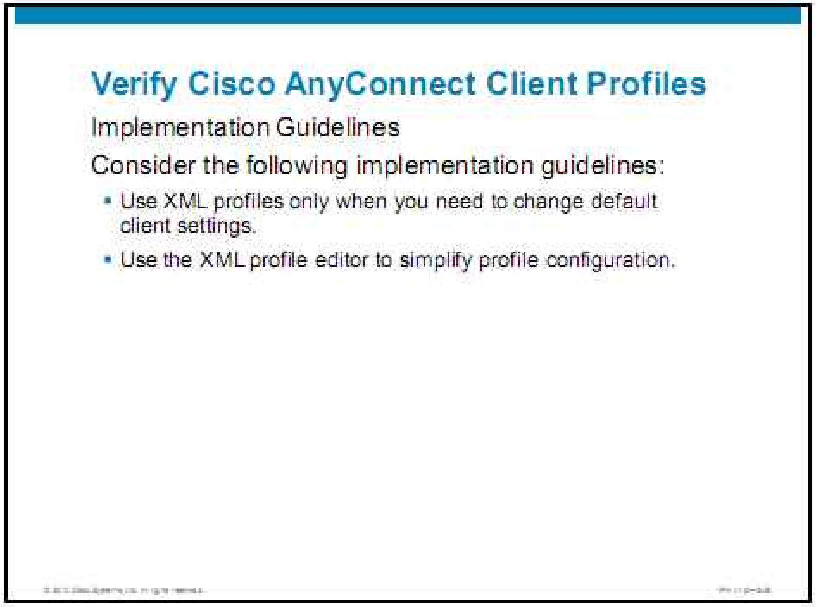
Verify that the XML profile is loaded by the client.

Event Viewer > Applications and Services Logs > Cisco AnyConnect VPN Client

Successful deployment of the XML profile file can also be checked using the Windows Event Viewer application:

**Step 1** In the Event Viewer window, choose **Applications and Services Logs > Cisco AnyConnect VPN Client** (the path may vary depending on the operating system and version).

**Step 2** Verify the XML profile usage by examining event details.



## Verify Cisco AnyConnect Client Profiles

Implementation Guidelines

Consider the following implementation guidelines:

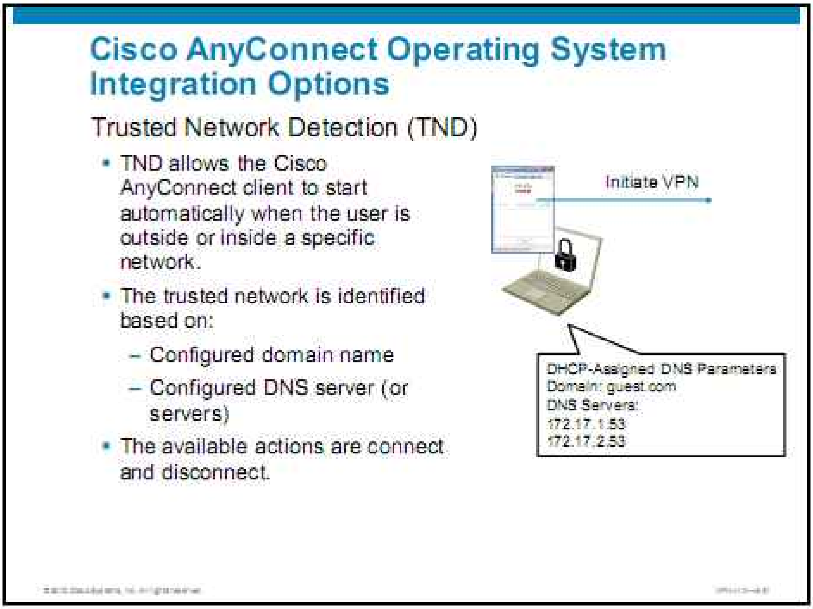
- Use XML profiles only when you need to change default client settings.
- Use the XML profile editor to simplify profile configuration.

The use of XML profiles is not mandatory. You can use them only when you need to change default Cisco AnyConnect client settings or add advanced features.

In order to avoid syntax errors and to simplify profile creation and configuration usage, it is recommended that you use the Cisco AnyConnect Profile Editor.

# Deploying Advanced Cisco AnyConnect Operating System Integration Options

This topic describes how to deploy advanced Cisco AnyConnect operating system integration options.



## Cisco AnyConnect Operating System Integration Options

### Trusted Network Detection (TND)

- TND allows the Cisco AnyConnect client to start automatically when the user is outside or inside a specific network.
- The trusted network is identified based on:
  - Configured domain name
  - Configured DNS server (or servers)
- The available actions are connect and disconnect.

DHCP-Assigned DNS Parameters
Domain: guest.com
DNS Servers:
172.17.1.53
172.17.2.53

Trusted Network Detection (TND) gives you the ability to have the Cisco AnyConnect client automatically disconnect a VPN connection when the user is inside the corporate network (the *trusted* network), and start the VPN connection when the user is outside corporate network (the *untrusted* network). TND does not interfere with the ability of the user to manually establish a VPN connection.

The Cisco AnyConnect client supports TND on Microsoft Windows XP and later, and on Mac OS X.

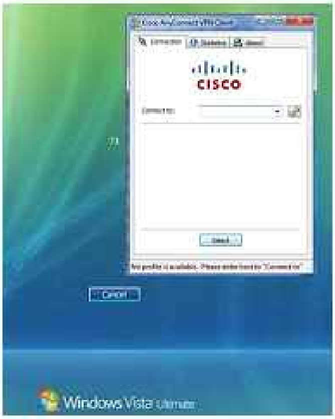
TND is configured in the Cisco AnyConnect profile. No changes are required to the security appliance configuration.

## Cisco AnyConnect Operating System Integration Options

Start Before Login (SBL)

SBL is a Windows-only Cisco AnyConnect feature that allows the client to start before user login to Windows.

- Useful to log in to domains or Microsoft Active Directory over a VPN connection
- Integrates with Windows login interface
- Required to establish VPN if Group Policy Object (GPO) does not allow caching

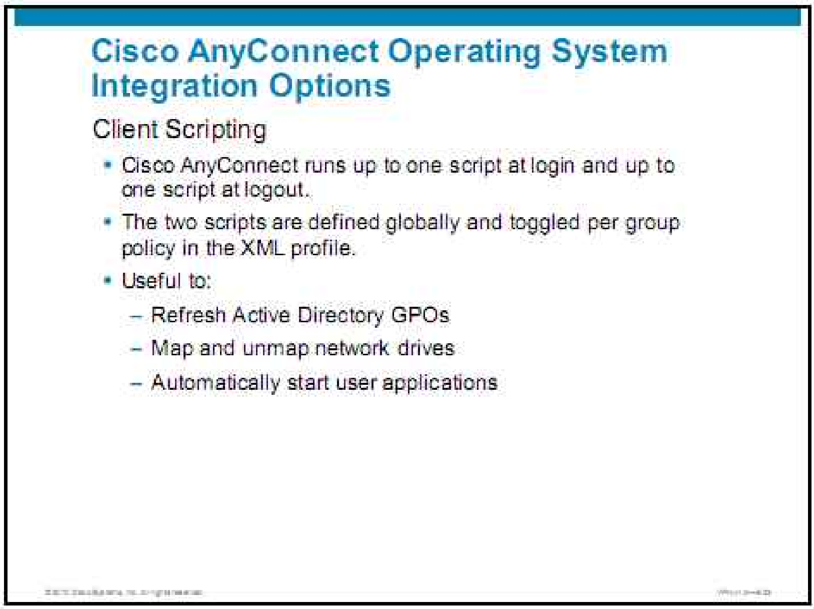


No profile is available. Please enter host to "Connect to"

Start Before Logon (SBL) forces the user to connect to the enterprise infrastructure over a VPN connection before logging into Windows. It accomplishes this forced connection by starting the Cisco AnyConnect client before the Windows login dialog box appears. After authenticating to the security appliance, the user logs in as usual through the Windows login dialog.

SBL is only available for Windows and lets you control the use of login scripts, password caching, network-drive-to-local-drive mapping, and more.

| | |
|---|---|
| **Note** | The Cisco AnyConnect client does not support SBL for Windows XP x64 (64-bit) Edition. |



## Cisco AnyConnect Operating System Integration Options

### Client Scripting

- Cisco AnyConnect runs up to one script at login and up to one script at logout.
- The two scripts are defined globally and toggled per group policy in the XML profile.
- Useful to:
  - Refresh Active Directory GPOs
  - Map and unmap network drives
  - Automatically start user applications

The Cisco AnyConnect client does not require the script to be written in a specific language, but it does require an application that can run the script to be installed on the client computer. Thus, for the Cisco AnyConnect client to launch the script, the script must be capable of running from the command line.

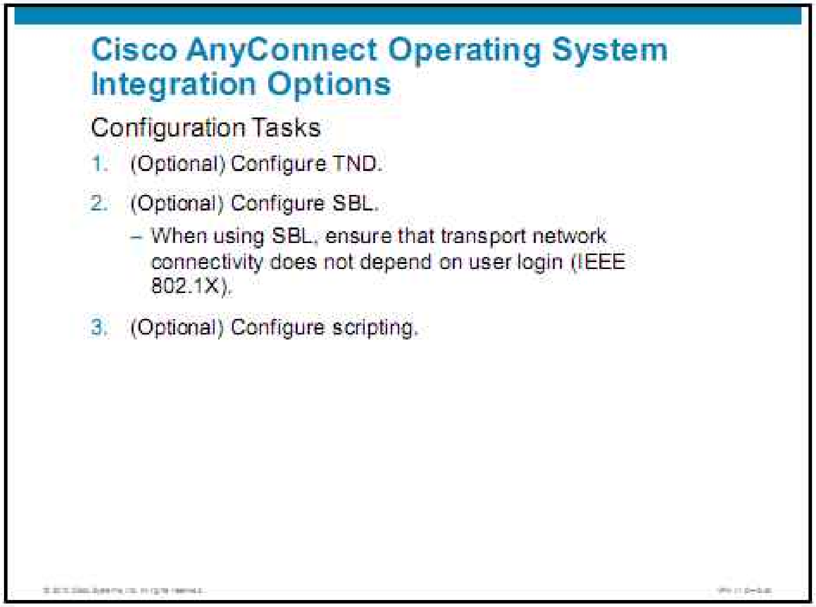
Write and test the script using the operating system type on which it will run when the AnyConnect client launches it.

**Note** You should write and test the script on the targeted operating system. If a script cannot run properly from the command line on the native operating system, the Cisco AnyConnect client cannot run it properly either.

The Cisco AnyConnect client supports script launching on all Microsoft Windows, Mac OS X, and Linux platforms that accommodate the AnyConnect software.

On Microsoft Windows, Cisco AnyConnect can only launch scripts after the user logs into Windows and establishes a VPN session. Thus, the restrictions that are imposed by the security environment of the user apply to these scripts. Scripts can only execute functions that the user has rights to invoke. Cisco AnyConnect hides the command window during the execution of a script on Windows, so executing a script to display a message in a .bat file for testing purposes does not work.

On Linux-based operating systems, assign execute permissions to the script files for user, group, and other.



## Cisco AnyConnect Operating System Integration Options

Configuration Tasks

1. (Optional) Configure TND.
2. (Optional) Configure SBL.
   - When using SBL, ensure that transport network connectivity does not depend on user login (IEEE 802.1X).
3. (Optional) Configure scripting.

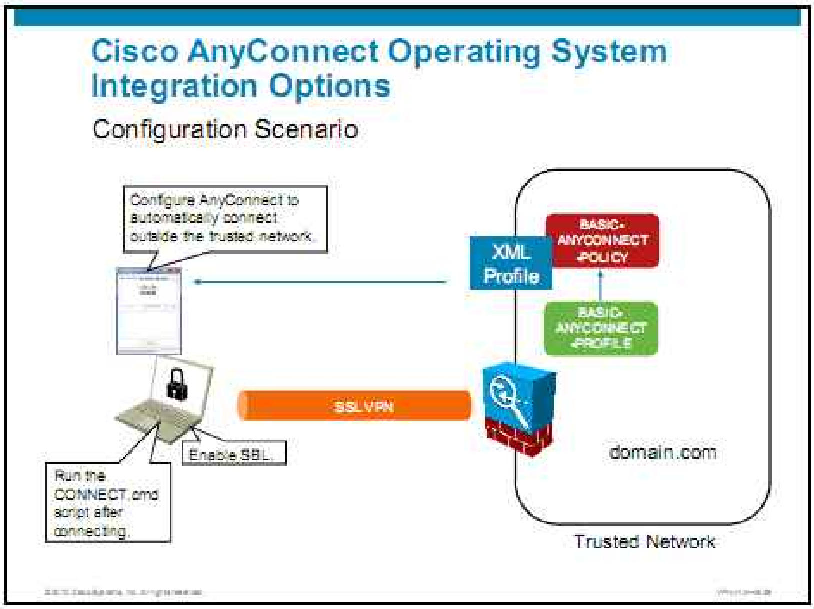
To configure Cisco AnyConnect advanced operating system integration options, perform the following tasks:

1. Configure the TND feature if you need automatic SSL VPN connection for remote computers when they are connected to an untrusted network.

2. Configure the SBL feature when SSL VPN connectivity is needed before the Microsoft login procedure.

**Note** When using SBL, ensure that the transport network connectivity does not depend on user login (IEEE 802.1X).

3. Configure scripting if you need to execute commands after the SSL VPN is successfully connected or when the SSL VPN tunnel connection is terminated.



## Cisco AnyConnect Operating System Integration Options

Configuration Scenario

Configure AnyConnect to automatically connect outside the trusted network.

Enable SBL.

Run the CONNECT.cmd script after connecting.

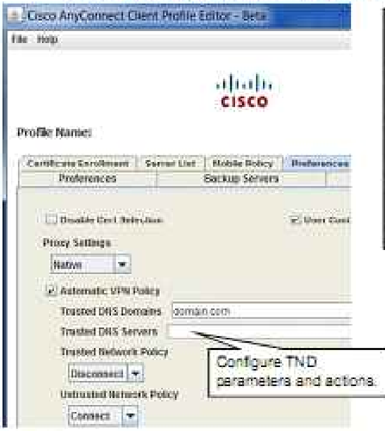
Configuration of all three Cisco AnyConnect client features is included in the XML profile. In the example, you will configure Trusted Network Detection (TND) and Start Before Login (SBL), and you will enable scripting to run the CONNECT.cmd script.

After successful user authentication, the XML profile is parsed for those configurations. If the security appliance has a newer version of scripts than those stored on remote computers, then those scripts are replaced and a new version of scripts is executed.

Also, TND and SBL configuration are refreshed on remote computers.

## Cisco AnyConnect Operating System Integration Options

### Task 1: (Optional) Configure TND



Profile Name:

Preferences

□ Disable Cert Selection

☑ User Cont

Proxy Settings: Native

☑ Automatic VPN Policy

Trusted DNS Domains: domain.com

Trusted DNS Servers:

Trusted Network Policy: Disconnect

Untrusted Network Policy: Connect

Configure TND parameters and actions.

```
<ClientInitialization>
...
<AutomaticVPNPolicy>true
<TrustedDNSDomains>domain.com
</TrustedDNSDomains>
<TrustedNetworkPolicy>Disconnect
</TrustedNetworkPolicy>
<UntrustedNetworkPolicy>Connect<
/UntrustedNetworkPolicy>
</AutomaticVPNPolicy>
...
</ClientInitialization>
```

TND is configured in the Cisco AnyConnect XML profile. No changes are required to the security appliance configuration except uploading of the changed XML profile.

To configure the XML profile using the Cisco AnyConnect Profile Editor to enable TND, follow these steps:

**Step 1** Choose the **Preferences** tab.

**Step 2** Enable TND by checking the **Automatic VPN Policy** check box.

**Step 3** In the Trusted DNS Domains field, enter a list of DNS suffixes (a string that is separated by commas) that a network interface may have when the client is in the trusted network. In the example, **domain.com** is the trusted domain.

**Step 4** In the Trusted DNS Servers field, enter a list of DNS server addresses (a string that is separated by commas) that a network interface may have when the client is in the trusted network.

**Note** If you configure both the Trusted DNS Domain and Trusted DNS Servers fields, users must match both settings in order to be included in the trusted network.

**Step 5** Select a network policy in the trusted network. In the example, when the client is connected to the trusted network, the network policy is configured to disconnect the Cisco AnyConnect client.

**Step 6** Select a network policy outside the trusted network. In the example, when the client is connected to the untrusted network, the network policy is configured to connect the Cisco AnyConnect client.

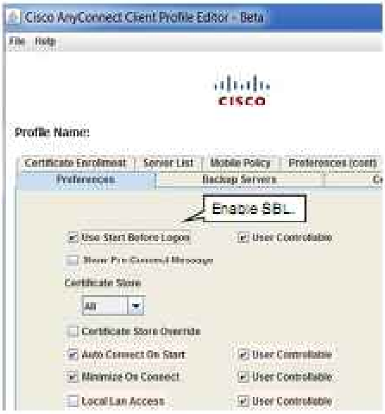
**Step 7** Choose **File > Save (Save As)** to save changes in policy.

The following example shows the *ClientInitialization* section of the profile file with TND configured. The output reflects the configuration for automatic connection to the VPN when the client is in the untrusted network, and automatic disconnection when it is in trusted network:

```
<AutomaticVPNPolicy>true
<TrustedDNSDomains>*.cisco.com</TrustedDNSDomains>
<TrustedDNSServers>161.44.124.*,64.102.6.247</TrustedDNSServer
s>
<TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
<UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
</AutomaticVPNPolicy>
```

## Cisco AnyConnect Operating System Integration Options

### Task 2: (Optional) Configure SBL


Cisco AnyConnect Client Profile Editor - Beta

☑ Use Start Before Logon ☑ User Controllable

□ Show Pre-Connect Message

Certificate Store: All

□ Certificate Store Override

☑ Auto Connect On Start ☑ User Controllable

☑ Minimize On Connect ☑ User Controllable

□ Local Lan Access ☑ User Controllable

```
<ClientInitialization>
...
<UseStartBeforeLogon
UserControllable="true">true
</UseStartBeforeLogon>
...
</ClientInitialization>
```

SBL is configured in the Cisco AnyConnect XML profile. To enable SBL, you must first specify the SBL module name in a group policy on the Cisco ASA security appliance.

To specify SBL module name, follow these steps using Cisco ASDM:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** (not shown in the figure).

**Step 2** Select a group policy and click **Edit**. The Edit Internal Group Policy window displays (not shown in the figure).

**Step 3** Choose **Advanced > SSL VPN Client** in the navigation pane on the left. The SSL VPN settings window displays (not shown in the figure).

**Step 4** Uncheck the **Inherit** check box for the Optional Client Modules for Download setting (not shown in the figure).

**Step 5** Enable the Start Before Logon (SBL) feature by checking the **vpngina** check box. This selection enables the security appliance to download a Graphical Identification and Authentication (GINA) for the Cisco AnyConnect client VPN connection (not shown in the figure).

**Step 6** Click **OK**, and click **Apply** to save the configuration changes to the Cisco ASA adaptive security appliance.

The XML profile configuration has to be changed and uploaded to the security appliance.

To configure the XML profile using the Cisco AnyConnect Profile Editor to enable SBL, follow these steps:

**Step 1** Choose the **Preferences** tab.

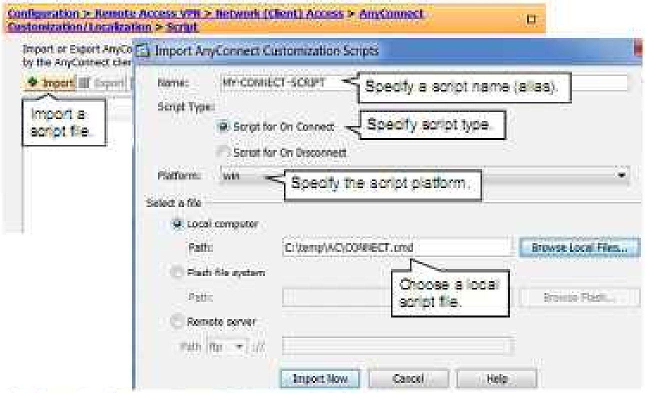
**Step 2** Enable SBL by checking the **Use Start Before Logon** check box.

**Step 3** Choose **File > Save (Save As)** to save the changes in policy.

**Note** The user must reboot the remote computer before SBL can take effect.

## Cisco AnyConnect Operating System Integration Options

### Task 3: (Optional) Configure Scripting



Name: MY-CONNECT-SCRIPT

Script Type:
● Script for On Connect
○ Script for On Disconnect

Platform: win

Select a file
● Local computer
Path: C:\temp\AC\CONNECT.cmd

Import a script file.

Specify a script name (alias).

Specify script type.

Specify the script platform.

Choose a local script file.

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Script

To enable scripting, follow these steps using Cisco ASDM:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Script**.

**Step 2** Click **Import**.

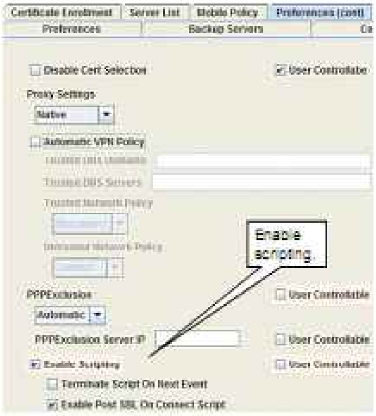
**Step 3** Specify the script name and script type. Then, select the remote computer operating platform for which the script is written.

**Step 4** Select the script file by filling in the path information.

**Step 5** Select **Import Now** to upload the script to the security appliance.

## Cisco AnyConnect Operating System Integration Options

### Task 3: (Optional) Configure Scripting (Cont.)



□ Disable Cert Selection ☑ User Controllable

Proxy Settings: Native

□ Automatic VPN Policy

Trusted DNS Domains

Trusted DNS Servers

Trusted Network Policy

Untrusted Network Policy

PPPExclusion: Automatic □ User Controllable

PPPExclusion Server IP □ User Controllable

☑ Enable Scripting □ User Controllable

□ Terminate Script On Next Event

☑ Enable Post SBL On Connect Script

```
<ClientInitialization>
...
<EnableScripting
UserControllable="false">true
<TerminateScriptOnNextEvent>false
</TerminateScriptOnNextEvent>
<EnablePostSBLOnConnectScript>true
</EnablePostSBLOnConnectScript>
</EnableScripting>
...
</ClientInitialization>
```

After the script is uploaded to the security appliance, the XML profile has to be changed in order to execute the scripts.

To configure the XML profile by using the Cisco AnyConnect Profile Editor to enable scripting, follow these steps:

**Step 1** Choose the **Preferences (Cont)** tab.

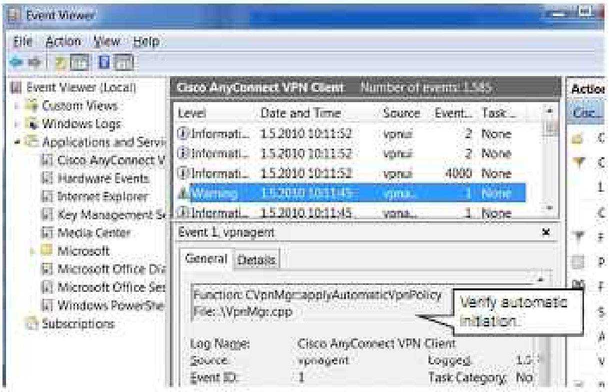
**Step 2** Enable scripting by checking the **Enable Scripting** check box.

**Step 3** Choose **File > Save (Save As)** to save the changes in policy.

**Step 4** Upload the XML profile file to the Cisco ASA adaptive security appliance as described in the previous topic.

## Verifying Cisco AnyConnect Operating System Integration

### Trusted Network Detection



Cisco AnyConnect VPN Client Number of events: 1,585

| Level | Date and Time | Source | Event... | Task ... |
|---|---|---|---|---|
| Informati... | 1.5.2010 10:11:52 | vpnui | 2 | None |
| Informati... | 1.5.2010 10:11:52 | vpnui | 2 | None |
| Informati... | 1.5.2010 10:11:52 | vpnui | 4000 | None |
| Warning | 1.5.2010 10:11:45 | vpna... | 1 | None |
| Informati... | 1.5.2010 10:11:45 | vpna... | 1 | None |

Event 1, vpnagent

General Details

Function: CVpnMgr::applyAutomaticVpnPolicy
File: .\VpnMgr.cpp

Log Name: Cisco AnyConnect VPN Client
Source: vpnagent Logged: 1.5.
Event ID: 1 Task Category: No

Verify automatic initiation.

Event Viewer > Applications and Services > Cisco AnyConnect VPN Client

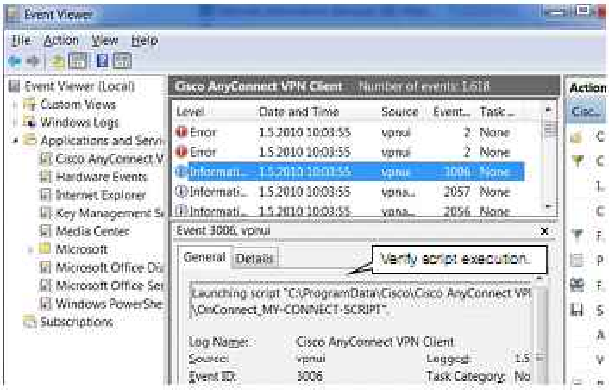
To verify TND on Windows operating systems, use the Event Viewer.

**Step 1** In the Event Viewer window, choose **Applications and Services Logs > Cisco AnyConnect VPN Client** (the path may vary based on the operating system and version).

**Step 2** Verify that the Cisco AnyConnect client will automatically initiate when a remote computer is in an untrusted network. If TND action is also configured for a trusted network, a separate event in Event Viewer verification should be recorded.

## Verifying Cisco AnyConnect Operating System Integration

### Scripting



Cisco AnyConnect VPN Client   Number of events: 1,618

| Level | Date and Time | Source | Event... | Task ... |
|---|---|---|---|---|
| Error | 1.5.2010 10:03:55 | vpnui | 2 | None |
| Error | 1.5.2010 10:03:55 | vpnui | 2 | None |
| Informati... | 1.5.2010 10:03:55 | vpnui | 3006 | None |
| Informati... | 1.5.2010 10:03:55 | vpna... | 2057 | None |
| Informati... | 1.5.2010 10:03:55 | vpna... | 2056 | None |

Event 3006, vpnui

Launching script "C:\ProgramData\Cisco\Cisco AnyConnect VPI \OnConnect_MY-CONNECT-SCRIPT".

| | | | |
|---|---|---|---|
| Log Name: | Cisco AnyConnect VPN Client | | |
| Source: | vpnui | Logged: | 1.5 |
| Event ID: | 3006 | Task Category: | No |

Verify script execution.

Event Viewer > Applications and Services > Cisco AnyConnect VPN Client

You can also use the Event Viewer to verify scripting on Windows operating systems.

**Step 1** In the Event Viewer window, choose **Applications and Services Logs > Cisco AnyConnect VPN Client** (the path may vary based on the operating system and version).

**Step 2** Verify that the Cisco AnyConnect client will automatically execute scripting after VPN connection. If scripting is also enabled upon VPN disconnection, a separate event in the Event Viewer should be created upon VPN disconnection.

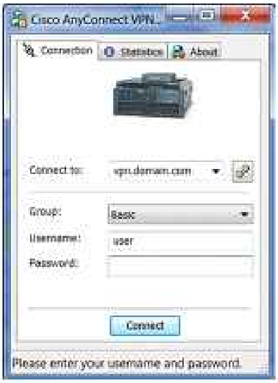
# Customizing the Cisco AnyConnect User Interface

This topic describes how to configure and verify Cisco AnyConnect user interface customization.

## Customizing Cisco AnyConnect User Interface

### Overview

- You can fully customize the Cisco AnyConnect client GUI.
  - Graphical elements (bitmaps, icons)
  - Language strings
- Most customization tasks are easily performed using the Cisco ASDM.
- For more extensive customization, replace the VPN GUI entirely and deploy a custom GUI application integrated with Cisco AnyConnect API.



Connect to: vpn.domain.com

Group: Basic

Username: user

Password:

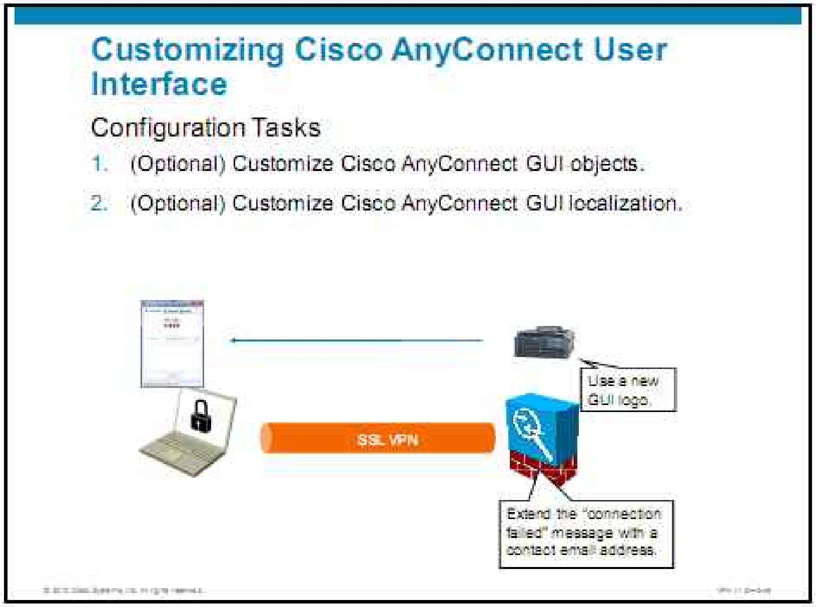
Please enter your username and password.

You can customize the Cisco AnyConnect client GUI elements and language strings; for example, you can configure it to display your own corporate image to remote users.

Customization can be performed on the Cisco AnyConnect client that runs on Windows, Linux, and Mac OS X computers. Customization is not supported for the Cisco AnyConnect client that runs on a Windows Mobile device.

You can use one of three methods to customize the client:

- Import individual client GUI and string components, such as the corporate logo, to the security appliance that deploys them to remote computers with the installer
- Import your own programs (Windows and Linux platforms only) that provide their own GUI or CLI and use the Cisco AnyConnect application programming interface (API)
- Import a transform (Windows only) that you create, and enable the security appliance to deploy it with an installer



## Customizing Cisco AnyConnect User Interface

### Configuration Tasks

1. (Optional) Customize Cisco AnyConnect GUI objects.
2. (Optional) Customize Cisco AnyConnect GUI localization.

SSL VPN
Use a new GUI logo.
Extend the "connection failed" message with a contact email address.

Both the GUI and string components of the Cisco AnyConnect client can be replaced by customized versions. Most of customization tasks are easily performed using Cisco ASDM.

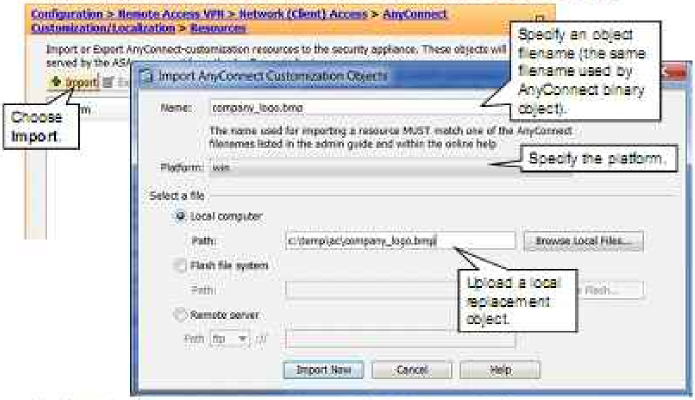
In this configuration scenario, you will change the Cisco AnyConnect GUI client logo and modify one of status messages.

GUI customization can be performed on all graphical elements and icons that the Cisco AnyConnect client GUI contains. If you create your own custom images to replace the Cisco AnyConnect client icons, your images must be the same size as the original Cisco images. In addition, filenames must be the same to those used by Cisco. The Cisco AnyConnect client uses different filenames for different operating systems.

Default AnyConnect client English messages can also be customized and, if needed, translated into other languages.

## Customizing Cisco AnyConnect User Interface

Task 1: (Optional) Customize Cisco AnyConnect GUI Objects



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Resources

Import or Export AnyConnect-customization resources to the security appliance. These objects will served by the ASA

Import AnyConnect Customization Objects

Name: company_logo.bmp

The name used for importing a resource MUST match one of the AnyConnect filenames listed in the admin guide and within the online help

Platform: win

Select a file

● Local computer

Path: c:\temp\ac\company_logo.bmp

○ Flash file system

○ Remote server

Path: ftp ://

Choose **Import**.

Specify an object filename (the same filename used by AnyConnect binary object).

Specify the platform.

Upload a local replacement object.

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Resources

To customize the client GUI by importing a new company logo, follow these steps using Cisco ASDM:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Resources**.

**Step 2** Click **Import**.

**Step 3** Enter the name of the file to import.

**Step 4** Select an operating system platform and specify the file to import. Your custom objects have to be the same size and use the same names as those objects that are used by default by the Cisco AnyConnect VPN client. You can find object names and sizes for all operating systems in the tables that follow.

**Step 5** Click **Import Now**. The file appears in the table.

**Step 6** Repeat Steps 2 through 5 for all the files that you want to import to the Cisco ASA adaptive security appliance.

**Step 7** Click **Apply** to apply the configuration changes to the security appliance.

The following tables list the files that you can replace for each operating system that supports the Cisco AnyConnect client.

**Note** If you create your own custom images to replace the client icons, your images must be the same size as the original Cisco images.

# Microsoft Windows

All files for Windows are located in the %PROGRAMFILES%\Cisco\Cisco AnyConnect VPN Client\res\ folder.

**Note** The %PROGRAMFILES% name refers to the environment variable by the same name. In most Windows installations, this is the C:\Program Files environment.

### Microsoft Windows Files

| Filename in Microsoft Windows Installation | Client GUI Area Affected | Image Size (Pixels, L x H) |
|---|---|---|
| AboutTab.ico | Icon that appears on the About tab | 16 x 16 |
| company_logo.bmp | Corporate logo that appears on each tab of the user interface | 142 x 92 |
| connected.ico | Tray icon that displays when the client is connected | 16 x 16 |
| ConnectionTab.ico | Icon that appears on the Connection tab | 16 x 16 |
| disconnecting.ico | Tray icon that displays when the client is in the process of disconnecting | 16 x 16 |
| GUI.ico | Icon that appears on the Windows Vista SBL screen | 48 x 48<br>32 x 32<br>24 x 24<br>16 x 16 |
| reconnecting.ico | Tray icon that displays when the client is in the process of reconnecting | 16 x 16 |
| StatsTab.ico | Icon that appears on the Statistics tab | 16 x 16 |
| unconnected.ico | Tray icon that displays when the client is not connected | 16 x 16 |

# Linux

All files for Linux are located in the /opt/cisco/vpn/pixmaps/ folder.

### Linux Files

| Filename in Linux Installation | Client GUI Area Affected | Image Size (Pixels, L x H) |
|---|---|---|
| company-logo.png | Corporate logo that appears on each tab of the user interface | 142 x 92 |
| cvc-about.png | Icon that appears on the About tab | 16 x 16 |
| cvc-connect.png | Icon that appears next to the Connect button, and on the Connection tab | 16 x 16 |
| cvc-disconnect.png | Icon that appears next to the Disconnect button | 16 x 16 |
| cvc-info.png | Icon that appears on the Statistics tab | 16 x 16 |
| systray_connected.png | Tray icon that displays when the client is connected | 16 x 16 |
| systray_notconnected.png | Tray icon that displays when the client is not connected | 16 x 16 |
| systray_disconnecting.png | Tray icon that displays when the client is disconnecting | 16 x 16 |
| systray_reconnecting.png | Tray icon that displays when the client is reconnecting | 16 x 16 |
| vpnui48.png | Main program icon | 48 x 48 |

## Mac OS X

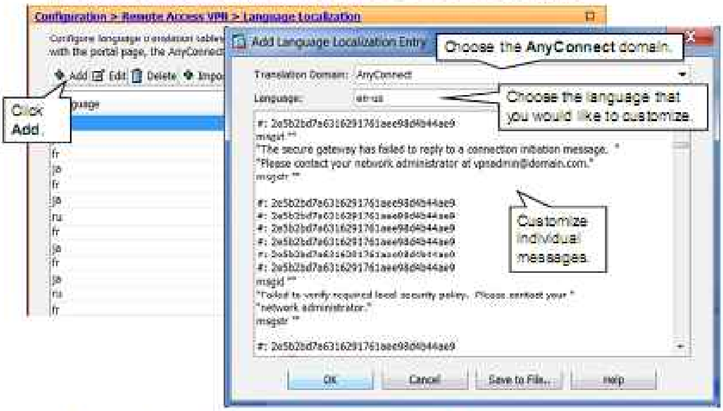
All files for Mac OS X are located in the /Applications/Cisco AnyConnect VPN Client/Contents/Resources folder.

### Mac OS X Files

| Filename in Mac OS X Installation | Client GUI Area Affected | Image Size (Pixels, L x H) |
|---|---|---|
| bubble.png | Notification bubble that appears when the client connects or disconnects | 142 x 92 |
| connected.png | Icon that displays under the disconnect button when the client is connected | 32 x 32 |
| logo.png | Logo icon that appears on main screen in the top right corner | 50 x 33 |
| menu_connected.png | Connected state menu bar icon | 16 x 16 |
| menu_error.png | Error state menu bar icon | 16 x 16 |
| menu_idle.png | Disconnected idle menu bar icon | 16 x 16 |
| menu_reconnecting.png | Reconnection in process menu bar icon | 16 x 16 |
| warning.png | Icon that replaces login fields on various authentication and certificate warnings | 40 x 40 |
| vpngui.icns | Mac OS X icon file format that is used for all icon services, such as Dock, Sheets, and Finder | 128 x 128 |

## Customizing Cisco AnyConnect User Interface

### Task 2: (Optional) Customize GUI Localization



Configuration > Remote Access VPN > Language Localization

Configure language translation tables ... with the portal page, the AnyConnect ...

Add Language Localization Entry

Translation Domain: AnyConnect

Language: en-us

```
#: 2e5b2bd7a6316291761aee98d4b44ae9
msgid ""
"The secure gateway has failed to reply to a connection initiation message. "
"Please contact your network administrator at vpnadmin@domain.com."
msgstr ""

#: 2e5b2bd7a6316291761aee98d4b44ae9
#: 2e5b2bd7a6316291761aee98d4b44ae9
#: 2e5b2bd7a6316291761aee98d4b44ae9
#: 2e5b2bd7a6316291761aee98d4b44ae9
#: 2e5b2bd7a6316291761aee98d4b44ae9
#: 2e5b2bd7a6316291761aee98d4b44ae9
msgid ""
"Failed to verify required local security policy.  Please contact your "
"network administrator."
msgstr ""

#: 2e5b2bd7a6316291761aee98d4b44ae9
```

Click **Add**.

Choose the **AnyConnect** domain.

Choose the language that you would like to customize.

Customize individual messages.

Configuration > Remote Access VPN > Language Localization

You can make changes to the English messages displayed on the Cisco AnyConnect client GUI by adding an English translation table and by changing message text within an editing window of Cisco ASDM.

The following procedure describes how to change the default English messages using Cisco ASDM:

**Step 1** Choose **Configuration > Remote Access VPN > Language Localization**.

**Step 2** **Click Add.**

**Step 3** **The Add Language Localization Entry window appears. Choose AnyConnect as the translation domain from** the Translation Domain drop-down menu.

**Step 4** Click the Language drop-down menu, choose **En-US** for English.

**Step 5** To customize messages, edit each message separately. Text between the quotes in a line beginning with the string *msgid* is, by default, English text and must not be changed. A customized string must be entered between the quotes in a line beginning with the string *msgstr*. Enter all custom string in corresponding lines.

**Step 6** Click **OK**, and click **Apply** to save the configuration changes to the security appliance.

For Windows, Linux, or Mac computers, you can deploy your own client that uses the Cisco AnyConnect client API. You can replace the Cisco AnyConnect GUI or the Cisco AnyConnect CLI by replacing the client binary file.

Your executable can call any resource files, such as logo images, that you import to the security appliance. When you deploy your own executable, any filename can be used for your resource files.

Executable filenames must be exact for each operating system.

### Executable Filenames

| Client Operating System | Client GUI Filename | Client CLI Filename |
|---|---|---|
| Microsoft Windows | vpnui.exe | vpncli.exe |
| Linux | vpnui | vpn |
| Mac | Not supported for security appliance deployment | vpn |

In order to import your executable to customize the client GUI, follow these steps using Cisco ASDM (not shown in the figure):

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Binary**.

**Step 2** Choose **Import**.

**Step 3** Enter the name of the file to import.

**Step 4** Choose an operating system platform and specify the file to import.

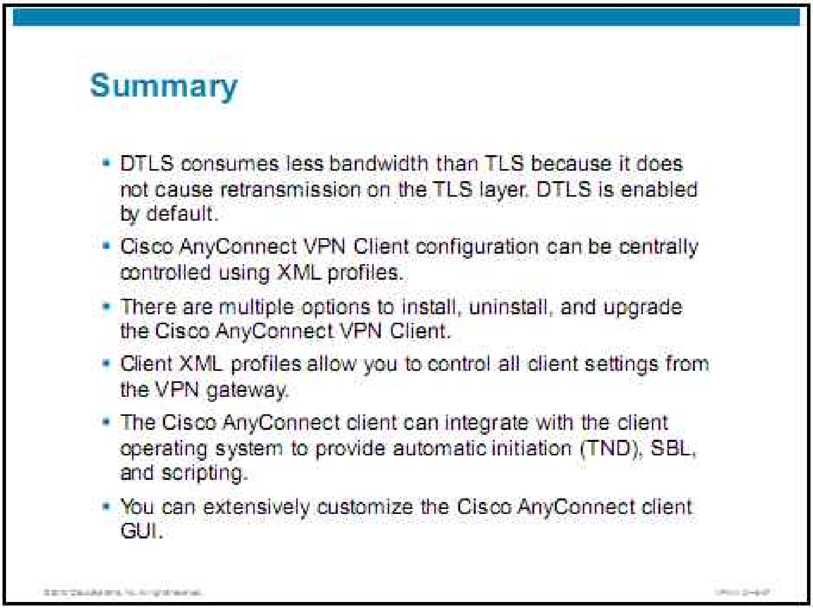
**Step 5** Click **Import Now**. The file appears in the table.

**Step 6** Repeat the previous four steps for all files that you want to import to the Cisco ASA adaptive security appliance.

**Step 7** Click **OK**, and click **Apply** to apply the configuration changes to the security appliance.

# Summary

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



## Summary

- DTLS consumes less bandwidth than TLS because it does not cause retransmission on the TLS layer. DTLS is enabled by default.
- Cisco AnyConnect VPN Client configuration can be centrally controlled using XML profiles.
- There are multiple options to install, uninstall, and upgrade the Cisco AnyConnect VPN Client.
- Client XML profiles allow you to control all client settings from the VPN gateway.
- The Cisco AnyConnect client can integrate with the client operating system to provide automatic initiation (TND), SBL, and scripting.
- You can extensively customize the Cisco AnyConnect client GUI.

# References

For additional information, refer to these resources:

- *Cisco ASA 5500 Series Command Reference, 8.2* at http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/cmd_ref.html
- *Cisco AnyConnect VPN Client Administrator Guide, Release 2.4* at http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/administration/guide/anyconnectadmin24.html

## Lesson 3

# Deploying Advanced Authentication in Cisco AnyConnect Full Tunnel SSL VPNs

## Overview

When deploying virtual private networks (VPNs) in general, it is very important to use strong authentication options. This lesson describes several advanced authentication options that you have when implementing Cisco AnyConnect full tunnel Secure Sockets Layer (SSL) VPNs on the Cisco ASA adaptive security appliance. These authentication options offer adequate security and scalability, as opposed to the basic local authentication that was described in the previous lesson. This lesson describes advanced password-based authentication using external authentication, authorization, and accounting (AAA) servers, certificate-based authentication using the local certificate authority (CA) of the security appliance, and options that are available to verify user certificates for revocation.

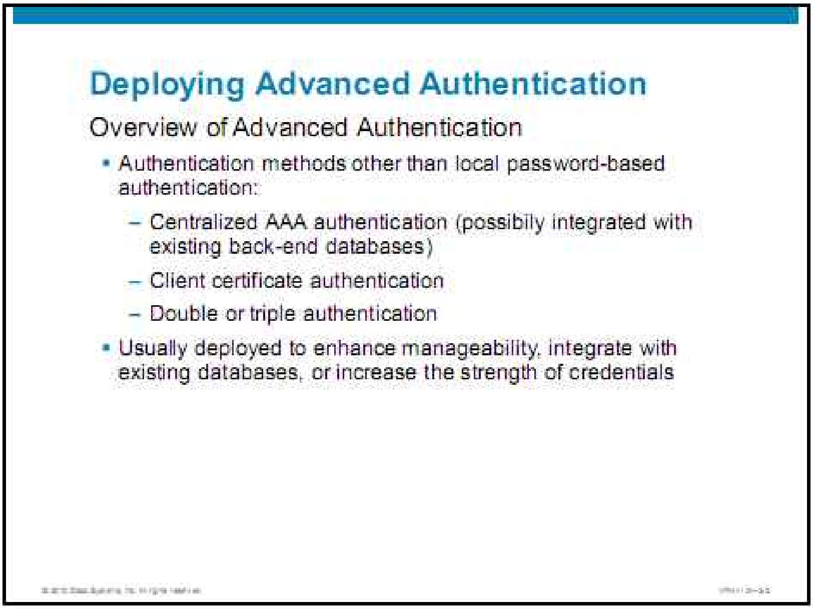
## Objectives

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

- Plan the deployment of advanced client authentication
- Configure and verify the advanced password-based client authentication
- Configure and verify the local CA on the Cisco ASA adaptive security appliance and on the Cisco AnyConnect client with client certificates that are provisioned by the security appliance
- Configure and verify integration with supporting PKI entities
- Configure and verify multiple client authentications

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic provides an overview of how to plan the deployment of advanced client authentication.



## Deploying Advanced Authentication

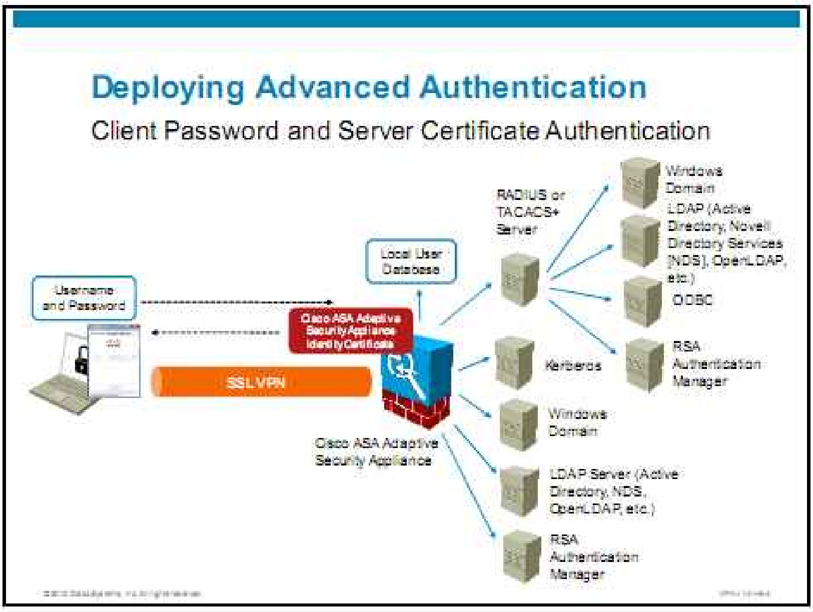
Overview of Advanced Authentication

- Authentication methods other than local password-based authentication:
  - Centralized AAA authentication (possibily integrated with existing back-end databases)
  - Client certificate authentication
  - Double or triple authentication
- Usually deployed to enhance manageability, integrate with existing databases, or increase the strength of credentials

Authentication of Secure Sockets Layer (SSL) virtual private network (VPN) clients using the local database is the most basic authentication option. More-advanced authentication options for SSL VPN users include the following:

- **Centralized AAA authentication:** You can authenticate clients with an existing external AAA database, such as a RADIUS or TACACS+ user database. Such an external database can also be integrated with other back-end databases, such as Rivest, Shamir, and Adleman (RSA) SecurID or Microsoft Active Directory.
- **Authentication with digital certificates:** You can configure the Cisco ASA adaptive security appliance to require digital certificates on clients. Before establishing a connection, the security appliance validates the certificate of a client and allows connection establishment only if the certificate can be validated using a public key that is stored on the certificate of a trusted certificate authority (CA).
- **Double and triple authentication:** Starting with Cisco ASA Software Version 8.2, the SSL VPN remote access (clientless and Cisco AnyConnect VPN Client) software supports double and triple authentication. You can combine certificate authentication with up to two AAA authentication methods that are performed in a row. The following examples are possible combinations that can be used:
  - — RSA/Security Dynamics International (SDI) + Lightweight Directory Access Protocol (LDAP) authentication
  - — Certificates + RADIUS
  - — Certificates + Radius + RSA/SDI

Such types of client authentication are deployed to enhance the manageability of users, to integrate VPN deployments with an existing user database infrastructure, or to increase strength of client authentication.



## Deploying Advanced Authentication

### Client Password and Server Certificate Authentication

Username and Password
Local User Database
Cisco ASA Adaptive Security Appliance Identity Certificate
SSL VPN
Cisco ASA Adaptive Security Appliance
RADIUS or TACACS+ Server
Windows Domain
LDAP (Active Directory, Novell Directory Services [NDS], OpenLDAP, etc.)
ODBC
RSA Authentication Manager
Kerberos
Windows Domain
LDAP Server (Active Directory, NDS, OpenLDAP, etc.)
RSA Authentication Manager

The figure illustrates an example where the clients authenticate the security appliance by using its digital certificate, and the appliance authenticates the clients by using usernames and passwords. The Cisco ASA adaptive security appliance can validate usernames and passwords on external authentication servers such as the following:

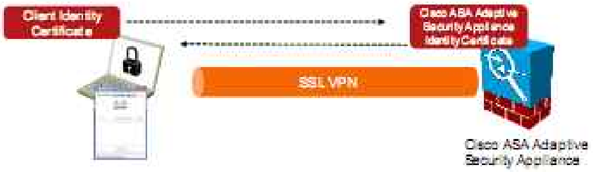
- RADIUS authentication server
- TACACS+ authentication server
- Kerberos authentication server
- Windows authentication server
- LDAP authentication server
- RSA SecurID authentication server

A RADIUS or TACACS+ authentication server can be configured to check the credentials of a user in back-end authentication servers. Back-end authentication servers can include the following:

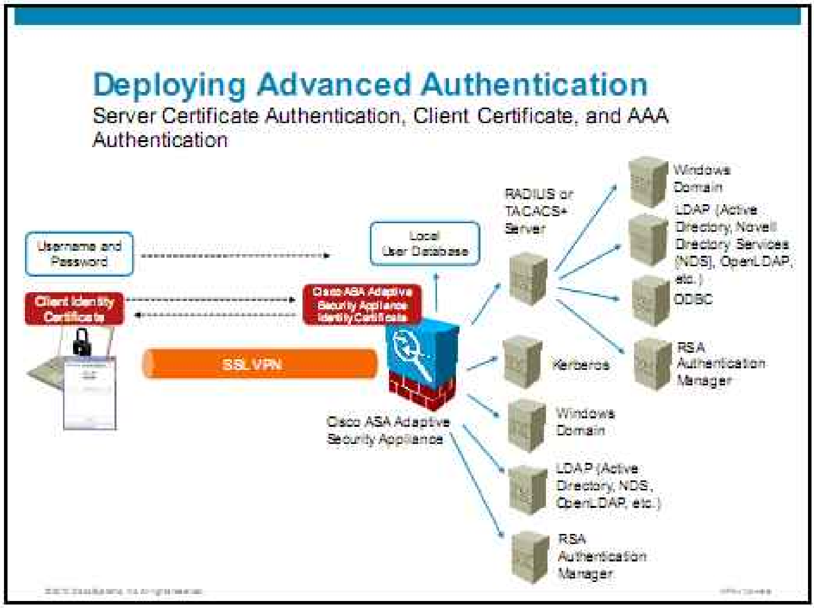
- Windows authentication server
- LDAP authentication server
- External Open DataBase Connectivity (ODBC) database
- RSA SecurID authentication server

## Deploying Advanced Authentication

### Client Certificate and Server Certificate Authentication


Client Identity Certificate
Cisco ASA Adaptive Security Appliance Identity Certificate
SSL VPN
Cisco ASA Adaptive Security Appliance

The figure illustrates an example where the clients authenticate the security appliance using its digital certificate, and the appliance authenticates the clients using their certificates. When each entity successfully validates the certificate of the other, the SSL VPN connection can be established.

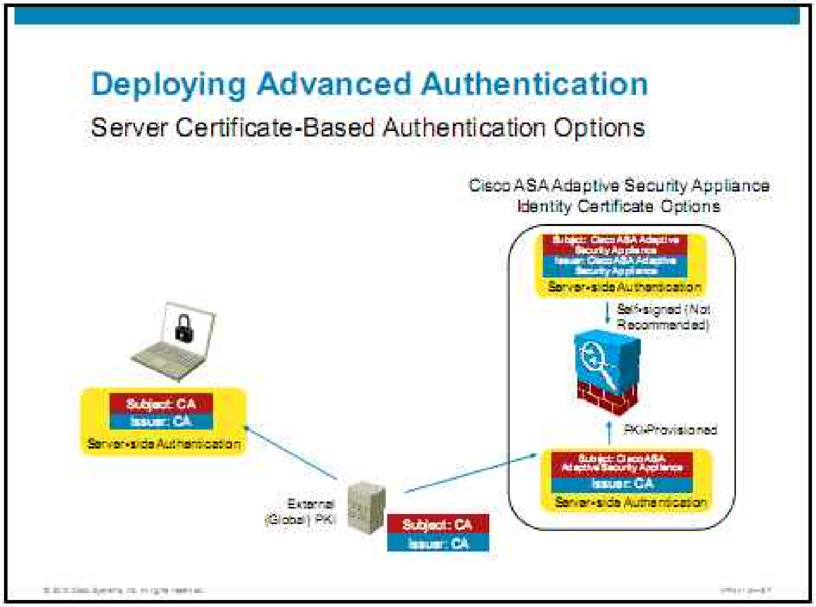


## Deploying Advanced Authentication

Server Certificate Authentication, Client Certificate, and AAA Authentication

Username and Password
Local User Database
Client Identity Certificate
Cisco ASA Adaptive Security Appliance Identity Certificate
SSL VPN
Cisco ASA Adaptive Security Appliance
RADIUS or TACACS+ Server
Windows Domain
LDAP (Active Directory, Novell Directory Services (NDS), OpenLDAP, etc.)
ODBC
RSA Authentication Manager
Kerberos
Windows Domain
LDAP (Active Directory, NDS, OpenLDAP, etc.)
RSA Authentication Manager

In the third example, the Cisco ASA adaptive security appliance again authenticates itself to the client using a digital certificate. In this scenario, the client first authenticates itself to the security appliance using a digital certificate. If the Cisco ASA adaptive security appliance successfully validates the client certificate, it prompts the user for a username and password. The security appliance then validates the credentials of a user by using external AAA servers. This type of advanced authentication is the most secure, but also requires the most configuration effort.



## Deploying Advanced Authentication

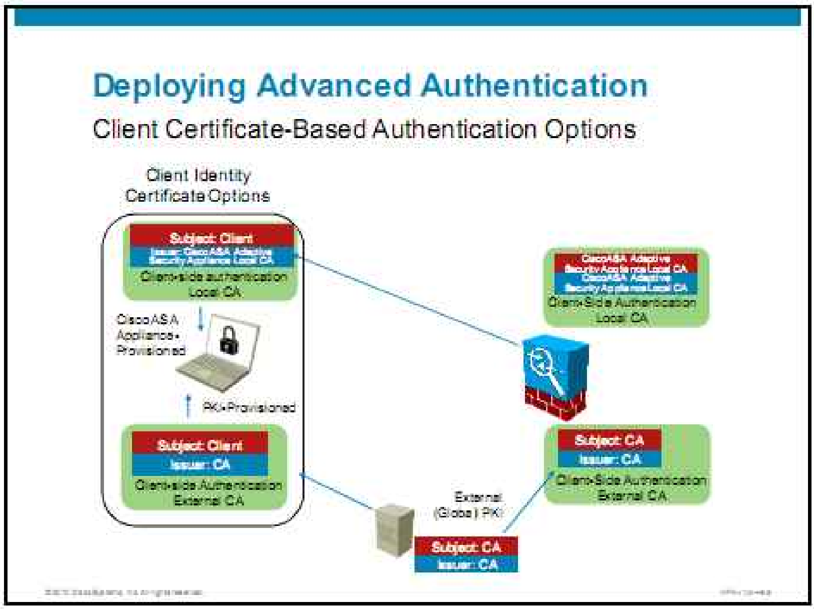
### Server Certificate-Based Authentication Options

Cisco ASA Adaptive Security Appliance
Identity Certificate Options
Subject: Cisco ASA Adaptive Security Appliance
Issuer: Cisco ASA Adaptive Security Appliance
Server-side Authentication
Self-signed (Not Recommended)
PKI-Provisioned
Subject: Cisco ASA Adaptive Security Appliance
Issuer: CA
Server-side Authentication
Subject: CA
Issuer: CA
Server-side Authentication
External (Global) PKI
Subject: CA
Issuer: CA

When you authenticate by using digital certificates, you have different deployment options. For server authentication, you can deploy the Cisco ASA adaptive security appliance identity certificate in two ways:

- **Self-signed certificate:** This option is not recommended, but it is the only approach if you do not use external public key infrastructure (PKI).
- **PKI-obtained certificate:** You can configure the Cisco ASA adaptive security appliance to obtain an identity certificate from the external PKI.

If you are using a PKI-obtained certificate, clients should have a CA certificate that is installed locally to verify the identity certificate of a server.



## Deploying Advanced Authentication

Client Certificate-Based Authentication Options

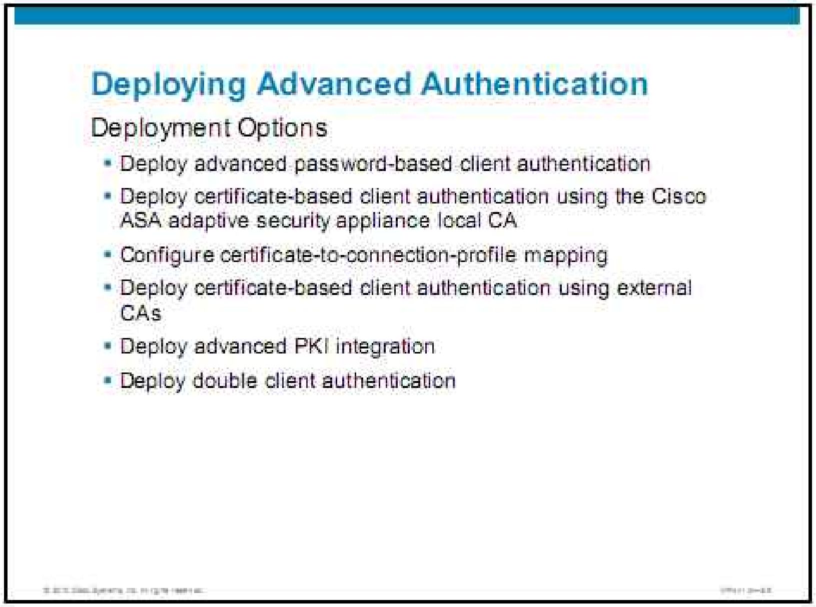
Client Identity
Certificate Options
Subject: Client
Issuer: Cisco ASA Adaptive Security Appliance Local CA
Client-side authentication Local CA
Cisco ASA Appliance-Provisioned
PKI-Provisioned
Subject: Client
Issuer: CA
Client-side Authentication External CA
Cisco ASA Adaptive Security Appliance Local CA
Cisco ASA Adaptive Security Appliance Local CA
Client-Side Authentication Local CA
Subject: CA
Issuer: CA
Client-Side Authentication External CA
External (Global) PKI
Subject: CA
Issuer: CA

For client-side authentication, clients can obtain their identity certificates by using two different options:

- You can enable a local CA on the Cisco ASA adaptive security appliance. In this case, the certificates of clients are issued and managed by the security appliance. The appliance still needs a self-signed or PKI-provided certificate to authenticate itself to clients.
- You can use an external PKI to issue identity certificates to the Cisco ASA adaptive security appliance and clients. In this case, certificates are managed by an external PKI system.

If you are using a PKI-obtained certificate, the server should have a CA certificate that is installed locally to verify the identity certificates of clients. If you are using a local CA on the security appliance, the appliance will create a self-signed certificate, which is used to sign certificates that are issued to clients.

**Note** The local CA on the Cisco ASA adaptive security appliance can be used for SSL VPNs only.



## Deploying Advanced Authentication

Deployment Options

- Deploy advanced password-based client authentication
- Deploy certificate-based client authentication using the Cisco ASA adaptive security appliance local CA
- Configure certificate-to-connection-profile mapping
- Deploy certificate-based client authentication using external CAs
- Deploy advanced PKI integration
- Deploy double client authentication

You have these options when deploying advanced authentication for SSL VPNs:

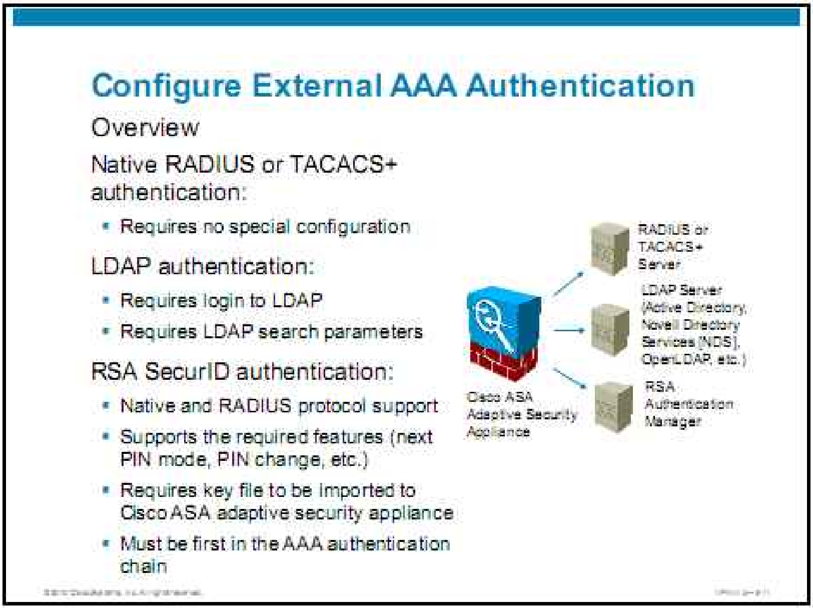
- Deploy advanced password-based client authentication
- Deploy certificate-based client authentication using the Cisco ASA adaptive security appliance local CA
- Configure certificate-to-connection-profile mappings
- Deploy certificate-based client authentication by using an external CA
- Deploy advanced PKI integration
- Deploy double client authentication

When deploying advanced authentication for SSL VPN connections on the Cisco ASA adaptive security appliance, you need specific input parameters:

- **Existing user databases and their location:** This parameter is needed to integrate the Cisco ASA adaptive security appliance with the external user databases.
- **Strength of existing user credentials:** This parameter is needed to determine whether an existing database is suitable for remote access connections.
- **Existing authentication protocols:** This parameter is needed to determine authentication protocol compatibility.
- **PKI information:** This parameter is needed to enroll the Cisco ASA adaptive security appliance and clients into a PKI.
- **Time-synchronization options:** This parameter is needed when you are using digital certificates. Time synchronization is very important to synchronize time on all entities that are involved in authentication.

# Deploying External AAA Authentication

This topic describes how to configure and verify the external AAA client authentication.



## Configure External AAA Authentication

Overview

Native RADIUS or TACACS+ authentication:

- Requires no special configuration

LDAP authentication:

- Requires login to LDAP
- Requires LDAP search parameters

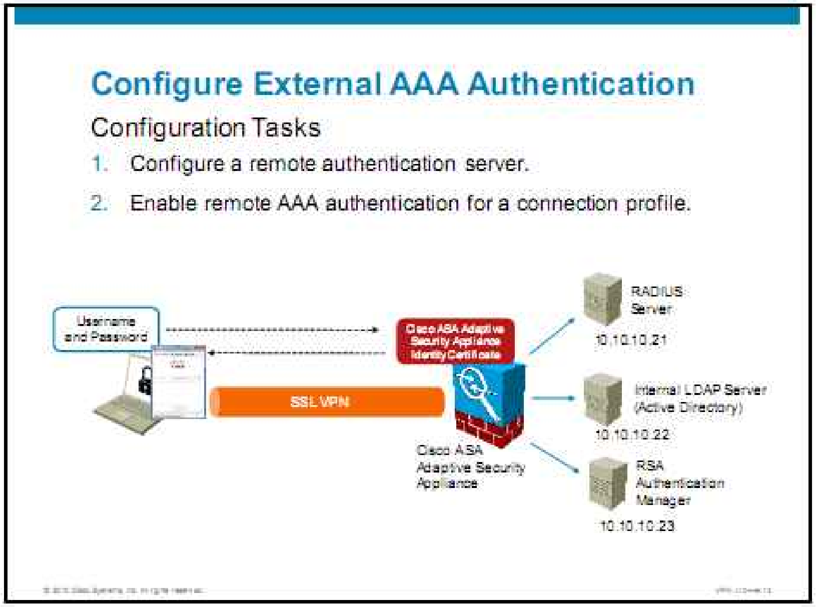
RSA SecurID authentication:

- Native and RADIUS protocol support
- Supports the required features (next PIN mode, PIN change, etc.)
- Requires key file to be imported to Cisco ASA adaptive security appliance
- Must be first in the AAA authentication chain

RADIUS or TACACS+ Server
LDAP Server (Active Directory, Novell Directory Services [NDS], OpenLDAP, etc.)
RSA Authentication Manager
Cisco ASA Adaptive Security Appliance

When configuring password-based client authentication, the following options are recommended:

- **RADIUS or TACACS+ authentication:** In this case, no special configuration is needed on the Cisco ASA adaptive security appliance. You only need to provide the IP address and shared key of the authentication server.
- **LDAP authentication:** When using authentication with LDAP server, you have to provide the IP address of the LDAP server on the Cisco ASA adaptive security appliance. The security appliance has to log into the LDAP server. Therefore, you also have to add the Cisco ASA adaptive security appliance as a user that has enough privileges in order to search for users in the LDAP server. Additionally, you must provide LDAP search parameters, which include base distinguished name (DN) and scope of the search.
- **RSA SecurID authentication:** The Cisco ASA adaptive security appliance supports the native SDI or RADIUS protocol between the security appliance and the RSA SecurID server. If multiple AAA servers are consulted in a row, the RSA SecurID host must be the first in the list.



## Configure External AAA Authentication

Configuration Tasks

1. Configure a remote authentication server.
2. Enable remote AAA authentication for a connection profile.

Username and Password
Cisco ASA Adaptive Security Appliance Identity Certificate
SSL VPN
Cisco ASA Adaptive Security Appliance
RADIUS Server
10.10.10.21
Internal LDAP Server (Active Directory)
10.10.10.22
RSA Authentication Manager
10.10.10.23

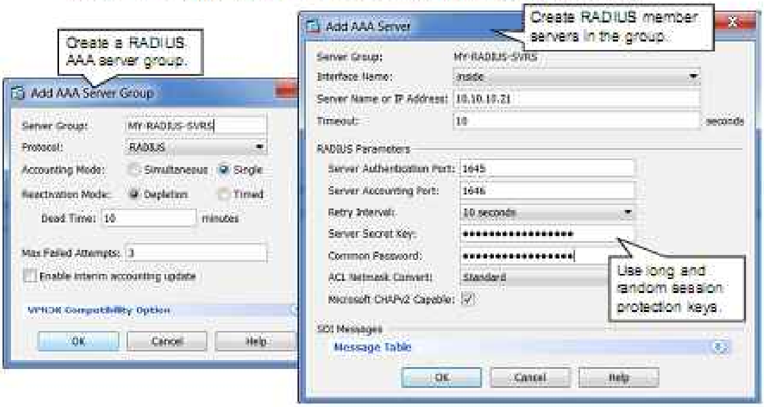
These are the configuration tasks when configuring advanced password-based client authentication:

1. Configure a remote authentication server on the Cisco ASA adaptive security appliance.
2. Enable remote AAA authentication in a connection profile.

The figure shows an example that will serve as the configuration scenario for ongoing configuration tasks. First, you will configure RADIUS, LDAP, and RSA SecurID authentication servers. Then, you will enable remote AAA authentication using configured servers in a connection profile.

## Configure External AAA Authentication

### Task 1: Configure a RADIUS Authentication Server



Create a RADIUS AAA server group.

Add AAA Server Group

Server Group: MY-RADIUS-SVRS
Protocol: RADIUS
Accounting Mode: ○ Simultaneous ● Single
Reactivation Mode: ● Depletion ○ Timed
Dead Time: 10 minutes
Max Failed Attempts: 3
□ Enable interim accounting update

Create RADIUS member servers in the group.

Add AAA Server

Server Group: MY-RADIUS-SVRS
Interface Name: inside
Server Name or IP Address: 10.10.10.21
Timeout: 10 seconds

RADIUS Parameters
Server Authentication Port: 1645
Server Accounting Port: 1646
Retry Interval: 10 seconds
Server Secret Key: ******************
Common Password: ******************
ACL Netmask Convert: Standard
Microsoft CHAPv2 Capable: ☑

Use long and random session protection keys.

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

In the first configuration task in this sequence, you will configure a AAA group to include the RADIUS authentication server and the authentication protocols of the group. You may also reuse an existing AAA group that is defined on the Cisco ASA adaptive security appliance.

To configure a RADIUS authentication server using the Cisco Adaptive Security Device Manager (ASDM), first create a RADIUS server group and then configure an individual server in the AAA server group. To create a AAA server group by using Cisco ASDM, complete the following steps:

**Step 1** Inside the Cisco ASDM, choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups.** The AAA Server Groups panel is displayed (not shown in the figure).

**Step 2** Click **Add** in the AAA Server Groups area (not shown in the figure). The Add AAA Server Group window opens.

**Step 3** Enter a name for the server group in the Server Group field. This example uses the name MY-RADIUS-SVRS to name the AAA server group.

**Step 4** From the Protocol drop-down list, choose the AAA protocol that the servers in the group support. You can choose RADIUS, TACACS+, Microsoft Windows NT Domain, SDI, Kerberos, LDAP, or HTTP form. In the figure, RADIUS is chosen.

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

To configure an individual authentication server in the RADIUS server group, complete the following steps:

**Step 1** Choose a configured server group from the AAA Server Groups table in the AAA Server Groups panel (not shown in the figure).

**Step 2** Click **Add** in the Servers in Selected Group area of the AAA Server Groups panel (not shown in the figure). The Add AAA Server window opens.

**Step 3** From the Interface Name drop-down list, choose the interface where the AAA server resides. In the figure, the inside interface is chosen.

**Step 4** Enter the name or IP address of the AAA server in the Server Name or IP Address field. In the figure, 10.10.10.21 is entered.

**Step 5** Optionally, specify the server authentication and accounting ports. RADIUS packets use UDP port 1812 for RADIUS authentication messages and UDP port 1813 for RADIUS accounting messages. Some earlier RADIUS implementations use UDP port 1645 for RADIUS authentication messages and UDP port 1646 for RADIUS accounting messages. In the figure, the default ports 1645 and 1646 are used.

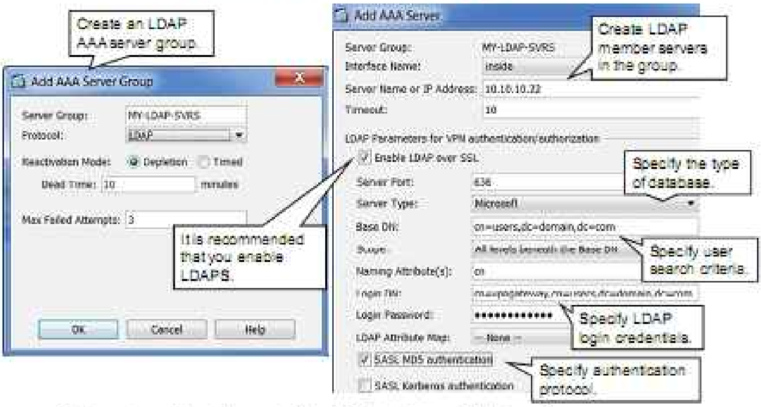
**Step 6** Enter an alphanumeric value up to 64 characters in the Server Secret Key field. The server secret key is used for cryptographic protection of the session between the security appliance and the RADIUS (access control server [ACS]) server. The key must be the same on both the security appliance and the RADIUS (ACS) server. The key value is a case-sensitive. The Server Secret Key field displays only asterisks.

**Step 7** Click **OK**.

Click **Apply** to apply the configuration.

## Configure External AAA Authentication

### Task 1: Configure an LDAP Authentication Server (Cont.)



Add AAA Server Group

Server Group: MY-LDAP-SVRS
Protocol: LDAP
Reactivation Mode: ● Depletion ○ Timed
Dead Time: 10 minutes
Max Failed Attempts: 3

Add AAA Server

Server Group: MY-LDAP-SVRS
Interface Name: inside
Server Name or IP Address: 10.10.10.22
Timeout: 10

LDAP Parameters for VPN authentication/authorization
☑ Enable LDAP over SSL
Server Port: 636
Server Type: Microsoft
Base DN: cn=users,dc=domain,dc=com
Scope: All levels beneath the Base DN
Naming Attribute(s): cn
Login DN: cn=aupogateway,cn=users,dc=domain,dc=com
Login Password: *************
LDAP Attribute Map: -- None --
☑ SASL MD5 authentication
☐ SASL Kerberos authentication

Create an LDAP AAA server group.
OK
Cancel
Help
Create LDAP member servers in the group.
It is recommended that you enable LDAPS.
Specify the type of database.
Specify user search criteria.
Specify LDAP login credentials.
Specify authentication protocol.

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

To configure an LDAP authentication server by using Cisco ASDM, first create an LDAP server group, and then configure individual servers in the AAA server group. To create a AAA server group by using Cisco ASDM, complete the following steps:

**Step 1** Inside the Cisco ASDM, choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups.** The AAA Server Groups panel is displayed (not shown in the figure).

**Step 2** Click **Add** in the AAA Server Groups area (not shown in the figure). The Add AAA Server Group window opens.

**Step 3** Enter a name for the server group in the Server Group field. This example uses the name MY-LDAP-SVRS to name the AAA server group.

**Step 4** From the Protocol drop-down list, choose the AAA protocol that the servers in the group support. You can choose RADIUS, TACACS+, Windows NT Domain, SDI, Kerberos, LDAP, or HTTP form. In the figure, LDAP is chosen.

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

To configure an individual authentication server in the LDAP server group, complete the following steps:

**Step 1** Choose a configured server group from the AAA Server Groups table in the AAA Server Groups panel (not shown in the figure).

**Step 2** Click **Add** in the Servers in Selected Group area of the AAA Server Groups panel (not shown in the figure). The Add AAA Server window opens.

**Step 3** From the Interface Name drop-down list, choose the interface where the AAA server resides. In the figure, the inside interface is chosen.

**Step 4** Enter the name or IP address of the AAA server in the Server Name or IP Address field. In the figure, 10.10.10.22 is entered.

**Step 5** Optionally, check the **Enable LDAP over SSL** check box to enable secure communication between the Cisco ASA adaptive security appliance and the LDAP server. It is recommended to enable this option.

**Step 6** Optionally, specify a nondefault port for communication between the Cisco ASA adaptive security appliance and the LDAP server by entering a number into the Server Port input field. By default, LDAP uses 389 and LDAP over SSL (LDAPS) uses 636.

**Step 7** Choose an LDAP server type from the Server Type drop-down menu. You have the following options:

- Detect Automatically/Use Generic Type
- Microsoft
- Novell
- OpenLDAP
- Sun

In the example, the Microsoft server type is selected.

**Step 8** In the Base DN input field, enter a base distinguished name (DN) or a location in the LDAP hierarchy where the server should begin searching when it receives an LDAP request. In the example, cn=users,dc=domain,dc=com is entered as the base DN.

**Step 9** Choose an option from the Scope drop-down menu to specify the extent to which the server should search the LDAP hierarchy when it receives an authorization request. The available options include the following:

- **One Level:** Searches only one level beneath the base DN. This option is quicker.
- **All Levels:** Searches all levels beneath the base DN. This option tells the server to search the entire subtree hierarchy. This option takes more time.

In the example, the All Levels option is selected.

**Step 10** Enter a login DN into the Login DN input field. This name should be the DN of a user who has enough privileges to search for users in the LDAP server. In the example, cn=vpngateway,cn=users,dc=domain,dc=com is entered.

**Step 11** Enter a password for the login DN user account into the Login Password input field.

**Note** The Cisco ASA adaptive security appliance uses the login DN and login password to establish trust (bind) with an LDAP server. The login DN represents a user record in the LDAP server that the administrator uses for binding.

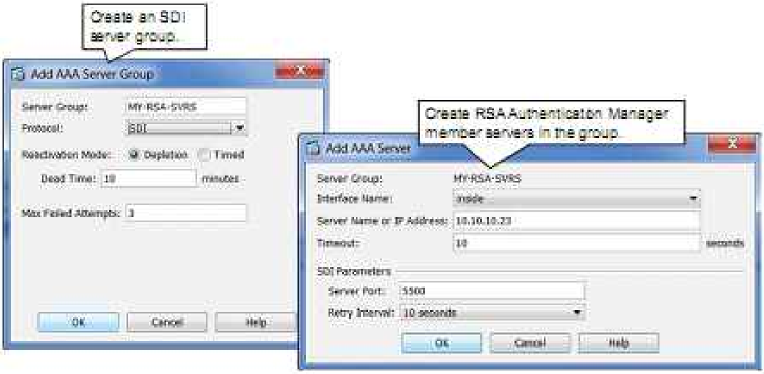
**Step 12** Optionally, enable Simple Authentication and Security Layer (SASL) authentication by checking the SASL MD5 Authentication or SASL Kerberos Authentication check box.

**Step 13** Click **OK**.

**Step 14** Click **Apply** to apply the configuration.

## Configure External AAA Authentication

### Task 1: Configure an RSA Authentication Server (Cont.)



Create an SDI server group.

Add AAA Server Group

Server Group: MY-RSA-SVRS

Protocol: SDI

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

Create RSA Authentication Manager member servers in the group.

Add AAA Server

Server Group: MY-RSA-SVRS

Interface Name: inside

Server Name or IP Address: 10.10.10.23

Timeout: 10 seconds

SDI Parameters

Server Port: 5500

Retry Interval: 10 seconds

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

To configure an RSA authentication server by using Cisco ASDM, first create an RSA server group, and then configure an individual server in the AAA server group. To create a AAA server group by using Cisco ASDM, complete the following steps:

**Step 1** Inside the Cisco ASDM, choose **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups.** The AAA Server Groups panel is displayed (not shown in the figure).

**Step 2** Click **Add** in the AAA Server Groups area (not shown in the figure). The Add AAA Server Group window opens.

**Step 3** Enter a name for the server group in the Server Group field. This example uses the name MY-RSA-SVRS to name the AAA server group.

**Step 4** From the **Protocol** drop-down list, choose the AAA protocol that the servers in the group support. You can choose RADIUS, TACACS+, Windows NT Domain, SDI, Kerberos, LDAP, or HTTP form. In the figure, SDI is chosen.

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

To configure an individual authentication server in the SDI server group, complete the following steps:

**Step 1** Choose a configured server group from the AAA Server Groups table in the AAA Server Groups panel (not shown in the figure).

**Step 2** Click **Add** in the Servers in Selected Group area of the AAA Server Groups panel (not shown in the figure). The Add AAA Server window opens.

**Step 3** From the Interface Name drop-down list, choose the interface where the AAA server resides. In the figure, the inside interface is chosen.

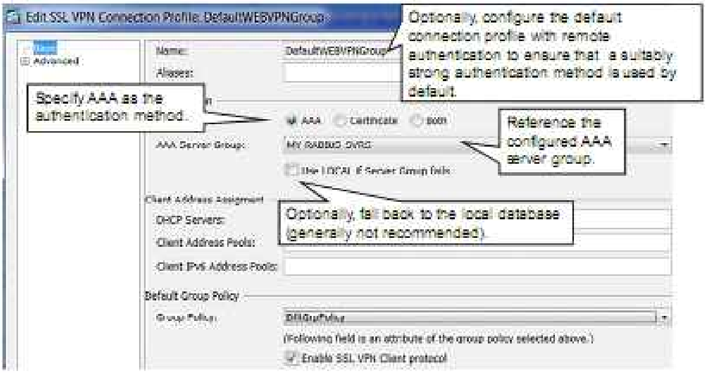
**Step 4** Enter the name or IP address of the AAA server in the Server Name or IP Address field. In the figure, 10.10.10.23 is entered.

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

**Step 6** Click **Apply** to apply the configuration.

## Configure External AAA Authentication

Task 2: Enable Remote AAA Authentication



Edit SSL VPN Connection Profile: DefaultWEBVPNGroup

Name: DefaultWEBVPNGroup

Aliases:

● AAA ○ Certificate ○ Both

AAA Server Group: MY-RADIUS-SVRS

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: DfltGrpPolicy

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN Client protocol

Optionally, configure the default connection profile with remote authentication to ensure that a suitably strong authentication method is used by default.

Specify AAA as the authentication method.

Reference the configured AAA server group.

Optionally, fall back to the local database (generally not recommended).

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

You can enable remote AAA authentication for the default connection profile to ensure that a strong authentication method is used by default. To enable remote AAA authentication from the default connection profile by using Cisco ASDM, complete the following steps:

**Step 1** Inside the Cisco ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. The AnyConnect Connection Profiles window is displayed (not shown in the figure).

**Step 2** Choose the **DefaultWebVPNGroup** connection profile from the Connection Profiles table. Click **Edit** (not shown in the figure).

**Step 3** The Edit SSL VPN Connection Profile window is displayed, as shown in the figure.

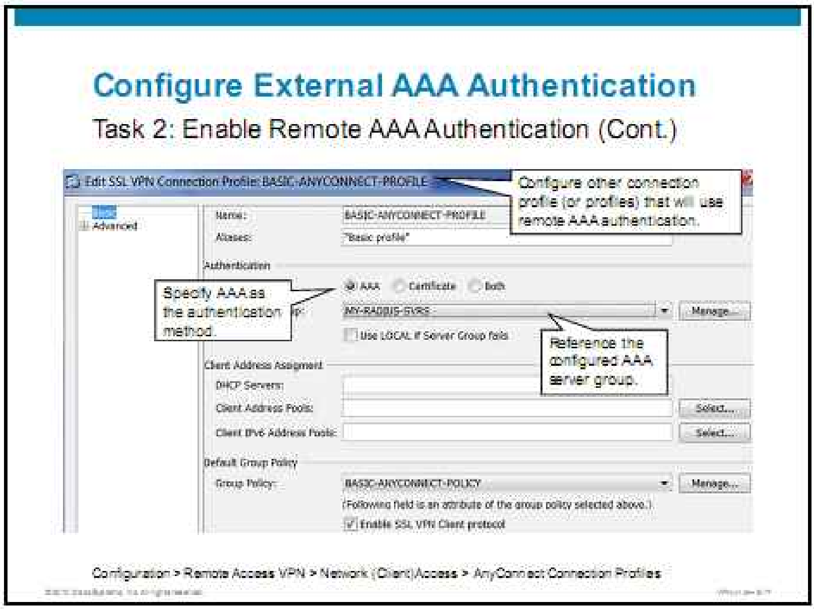
**Step 4** Check the **AAA** radio button.

**Step 5** Choose the configured AAA server group from the AAA Server Group drop-down menu. In the example, the MY-RADIUS-SVRS server group is selected.

**Step 6** Optionally, check the **Use Local If Server Group Fails** check box to enable fallback to the local database if a server group fails. This selection is generally not recommended.

**Step 7** Click **OK**.

**Step 8** Click **Apply** to apply the configuration.



## Configure External AAA Authentication

### Task 2: Enable Remote AAA Authentication (Cont.)

Edit SSL VPN Connection Profile: BASIC-ANYCONNECT-PROFILE

Name: BASIC-ANYCONNECT-PROFILE

Aliases: "Basic profile"

Authentication

● AAA ○ Certificate ○ Both

MY-RADIUS-SVRS

☐ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: BASIC-ANYCONNECT-POLICY

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN Client protocol

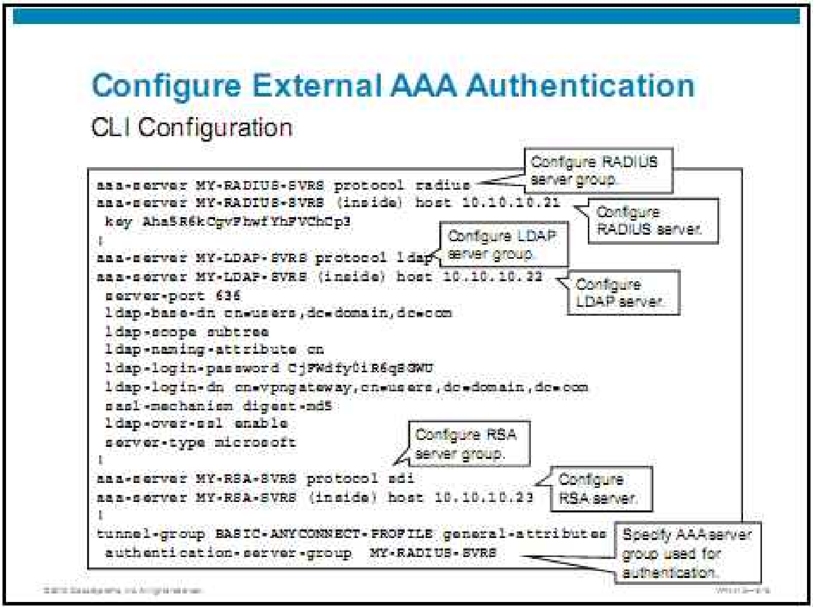
Configure other connection profile (or profiles) that will use remote AAA authentication.

Specify AAA as the authentication method.

Reference the configured AAA server group.

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

Repeat the steps that are described in the previous figure to enable remote AAA authentication for any other connection profiles. In the example, the BASIC-ANYCONNECT-PROFILE is also configured for authentication with the authentication server in the MY-RADIUS-SRV server group.



## Configure External AAA Authentication

### CLI Configuration

```
aaa-server MY-RADIUS-SVRS protocol radius
aaa-server MY-RADIUS-SVRS (inside) host 10.10.10.21
 key Aha5R6kCgvFhwfYhFVChCp3
!
aaa-server MY-LDAP-SVRS protocol ldap
aaa-server MY-LDAP-SVRS (inside) host 10.10.10.22
 server-port 636
 ldap-base-dn cn=users,dc=domain,dc=com
 ldap-scope subtree
 ldap-naming-attribute cn
 ldap-login-password CjFWdfy0iR6qBGWU
 ldap-login-dn cn=vpngateway,cn=users,dc=domain,dc=com
 sasl-mechanism digest-md5
 ldap-over-ssl enable
 server-type microsoft
!
aaa-server MY-RSA-SVRS protocol sdi
aaa-server MY-RSA-SVRS (inside) host 10.10.10.23
!
tunnel-group BASIC-ANYCONNECT-PROFILE general-attributes
 authentication-server-group  MY-RADIUS-SVRS
```

Configure RADIUS server group.

Configure RADIUS server.

Configure LDAP server group.

Configure LDAP server.

Configure RSA server group.

Configure RSA server.

Specify AAA server group used for authentication.

To configure advanced password-based authentication using the command-line interface (CLI), use the following commands.

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, followed by a server group name, the interface through which the server is reachable, and the 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 AAA server configuration mode.

In the example, three server groups are configured. The MY-RADIUS-SVRS server group is configured as a RADIUS server group, and the server at the 10.10.10.21 address is configured as a member of the MY-RADIUS-SVRS server group. The MY-LDAP-SVRS server group is configured as an LDAP server group, and the server at the 10.10.10.22 address is configured as a member of the MY-LDAP-SVRS server group. The MY-RSA-SVRS server group is configured as an RSA server group, and the server at the 10.10.10.23 address is configured as a member of the MY-RSA-SVRS server group.

To configure parameters inside the LDAP server group, use the following commands in server group configuration mode. Use the **server-port** command to specify the port that is used between the Cisco ASA adaptive security appliance and the LDAP server. 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 the 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 that the Cisco ASA adaptive security appliance will use to search the LDAP directory. Use the **sasl-mechanism** command to enable SASL authentications, and use the **ldap-over-ssl enable** command to enable LDAPS. Use the **server-type** command to specify the LDAP authentication server type.

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

In the example, the connection profile BASIC-ANYCONNECT-PROFILE is configured for authentication using the MY-RADIUS-SVRS server group.

## aaa-server

To create a 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 |
|---|---|
| *server-tag* | Specifies the server group name, which is matched by the name that is specified by the **aaa-server host** commands. Other AAA commands make reference to the AAA server group name. |
| **protocol** *server-protocol* | Specifies the AAA protocol that the servers in the group support:<br>▪ **http-form**<br>▪ **kerberos**<br>▪ **ldap**<br>▪ **nt**<br>▪ **radius**<br>▪ **sdi**<br>▪ **tacacs+** |

## aaa-server host

To configure a AAA server as part of a 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 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 |
|---|---|
| *(interface-name)* | (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 the inside interface, if available. |
| *key* | (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 the 127-character maximum 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 the server systems. Spaces are not permitted in the key, but other special characters are allowed. You can add or modify the key using the **key** command in host mode. |
| *name* | Specifies the name of the server using either a name that is assigned locally using the **name** command or a Domain Name System (DNS) name. The maximum number of characters is 128 for DNS names and 63 characters for names that are assigned using the **name** command. |
| *server-ip* | Specifies the IP address of the AAA server. |
| *server-tag* | Specifies a symbolic name of the server group, which is matched by the name that is specified by the **aaa-server** command. |
| **timeout** *seconds* | (Optional) The timeout interval for the request. This value 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 by using the **timeout** command in host mode. |

## 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 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 |
|---|---|
| *string* | 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; for example, OU=Cisco. Spaces are not permitted in the string, but other special characters are allowed. |

## ldap-scope

To specify the extent to which the server should search the LDAP hierarchy when it receives an authorization request, use the **ldap-scope** command in aaa-server host configuration mode. The aaa-server host configuration mode is accessible from the aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command.

**ldap-scope** *scope*

### ldap-scope Parameters

| Parameter | Description |
|---|---|
| *scope* | The number of levels in the LDAP hierarchy in which the server should search when it receives an authorization request. Valid values include the following:<br>■ **onelevel:** Search only one level beneath the base DN.<br>■ **subtree:** Search all levels beneath the base DN. |

## ldap-naming-attribute

To specify the relative distinguished name attribute, use the **ldap-naming-attribute** command in aaa-server host configuration mode. The aaa-server host configuration mode is accessible from the aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command:

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

### ldap-naming-attribute Parameters

| Parameter | Description |
|---|---|
| *string* | 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 with which the system should bind, use the **ldap-login-dn** command in aaa-server host configuration mode. The aaa-server host configuration mode is accessible from the aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command.

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

### ldap-login-dn Parameters

| Parameter | Description |
|---|---|
| *string* | 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 aaa-server host configuration mode. The aaa-server host configuration mode is accessible from the aaa-server protocol configuration mode. To remove this password specification, use the **no** form of this command:

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

### ldap-login-password Parameters

| Parameter | Description |
|---|---|
| *string* | A case-sensitive, alphanumeric password, up to 64 characters long. The password cannot contain space characters. |

## ldap-over-ssl

To establish a secure SSL connection between the adaptive security appliance and the LDAP server, use the **ldap-over-ssl** command in aaa-server host configuration mode. To disable SSL for the connection, use the **no** form of this command.

**ldap-over-ssl enable**

### ldap-over-ssl Parameters

| Parameter | Description |
|---|---|
| **enable** | Specifies that SSL secures a connection to an LDAP server |

## sasl-mechanism

To specify a SASL mechanism for authenticating an LDAP client to an LDAP server, use the **sasl-mechanism** command in aaa-server host configuration mode. The SASL authentication mechanism options are digest-md5 and kerberos.

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

**sasl-mechanism** {**digest-md5** | **kerberos** *server-group-name*}

**Note** Because the adaptive security appliance serves as a client proxy to the LDAP server for VPN users, the LDAP client that is referred to here is the adaptive security appliance.

### sasl-mechanism Parameters

| Parameter | Description |
|---|---|
| **digest-md5** | The adaptive security appliance responds with a Message Digest 5 (MD5) value that is computed from the username and password |
| **kerberos** | The adaptive security appliance responds by sending the username and realm using the Generic Security Services Application Programming Interface (GSSAPI) Kerberos mechanism |
| *server-group-name* | Specifies the Kerberos aaa-server group, up to 64 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 |
|---|---|
| `auto-detect` | Specifies that the adaptive security appliance determines the LDAP server type through autodetection. |
| `generic` | Specifies LDAPv3-compliant directory servers other than Sun and Microsoft LDAP directory servers. Password management is not supported with generic LDAP servers. |
| `microsoft` | Specifies that the LDAP server is a Microsoft Active Directory server. |
| `openldap` | Specifies that the LDAP server is an OpenLDAP server. |
| `novell` | Specifies that the LDAP server is a Novell server. |
| `sun` | Specifies that the LDAP server is a Sun Microsystems Java System Directory Server. |

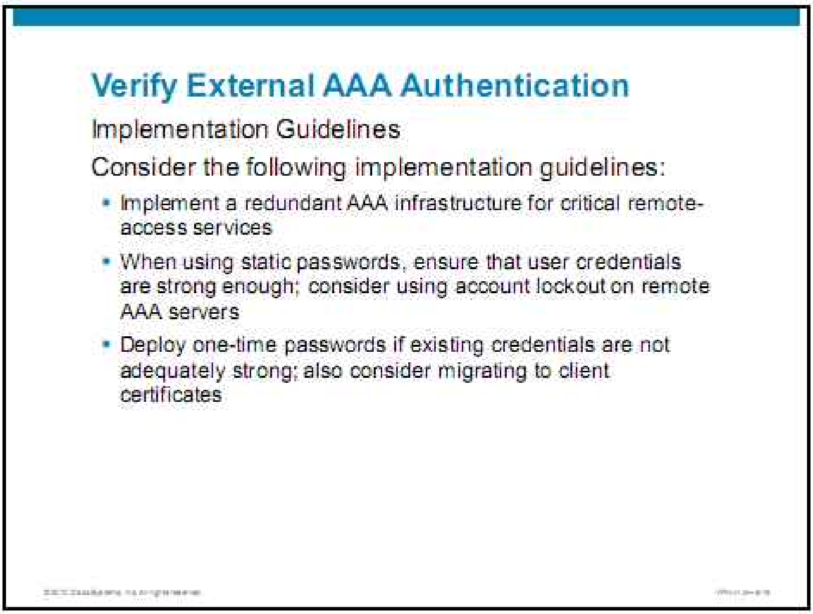
## authentication-server-group (tunnel-group general-attributes)

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 |
|---|---|
| *interface_name* | (Optional) Specifies the interface where the IP Security (IPsec) tunnel terminates. |
| `LOCAL` | (Optional) Requires authentication against the local user database if all of the servers in the server group have been deactivated due to communication failures. If the server group name is either LOCAL or NONE, do not use the **LOCAL** keyword here. |
| `NONE` | (Optional) Specifies the server group name as NONE, indicating that authentication is not required. |
| *server_group* | Identifies the previously configured authentication server or group of servers. |



## Verify External AAA Authentication

Implementation Guidelines

Consider the following implementation guidelines:

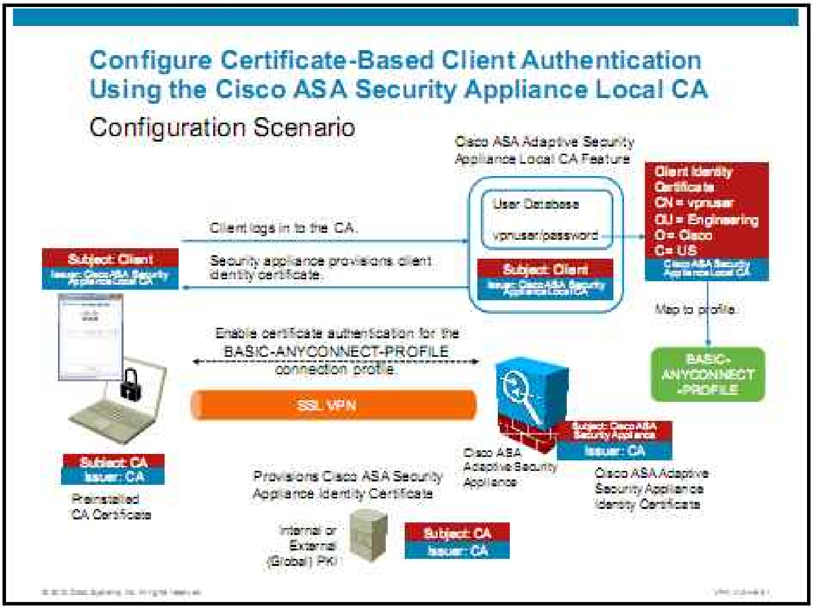
- Implement a redundant AAA infrastructure for critical remote-access services
- When using static passwords, ensure that user credentials are strong enough; consider using account lockout on remote AAA servers
- Deploy one-time passwords if existing credentials are not adequately strong; also consider migrating to client certificates

When implementing advanced password-based client authentication, consider the following implementation guidelines:

- Create redundant AAA infrastructure for critical remote access services
- When using static passwords, ensure that user credentials are strong enough; also consider using account lockout on remote AAA servers
- Deploy one-time passwords (OTPs) if existing credentials are not adequately strong; also consider migrating to client certificates

# Deploying Certificate-Based Client Authentication Using the Cisco ASA Adaptive Security Appliance Local CA

This topic describes how to configure and verify the local CA on the Cisco ASA adaptive security appliance and the Cisco AnyConnect client by using client certificates that are provisioned by the security appliance.



## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

Configuration Scenario

Cisco ASA Adaptive Security Appliance Local CA Feature
User Database
vpnuser/password
Client Identity Certificate
CN = vpnuser
OU = Engineering
O= Cisco
C= US
Cisco ASA Security Appliance Local CA
Client logs in to the CA.
Security appliance provisions client identity certificate.
Subject: Client
Issuer: Cisco ASA Security Appliance Local CA
Subject: Client
Issuer: Cisco ASA Security Appliance Local CA
Map to profile.
Enable certificate authentication for the BASIC-ANYCONNECT-PROFILE connection profile.
BASIC-ANYCONNECT-PROFILE
SSL VPN
Subject: Cisco ASA Security Appliance
Issuer: CA
Cisco ASA Adaptive Security Appliance
Cisco ASA Adaptive Security Appliance Identity Certificate
Subject: CA
Issuer: CA
Preinstalled CA Certificate
Provisions Cisco ASA Security Appliance Identity Certificate
Internal or External (Global) PKI
Subject: CA
Issuer: CA

When you configure certificate-based client authentication, you can configure the local certificate authority (CA) feature on the Cisco ASA adaptive security appliance. This local CA is capable of provisioning and managing identity certificates for clients. However, the local CA cannot issue an identity certificate to the Cisco ASA adaptive security appliance. That is why the security appliance has to obtain an identity certificate from an external PKI system. This identity certificate is signed by the external CA.

When you configure the local CA on the Cisco ASA adaptive security appliance, the appliance generates an additional self-signed certificate that is used to sign the identity certificates that are issued to the clients. When a client requests an identity certificate from the appliance, the appliance creates an identity certificate and signs it with its local CA root certificate. The identity certificate of the client can then be downloaded by the client. However, before a user can download its identity certificate from the Cisco ASA adaptive security appliance, you have to create user accounts on the appliance for users who will be eligible to obtain an identity certificate from the local CA of the security appliance.

When the client and the Cisco ASA adaptive security appliance want to establish an SSL VPN connection, they have to first exchange identity certificates. The security appliance sends a PKI-obtained identity certificate to the client. The client verifies the certificate of the Cisco ASA adaptive security appliance by using the certificate of the CA, which has to be installed on the client. The client also sends its identity certificate (which has been obtained from the Cisco ASA adaptive security appliance) to the security appliance. The appliance verifies the client identity certificate using its self-signed certificate, which was used to sign the identity certificate of the client in the first place. If both certificates can be verified, the client and the Cisco ASA adaptive security appliance establish the SSL VPN connection.

The figure shows an example that will serve as a configuration scenario for ongoing configuration tasks. First, you will configure a local CA on the Cisco ASA adaptive security appliance and create a user account for a user to download a certificate. Then, you will enable certificate-based authentication for the BASIC-ANYCONNECT-PROFILE. Lastly, you will configure mapping between the certificate and the connection profile to map users to the BASIC-ANYCONNECT-PROFILE connection profile.

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

Configuration Tasks

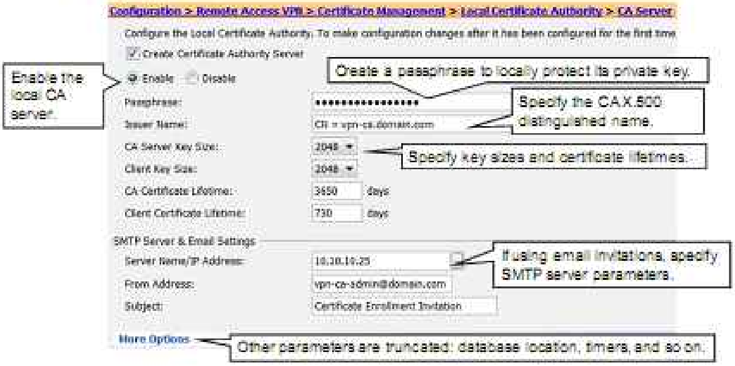
1. Configure the local CA of the Cisco ASA adaptive security appliance.
2. Create CA user accounts.
3. Provision client identity certificates.
4. Install a client certificate on the Cisco AnyConnect client.
5. Map certificates to connection profiles.
6. Enable client certificate authentication for a connection profile.

Perform these configuration tasks to configure certificate-based client authentication by using the local CA of the Cisco ASA adaptive security appliance:

1. Configure the Cisco ASA adaptive security appliance local CA.
2. Create CA user accounts.
3. Provision client identity certificates.
4. Install a client certificate on the Cisco AnyConnect VPN Client.
5. Map certificates to connection profiles.
6. Enable client certificate authentication for a connection profile.

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

Task 1: Configure the Local CA of the Cisco ASA Adaptive Security Appliance



Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server

Configure the Local Certificate Authority. To make configuration changes after it has been configured for the first time

☑ Create Certificate Authority Server

● Enable ○ Disable

Passphrase: ****************

Issuer Name: CN = vpn-ca.domain.com

CA Server Key Size: 2048

Client Key Size: 2048

CA Certificate Lifetime: 3650 days

Client Certificate Lifetime: 730 days

SMTP Server & Email Settings

Server Name/IP Address: 10.10.10.25

From Address: vpn-ca-admin@domain.com

Subject: Certificate Enrollment Invitation

More Options

Enable the local CA server.

Create a passphrase to locally protect its private key.

Specify the CA X.500 distinguished name.

Specify key sizes and certificate lifetimes.

If using email invitations, specify SMTP server parameters.

Other parameters are truncated: database location, timers, and so on.

Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA

To configure the Cisco ASA adaptive security appliance local CA by using Cisco ASDM, complete the following steps:

**Step 1** Inside the ASDM, choose **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server** (not shown in the figure). The CA Server panel is displayed.

**Step 2** Check the **Create Certificate Authority Server** check box.

**Step 3** Click the **Enable** radio button to activate the local CA server. The default is disabled. After you enable the local CA server, the security appliance generates the local CA server certificate, key pair, and necessary database files. It then archives the local CA server certificate and key pair in a Public Key Cryptography Standard #12 (PKCS12) file.

**Step 4** When you enable the local CA for the first time, you must provide an alphanumeric enable passphrase, which must have a minimum of seven alphanumeric characters. The passphrase protects the local CA certificate and the local CA certificate key pair that is archived in storage. It also secures the local CA server from unauthorized or accidental shutdown. The passphrase is required to unlock the PKCS12 archive if the local CA certificate or key pair is lost and must be restored.

**Step 5** Enter the issuer subject name into the Issuer Name input field in CN=FQDN format. By default, this field is populated with CN=hostname.domain_name.

**Step 6** From the CA Server Key Size drop-down list, choose the CA server key size of the key pair to be generated for the CA certificate. Key sizes can be 512, 768, 1024, or 2048 bits per key. The default is 1024 bits per key.

**Step 7** From the Client Key Size drop-down list, choose the client key size of the key pair to be generated for each user certificate that is issued by the local CA server. Key sizes can be 512, 768, 1024, or 2048 bits per key. The default is 1024 bits per key.

**Step 8** Enter the CA certificate lifetime value into the CA Certificate Lifetime input field. This value specifies the number of days that the CA server certificate is valid. The default is 3650 days (10 years).

**Step 9** Enter the client certificate lifetime value into the Client Certificate Lifetime input field. This value specifies the number of days that a user certificate that is issued by the CA server is valid. The default is 365 days (1 year).

**Step 10** In the Simple Mail Transfer Protocol (SMTP) Server & Email Settings area, you set up email access for the local CA server by specifying the settings that follow. Local CA needs email access if you want to send email notifications with instructions on how to obtain an identity certificate to users. Complete the following substeps to set up email access:

- Enter the SMTP mail server name or IP address. Alternatively, click the ellipsis (**...**) to display the Browse Server Name/IP Address dialog box, where you can choose the server name or IP address. Click **OK** when you are finished to close the Browse Server Name/IP Address dialog box.
- Enter the address from which to send email messages to local CA users, in adminname@host.com format. Automatic email messages carry OTPs to newly enrolled users and issue email messages when certificates need to be renewed or updated.
- Enter the subject, which specifies the subject line in all messages that are sent to users by the local CA server. If you do not specify a subject, the default is Certificate Enrollment Invitation.

**Step 11** Optionally, configure additional options by clicking the **More Options** drop-down bar (not shown in the figure).

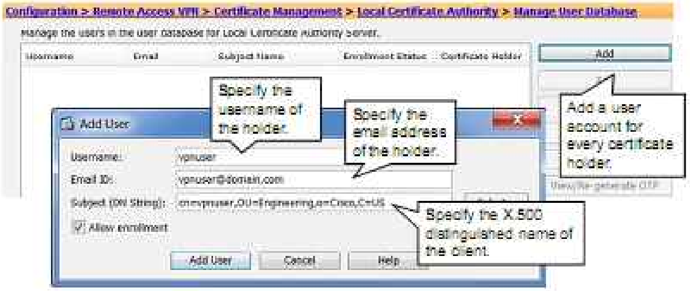
**Step 12** Optionally, enter the certificate revocation list (CRL) distribution point location into the CRL Distribution Point URL input field. The default location is http://hostname.domain/+CSCOCA+/asa_ca.crl (not shown in the figure).

**Step 13** Optionally, specify CA database storage by entering a database storage location into the Database Storage Location input field. The security appliance accesses and implements user information, issued certificates, and revocation lists by using a local CA database. Alternatively, to specify an external file, enter the pathname to the external file or click **Browse** to display the Database Storage Location dialog box (not shown in the figure.)

**Step 14** Click **Apply** to apply the configuration.

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Task 2: Create CA User Accounts



Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

Manage the users in the user database for Local Certificate Authority Server.

Add User

Username: vpnuser

Email ID: vpnuser@domain.com

Subject (DN String): cn=vpnuser,OU=Engineering,o=Cisco,C=US

☑ Allow enrollment

Specify the username of the holder.

Specify the email address of the holder.

Add a user account for every certificate holder.

Specify the X.500 distinguished name of the client.

Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

When you are finished creating the local CA, you have to create user accounts on the Cisco ASA adaptive security appliance for all users who are eligible to obtain a certificate from the Cisco ASA adaptive security appliance. To create a user account on the local CA using Cisco ASDM, complete the following steps:

**Step 1** Inside the ASDM, choose **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database** (not shown in the figure). The Manage User Database panel is displayed.

**Step 2** Click **Add** in the Manage User Database panel. The Add User window opens.

**Step 3** Enter a valid username into the Username input field.

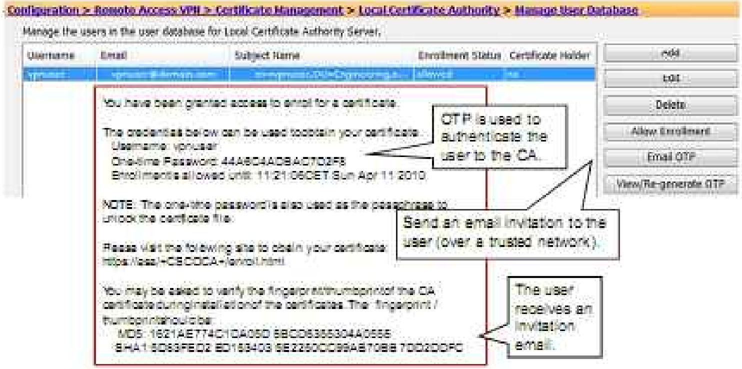
**Step 4** Enter the email address of a user into the Email ID input field.

**Step 5** Enter the subject name into the Subject (DN String) input field. This name will be used in a certificate as a subject name.

**Step 6** Click **Add User**.

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Task 3A: Provision Client Identity Certificates (Email)



Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

Manage the users in the user database for Local Certificate Authority Server.

| Username | Email | Subject Name | Enrollment Status | Certificate Holder |
|---|---|---|---|---|
| vpnuser | vpnuser@domain.com | cn=vpnuser,OU=Engineering,... | allowed | no |

You have been granted access to enroll for a certificate.

The credentials below can be used toobtain your certificate.
Username: vpnuser
One-time Password: 44A6C4ADBAC7D2F8
Enrollment is allowed until: 11:21:06CET Sun Apr 11 2010

NOTE: The one-time password is also used as the passphrase to unlock the certificate file.

Please visit the following site to obtain your certificate:
https://asa/+CSCOCA+/enroll.html

You may be asked to verify the fingerprint/thumbprint of the CA certificate during installation of the certificates. The fingerprint / thumbprint should be:
MD5: 1621AE774C1DA05D 5BCD6356304A0556
SHA1: 6D63FED2 ED183403 5E2250CC99A570B8 7DD2DDFC

OTP is used to authenticate the user to the CA.

Send an email invitation to the user (over a trusted network).

The user receives an invitation email.

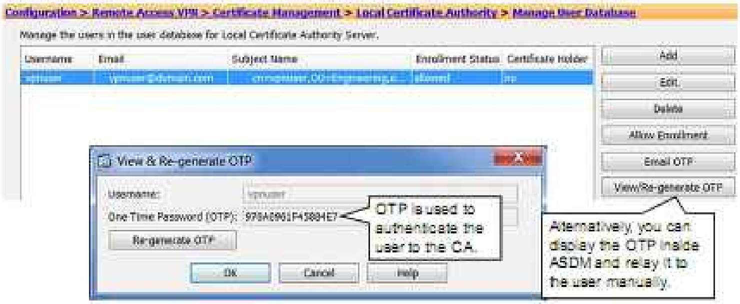
Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Certificates

When you are finished with creating user accounts, a user can obtain a certificate using a web browser or the Cisco AnyConnect client. When a user wants to connect to the Cisco ASA adaptive security appliance by using the Cisco AnyConnect client, and a certificate is needed, the user will get an option to download the certificate. Before downloading the certificate, the user has to authenticate to the Cisco ASA adaptive security appliance by using a username (defined in the previous task when creating user accounts on the local CA) and an OTP, which are generated by the security appliance. A user can be notified about the username and OTP in two different ways. The first way is to allow the Cisco ASA adaptive security appliance to send an email notification to the user. Click the **Email OTP** button in the Manage User Database panel to send an email notification to the user. An example of the email notification that is composed and sent to the user is shown in the figure.

**Note** You have to configure email settings in the SMTP Server & Email Settings area of the CA Server panel in order for the Cisco ASA adaptive security appliance to send email notifications.

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Task 3B: Provision Client Identity Certificates (Out-of-Band)



Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

Manage the users in the user database for Local Certificate Authority Server.

| Username | Email | Subject Name | Enrollment Status | Certificate Holder |
|---|---|---|---|---|
| vpnuser | vpnuser@domain.com | cn=vpnuser,OU=Engineering,c... | allowed | no |

Username: vpnuser

One Time Password (OTP): 970A0901F45884E7

OTP is used to authenticate the user to the CA.

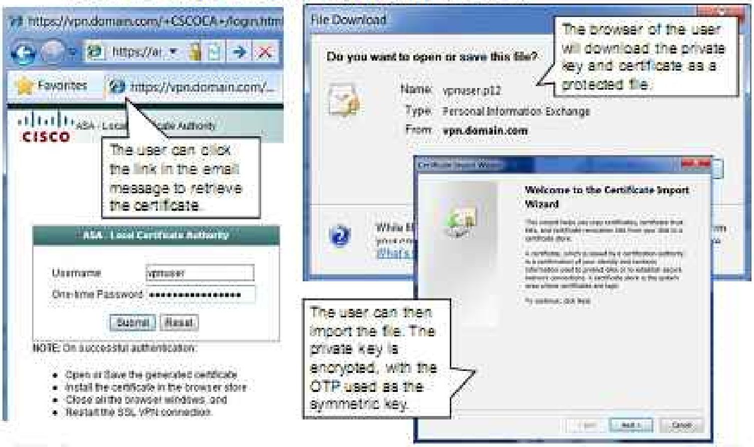
Alternatively, you can display the OTP inside ASDM and relay it to the user manually.

Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Certificates

Another way to notify the user about the username and OTP is to relay the username and OTP to the user manually (for example, using a phone). Choose a user from the username table and click the **Verify/Re-generate OTP** button to display the OTP for that specific user. You can then cut and paste the OTP and relay it to the user by using other communication channels.

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

Task 4A: Install Client Certificate (Portal)



https://vpn.domain.com/+CSCOCA+/login.html

ASA - Local Certificate Authority

Username: vpnuser

One-time Password: ••••••••••••••••

NOTE: On successful authentication:

- Open or Save the generated certificate
- Install the certificate in the browser store
- Close all the browser windows, and
- Restart the SSL VPN connection.

File Download

Do you want to open or save this file?

Name: vpnuser.p12

Type: Personal Information Exchange

From: vpn.domain.com

Welcome to the Certificate Import Wizard

The user can click the link in the email message to retrieve the certificate.

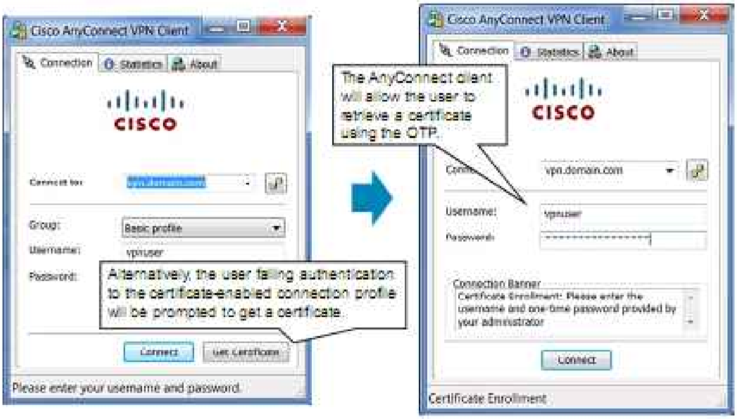
The browser of the user will download the private key and certificate as a protected file.

The user can then import the file. The private key is encrypted, with the OTP used as the symmetric key.

The figure shows a procedure for how a user can obtain a certificate. If you decided to notify a user by using an email notification, the user can click the link in the email. A web page will open where the user has to enter a username and OTP. When the user enters the correct username and password, the certificate will be downloaded. After the user installs the certificate into the appropriate certificate store, the user can authenticate to the Cisco ASA adaptive security appliance by using the certificate.

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Task 4B: Install Client Certificate (Cisco AnyConnect)



Connect to: vpn.domain.com

Group: Basic profile

Username: vpnuser

Password:

Please enter your username and password.

Alternatively, the user failing authentication to the certificate-enabled connection profile will be prompted to get a certificate.

The AnyConnect client will allow the user to retrieve a certificate using the OTP.

Connect to: vpn.domain.com

Username: vpnuser

Password: ••••••••••••••••

Connection Banner

Certificate Enrollment: Please enter the username and one-time password provided by your administrator

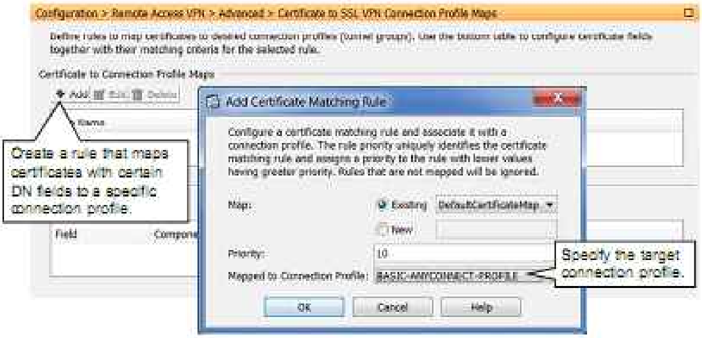
Certificate Enrollment

A user can also download a certificate by using the Cisco AnyConnect client. If a certificate is required for a connection profile and a user does not have one, the Cisco AnyConnect client will display a Get Certificate button. When the user clicks the button, the Cisco AnyConnect window content changes. A user can then retrieve a certificate by entering a username and OTP and by clicking the Connect button. After the user clicks the Connect button, the certificate will be downloaded and installed automatically into the appropriate certificate store. At that point, an SSL connection will establish automatically.

| | |
|---|---|
| **Note** | Before a user can download a certificate using the Cisco AnyConnect client, you have to enable certificate-based authentication for a specific connection profile. This process is shown in the next, fourth task. |

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Task 5: Map Certificates to Connection Profiles



Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps

Define rules to map certificates to desired connection profiles (tunnel groups). Use the bottom table to configure certificate fields together with their matching criteria for the selected rule.

Certificate to Connection Profile Maps

Add Certificate Matching Rule

Configure a certificate matching rule and associate it with a connection profile. The rule priority uniquely identifies the certificate matching rule and assigns a priority to the rule with lesser values having greater priority. Rules that are not mapped will be ignored.

Map: ● Existing DefaultCertificateMap ○ New

Priority: 10

Mapped to Connection Profile: BASIC-ANYCONNECT-PROFILE

Create a rule that maps certificates with certain DN fields to a specific connection profile.

Specify the target connection profile.

Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps

In this task, you will enable certificate-based authentication for a connection profile. You will first configure mapping between certificates and a connection profile to enable the Cisco ASA adaptive security appliance to use the proper connection profile for users who are authenticating with a certificate. When the Cisco AnyConnect client is establishing a connection with the Cisco ASA adaptive security appliance, the Cisco AnyConnect client immediately tries to authenticate to the security appliance with the client identity certificate that is found in a certificate store (if there is one). The Cisco ASA adaptive security appliance can use the proper connection profile for that user based on the subject attributes in the received client identity certificate.

To configure certificate-to-connection-profile mapping by using Cisco ASDM, complete the following steps:

**Step 1** Inside the 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** Choose an existing map from the map drop-down menu.

**Step 3** Alternatively, click the **New** radio button in the Map area and provide a name for the connection profile map.

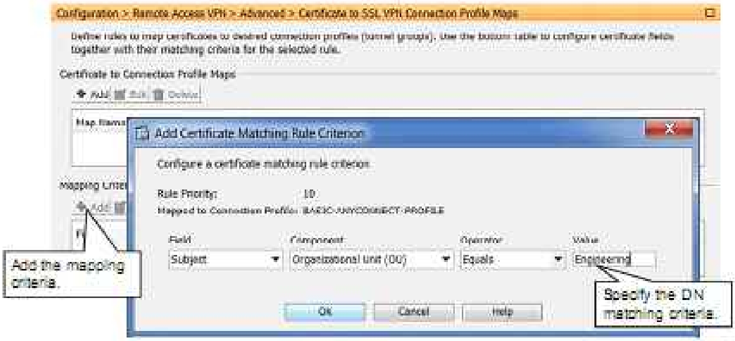
**Step 4** Configure the rule priority by entering a value into the Priority input field. A rule with a lower priority number will be consulted before a rule with a higher priority number.

**Step 5** Choose the desired connection profile from the Mapped to Connection Profile drop-down menu. In the example, BASIC-ANYCONNECT-PROFILE is chosen.

**Step 6** Click **OK** to accept the profile map.

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Task 5: Map Certificates to Connection Profiles (Cont.)



Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps

Define rules to map certificates to desired connection profiles (tunnel groups). Use the bottom table to configure certificate fields together with their matching criteria for the selected rule.

Certificate to Connection Profile Maps

Add Certificate Matching Rule Criterion

Configure a certificate matching rule criterion

Rule Priority: 10

Mapped to Connection Profile: BASIC-ANYCONNECT-PROFILE

Field: Subject

Component: Organizational Unit (OU)

Operator: Equals

Value: Engineering

Add the mapping criteria.

Specify the DN matching criteria.

Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps

After the profile map has been configured, configure the rule criterion to identify to the Cisco ASA adaptive security appliance what will be used to map the connecting users to the desired connection profile.

**Step 1** At the same Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps submenu, click the **Add** button under the Mapping Criteria area.

**Step 2** Configure the **Field**, **Component**, **Operator**, and **Value** fields for the mapping criteria. Click **OK** to accept the changes.

The following items can be selected under the Mapping Criteria:

- **Field:** From the drop-down list, choose the part of the certificate that you want to evaluate.
  - **Subject:** The person or system that uses the certificate. For a CA root certificate, the subject and issuer are the same.
  - **Alternative Subject:** The alternative subject 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 component 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 name or names of a subject as an unstructured ASCII string.
- **IP Address (IP):** IP address field.

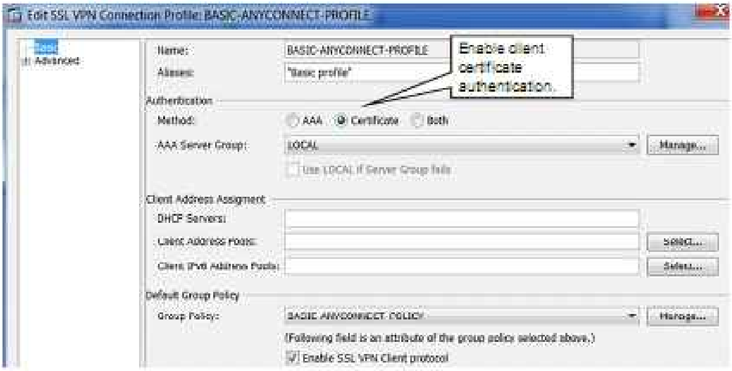
- **Operator:** Choose the operator that is used in the rule:
  - **Equals:** The distinguished name field must exactly match the value.
  - **Contains:** The distinguished name field must include the value within it.
  - **Does Not Equal:** The distinguished name field must not match the value.
  - **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 organizational unit field of a certificate contains the "Engineering" string, a user with that certificate will be mapped to the BASIC-ANYCONNECT-PROFILE connection profile.

**Step 3** Click **Apply** to apply the configuration.

## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Task 6: Enable Certificate Authentication in Connection Profile



Edit SSL VPN Connection Profile: BASIC-ANYCONNECT-PROFILE

Name: BASIC-ANYCONNECT-PROFILE

Aliases: "Basic profile"

Authentication

Method: ○ AAA ● Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: BASIC-ANYCONNECT-POLICY

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN Client protocol

Enable client certificate authentication.

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

Finally, you have to enable certificate-based authentication for a specific connection profile. To enable client-based authentication for a specific connection profile by using Cisco ASDM, complete the following steps:

**Step 1** Inside the ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. The AnyConnect Connection Profiles window is displayed (not shown in the figure).

**Step 2** Choose a connection profile from the Connection Profiles table and click **Edit**. In the example, the BASIC-ANYCONNECT-PROFILE has been selected (not shown in the figure). The Edit SSL VPN Connection Profile window is displayed.

**Step 3** Click the **Certificate** radio button in the Authentication section of the window.

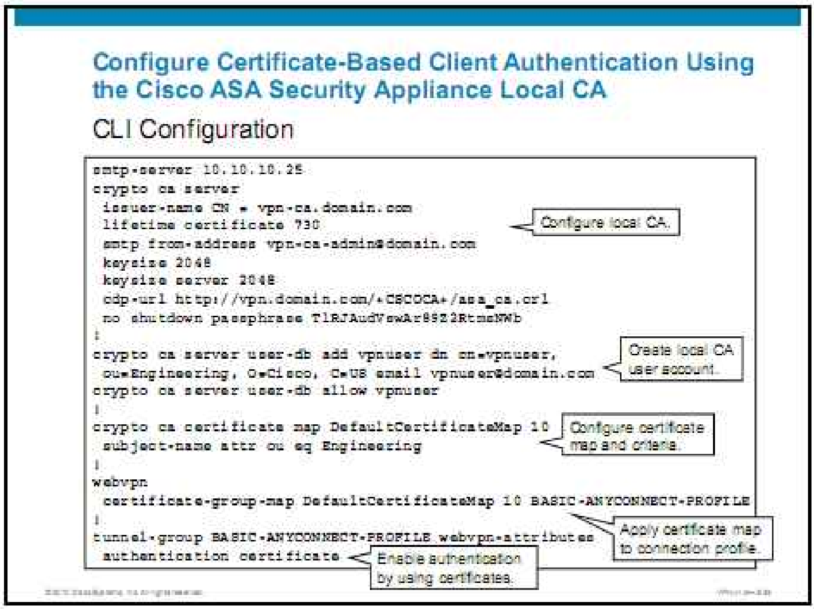
**Step 4** Click **OK**.

**Step 5** Click **Apply** to apply the configuration.

---

**Note** The Cisco ASA adaptive security appliance has supported certificate authentication per connection profile since the Cisco ASA Software Release 8.2(1).

---



## Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

CLI Configuration

```
smtp-server 10.10.10.25
crypto ca server
 issuer-name CN = vpn-ca.domain.com
 lifetime certificate 730
 smtp from-address vpn-ca-admin@domain.com
 keysize 2048
 keysize server 2048
 cdp-url http://vpn.domain.com/+CSCOCA+/asa_ca.crl
 no shutdown passphrase T1RJAudVswAr8522RtmsNWb
!
crypto ca server user-db add vpnuser dn cn=vpnuser,
 ou=Engineering, O=Cisco, C=US email vpnuser@domain.com
crypto ca server user-db allow vpnuser
!
crypto ca certificate map DefaultCertificateMap 10
 subject-name attr ou eq Engineering
!
webvpn
 certificate-group-map DefaultCertificateMap 10 BASIC-ANYCONNECT-PROFILE
!
tunnel-group BASIC-ANYCONNECT-PROFILE webvpn-attributes
 authentication certificate
```

Configure local CA.

Create local CA user account.

Configure certificate map and criteria.

Apply certificate map to connection profile.

Enable authentication by using certificates.

To use the CLI to configure certificate-based authentication using the local CA, use the following commands. To configure the SMTP server that is used to send email notification, use the **SMTP-server** command. To enable the local CA server, first use the **crypto ca server** to enter CA server configuration mode. Inside CA server configuration mode, configure the CA name by using the **issuer-name** command. Specify the lifetime of issued certificates by using the **lifetime certificate** command. Use the **smtp from-address** command to specify the email address that the Cisco ASA adaptive security appliance will use as a from address to send email notifications with certificate download instructions. Specify the size of the key that is used for the CA certificate and the size of the key that is used for the certificates of clients by using the **keysize server** and **keysize** commands, respectively. Specify the CRL distribution point that will be included in certificates using the **cdp-url** command. Finally, enable the local CA server by using the **no shutdown** command, followed by a **passphrase** keyword and a password to protect the CA certificate and key pair archive.

To create user accounts for users who are eligible to obtain a certificate, use the **crypto ca server user-db add** command, followed by the DN and email address of the user. To allow a user to obtain a certificate, use the **crypto ca sever user-db allow** command.

To create a certificate-to-connection-profile mapping using the CLI, use the following commands. First, create a certificate-to-connection-profile map by using the **crypto ca certificate map** command, followed by a name and rule priority number. Then use the **subject-name atrr** 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. In the example, if the Cisco ASA adaptive security appliance receives a certificate where the organizational unit field of a subject name contains "Engineering," the Cisco ASA adaptive security appliance will use the BASIC-CONNECTION-PROFILE connection profile for that user.

Finally, enable certificate-based authentication for a specific connection profile (tunnel group) using the **authentication certificate** command in tunnel group configuration mode.

## smtp-server

To configure an SMTP server, use the **smtp-server** command in global configuration mode. To remove the attribute from the configuration, use the **no** form of this command.

**smtp-server** {*primary_server*} [*backup_server*]

### smtp-server Parameters

| Parameter | Description |
|---|---|
| *backup_server* | Identifies a backup SMTP server to relay event messages if the primary SMTP server is unavailable. Use either an IP address or DNS name. |
| *primary_server* | Identifies the primary SMTP server. Use either an IP address or DNS name. |

## issuer-name

To specify the issuer name DN of all issued certificates, use the **issuer-name** command in local CA server configuration mode. To remove the subject DN from the certificate authority certificate, use the **no** form of this command.

**issuer-name** *DN-string*

### issuer-name Parameters

| Parameter | Description |
|---|---|
| *DN-string* | Specifies the distinguished name of the certificate, which is also the subject name DN of the self-signed CA certificate. Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains a comma. An issuer name must be less than 500 alphanumeric characters. |

## lifetime (ca server mode)

To specify the length of time that the local CA certificate, each issued user certificate, or the certificate revocation list (CRL) is valid, use the **lifetime** command in CA server configuration mode. To reset the lifetime to the default setting, use the **no** form of this command.

**lifetime** {**ca-certificate** | **certificate** | **crl**} *time*

### lifetime (ca server mode) Parameters

| Parameter | Description |
|---|---|
| **ca-certificate** | Specifies the lifetime of the local CA server certificate. |
| **certificate** | Specifies the lifetime of all user certificates that are issued by the CA server. |
| **crl** | Specifies the lifetime of the CRL. |
| *time* | For the CA certificate and all issued certificates, *time* specifies the number of days that the certificate is valid. The valid range is from 1 to 3650 days.<br>For the CRL, *time* specifies the number of hours that the CRL is valid. The valid range for the CRL is from 1 to 720 hr. |

## smtp from-address

To specify the email address to use in the E-mail From field for all emails that are generated by the local CA server (such as distribution of OTPs), use the **smtp from-address** command in CA server configuration mode. To reset the email address to the default, use the **no** form of this command.

**smtp from-address** *e-mail_address*

### smtp from-address Parameters

| Parameter | Description |
|---|---|
| *e-mail_address* | Specifies the email address that appears in the Email From field of all emails that are generated by the CA server. |

## keysize

To specify the size of the public and private keys that are generated by the local CA server at user certificate enrollment, use the **keysize** command in CA server configuration mode. To reset the key size to the default length of 1024 bits, use the **no** form of this command.

**keysize** {**512** | **768** | **1024** | **2048**}

### keysize Parameters

| Parameter | Description |
|---|---|
| 512 | Specifies a size of 512 bits for the public and private keys that are generated at certificate enrollment |
| 768 | Specifies a size of 768 bits for the public and private keys that are generated at certificate enrollment |
| 1024 | Specifies a size of 1024 bits for the public and private keys that are generated at certificate enrollment |
| 2048 | Specifies a size of 2048 bits for the public and private keys that are generated at certificate enrollment |

## keysize server

To specify the size of the public and private keys that are generated by the local CA server to configure the size of the key pair of the CA, use the **keysize server** command in CA server configuration mode. To reset the key size to the default length of 1024 bits, use the **no** form of this command.

**keysize server**{**512** | **768** | **1024** | **2048**}

### keysize server Parameters

| Parameter | Description |
|---|---|
| 512 | Specifies a size of 512 bits for the public and private keys that are generated at certificate enrollment |
| 768 | Specifies a size of 768 bits for the public and private keys that are generated at certificate enrollment |
| 1024 | Specifies a size of 1024 bits for the public and private keys that are generated at certificate enrollment |
| 2048 | Specifies a size of 2048 bits for the public and private keys that are generated at certificate enrollment |

## cdp-url

To specify the CRL distribution point (CDP) to be included in certificates that are issued by the local CA, use the **cdp-url** command in CA server configuration mode. To revert to the default CDP, use the **no** form of this command.

**[no] cdp-url** *url*

### cdp-url Parameters

| Parameter | Description |
|---|---|
| *url* | Specifies the URL where a validating party obtains revocation status for certificates that are issued by the local CA. The URL must be fewer than 500 alphanumeric characters. |

## shutdown (ca-server mode)

To disable the local CA server and render the enrollment interface inaccessible to users, use the **shutdown** command in CA server configuration mode. To enable the CA server, lock down the configuration from changes, and render the enrollment interface accessible, use the **no** form of this command.

[**no**] **shutdown**

## crypto ca server user-db add

To insert a new user into the CA server user database, use the **crypto ca server user-db add** command in privileged EXEC mode.

**crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*]

### crypto ca server user-db add Parameters

| Parameter | Description |
|---|---|
| **dn** *dn* | Specifies a subject name distinguished name for certificates that are issued to the added user. If a DN string contains a comma, enclose the value string with double quotes (for example, O="Company, Inc."). |
| **email** *e-mail-address* | Specifies the email address for the new user. |
| *user* | Specifies a single user to whom enrollment privileges may be granted. The username can be a simple username or an email address. |

## crypto ca server user-db allow

To permit a user or a group of users to enroll in the local CA server database, use the **crypto ca server user-db allow** command in privileged EXEC mode. This command also includes options to generate and display OTPs or to email them to the users.

**crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp** ]

### crypto ca server user-db allow Parameters

| Parameter | Description |
|---|---|
| `all-certholders` | Specifies that enrollment privileges be granted to all users in the database who have been issued a certificate, whether the certificate is currently valid or not. This specification is equivalent to granting renewal privileges. |
| `all-unenrolled` | Specifies that enrollment privileges be granted to all users in the database who have not been issued a certificate. |
| `email-otp` | (Optional) Sends the specified users OTPs by email to their configured email addresses. |
| `replace-otp` | (Optional) Specifies that OTPs be regenerated for all specified users who originally had valid OTPs. |
| `display-otp` | (Optional) Displays the OTPs for all specified users to the console. |
| *`username`* | Specifies a single user to whom enrollment privileges may be granted. The username can be a simple username or an email address. |

## crypto ca certificate map

To enter CA certificate map mode, use the **crypto ca certificate map** command in global configuration mode. Executing this command places you in CA certificate map mode. Use this group of commands to maintain a prioritized list of certificate mapping rules. The sequence number orders the mapping rules. To remove a crypto CA certificate map rule, use the **no** form of the command.

**crypto ca certificate map** {*sequence-number* | *map-name sequence-number*}

### crypto ca certificate map Parameters

| Parameter | Description |
|---|---|
| *`map-name`* | Specifies a name for a certificate-to-group map. |
| *`sequence-number`* | Specifies a number for the certificate map rule that you are creating. The range is 1 through 65,535. You can use this number when creating a tunnel group map, which maps a tunnel group to a certificate map rule. |

## subject-name (crypto ca certificate map)

To indicate that a rule entry is applied to the subject DN of the IPsec peer certificate, use the **subject-name** command in crypto CA certificate map configuration mode. To remove a subject name, use the **no** form of the command.

**subject-name** [**attr** *tag* **eq** | **ne** | **co** | **nc** *string*]

### subject-name (crypto ca certificate map) Parameters

| Parameter | Description |
|---|---|
| **attr** *tag* | Indicates that only the specified attribute value from the certificate DN will be compared to the rule entry string. The tag values are as follows:<br>■ C = Country<br>■ CN = Common name<br>■ DNQ = DN qualifier<br>■ EA = Email address<br>■ GENQ = Generational qualifier<br>■ GN = Given name<br>■ I = Initials<br>■ IP = IP address<br>■ L = Locality<br>■ N = Name<br>■ O = Organization name<br>■ OU = Organizational unit<br>■ SER = Serial number<br>■ SN = Surname<br>■ SP = State/Province<br>■ T = Title<br>■ UNAME = Unstructured name |
| **co** | Specifies that the rule entry string must be a substring in the DN string or indicated attribute. |
| **eq** | Specifies that the DN string or indicated attribute must match the entire rule string. |
| **nc** | Specifies that the rule entry string must not be a substring in the DN string or indicated attribute. |
| **ne** | Specifies that the DN string or indicated attribute must not match the entire rule string. |
| *string* | Specifies the value to be matched. |

## certificate-group-map

To associate a rule entry from a certificate map with a tunnel group, use the **certificate-group-map** command in webvpn configuration mode. To clear current tunnel group map associations, use the **no** form of this command.

**certificate-group-map** *certificate_map_name index tunnel_group_name*

### certificate-group-map Parameters

| Parameter | Description |
|---|---|
| *certificate_map_name* | The name of a certificate map. |
| *index* | The numeric identifier for a map entry in the certificate map. The index value can be range from 1 to 65,535. |
| *tunnel_group_name* | The name of the tunnel group that is chosen if the map entry matches the certificate. The tunnel group name must already exist. |

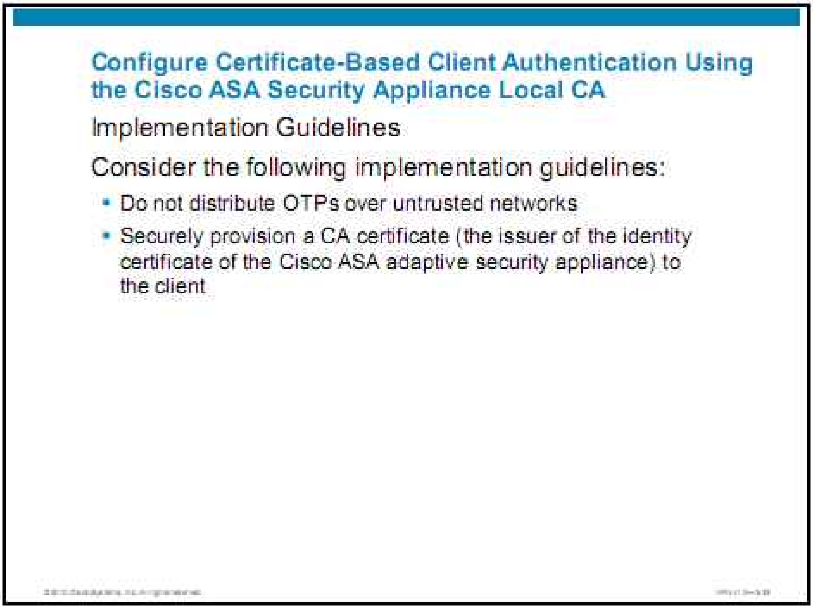
## authentication-certificate

To request a certificate from a WebVPN client that is establishing a connection, use the **authentication-certificate** command in webvpn configuration mode. To cancel the requirement for a client certificate, use the **no** form of this command.

**authentication-certificate** *interface-name*

### authentication-certificate Parameters

| Parameter | Description |
|---|---|
| *interface-name* | The name of the interface that is used to establish the connection. Available interfaces names include the following:<br>■ **Inside:** Name of interface GigabitEthernet 0/1<br>■ **Outside:** Name of interface GigabitEthernet 0/0 |



Configure Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

Implementation Guidelines

Consider the following implementation guidelines:

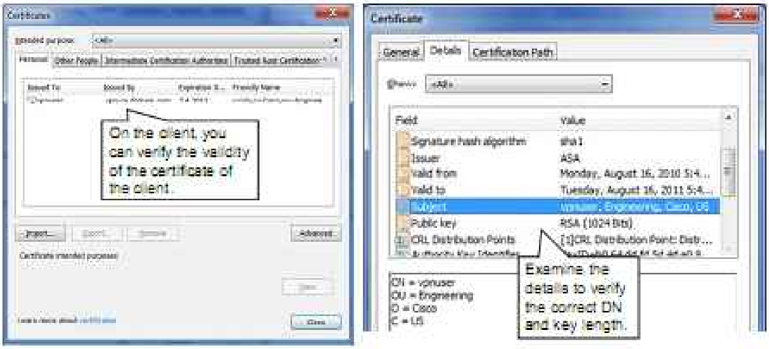
- Do not distribute OTPs over untrusted networks
- Securely provision a CA certificate (the issuer of the identity certificate of the Cisco ASA adaptive security appliance) to the client

When implementing certificate-based authentication, consider the following implementation guidelines:

- Ensure that you do not distribute OTPs that are needed to obtain the client identity certificates, over untrusted networks.
- The local CA is capable of provisioning and managing identity certificates for clients. However, the local CA cannot issue an identity certificate to the Cisco ASA adaptive security appliance. That is why the security appliance has to obtain an identity certificate from an external PKI system. This identity certificate is signed by the external CA. For the client to authenticate the Cisco ASA adaptive security appliance, you must still securely provision a CA certificate (the issuer of the identity certificate of the security appliance) to the client.

## Verify Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Verify Client Certificates



| Field | Value |
|---|---|
| Signature hash algorithm | sha1 |
| Issuer | ASA |
| Valid from | Monday, August 16, 2010 5:4... |
| Valid to | Tuesday, August 16, 2011 5:4... |
| Subject | vpnuser, Engineering, Cisco, US |
| Public key | RSA (1024 Bits) |
| CRL Distribution Points | [1]CRL Distribution Point: Distr... |

CN = vpnuser
OU = Engineering
O = Cisco
C = US

On the client, you can verify the validity of the certificate of the client.

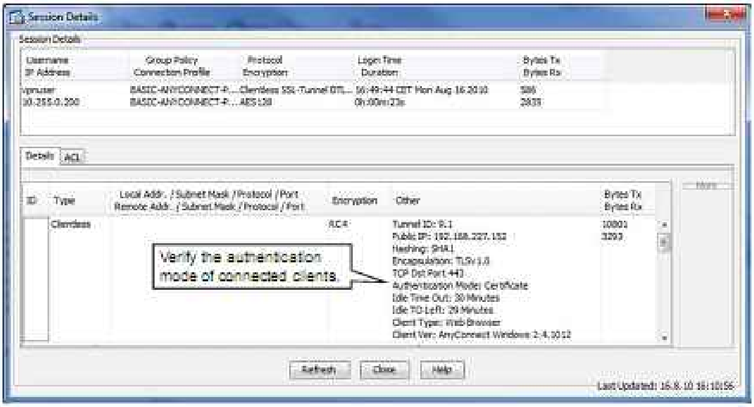
Examine the details to verify the correct DN and key length.

Internet Explorer > Tools > Internet Options > Content > Certificates

You can verify obtained client certificates by choosing **Tools > Internet Options > Content > Certificates** in Internet Explorer. A Certificates window is displayed where you can review your certificates. In the example, you can see in the certificate store that there is a certificate that is issued to vpnuser. You can verify the details of the certificate, such as certificate validity, DN, and key length, by double-clicking the certificate.

## Verify Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Verify Authentication Policy



Session Details

| Username<br>IP Address | Group Policy<br>Connection Profile | Protocol<br>Encryption | Login Time<br>Duration | Bytes Tx<br>Bytes Rx |
|---|---|---|---|---|
| vpnuser<br>10.255.0.200 | BASIC-ANYCONNECT-P...<br>BASIC-ANYCONNECT-P... | Clientless SSL-Tunnel DTL...<br>AES128 | 16:49:44 CET Mon Aug 16 2010<br>0h:00m:23s | 586<br>2835 |

| ID | Type | Local Addr. / Subnet Mask / Protocol / Port<br>Remote Addr. / Subnet Mask / Protocol / Port | Encryption | Other | Bytes Tx<br>Bytes Rx |
|---|---|---|---|---|---|
|  | Clientless |  | RC4 | Tunnel ID: 9.1<br>Public IP: 192.168.227.152<br>Hashing: SHA1<br>Encapsulation: TLSv1.0<br>TCP Dst Port: 443<br>Authentication Mode: Certificate<br>Idle Time Out: 30 Minutes<br>Idle TO Left: 29 Minutes<br>Client Type: Web Browser<br>Client Ver: AnyConnect Windows 2.4.1012 | 10801<br>3293 |

Verify the authentication mode of connected clients.

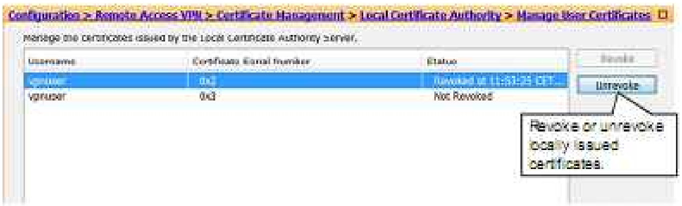
Last Updated: 16.8.10 16:10:56

Monitoring > VPN > VPN Statistics > Sessions > Details

To verify established SSL Cisco AnyConnect sessions using the Cisco ASDM, choose **Monitoring > VPN > VPN Statistics > Sessions** (not shown in the figure). Choose the SSL VPN Client option from the Filter By drop-down menu to show SSL Cisco AnyConnect connections (not shown in the figure). Select a specific connection from the table and click the **Details** button (not shown in the figure). The Session Details window is displayed. In the Session Details section of the window, verify which connection profile is used for the connection. In the example, the BASIC-ANYCONNECT-PROFILE is used for the connection. Click the Details tab to verify that certificates are used for authentication.

## Verify Certificate-Based Client Authentication Using the Cisco ASA Security Appliance Local CA

### Manage Certificates



Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Certificates

Manage the certificates issued by the Local Certificate Authority Server.

| Username | Certificate Serial Number | Status |
|---|---|---|
| vpnuser | 0x2 | Revoked at 11:53:25 CET... |
| vpnuser | 0x3 | Not Revoked |

Revoke or unrevoke locally issued certificates.

```
crypto ca server revoke cert-serial-no
```

Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Certificates

When using the Cisco ASA adaptive security appliance as a local CA, you can use Cisco ASDM to manage certificates that are issued to a client. The management of certificates includes revoking and unrevoking of the certificates of users. To revoke or unrevoke a certificate using Cisco ASDM, complete the following steps:

**Step 1** Inside the ASDM, choose **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Certificates**.

**Step 2** Select a certificate from the table.

**Step 3** Click the **Revoke** button to revoke the certificate.

**Step 4** Click the **Unrevoke** button to unrevoke a revoked certificate.

To revoke a certificate using the CLI, use the **crypto ca server revoke** command, followed by the certificate serial number.

To unrevoke a certificate, use the **crypto ca server unrevoked** command, followed by the certificate serial number.

## crypto ca server revoke

To mark a certificate that is issued by the local CA server as revoked in the certificate database and the CRL, use the **crypto ca server revoke** command in privileged EXEC mode.

**crypto ca server revoke** *cert-serial-no*

### crypto ca server revoke Parameters

| Parameter | Description |
|---|---|
| `cert-serial-no` | Specifies the serial number of the certificate to be revoked. Enter the serial number in hexadecimal format. |

## crypto ca server unrevoke

To unrevoke a previously revoked certificate that is issued by the local CA server, use the **crypto ca server unrevoke** command in privileged EXEC mode.

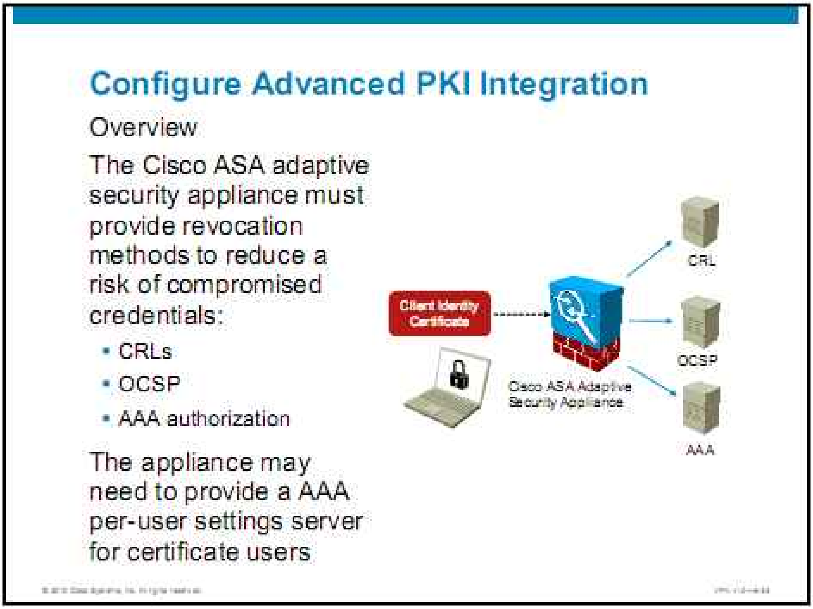
**crypto ca server unrevoke** *cert-serial-no*

### crypto ca server unrevoke Parameters

| Parameter | Description |
|---|---|
| *cert-serial-no* | Specifies the serial number of the certificate to be unrevoked. Enter the serial number in hexadecimal format. |

# Deploying Advanced PKI Integration

This topic describes how to configure and verify integration with supporting PKI entities.



## Configure Advanced PKI Integration

Overview

The Cisco ASA adaptive security appliance must provide revocation methods to reduce a risk of compromised credentials:

- CRLs
- OCSP
- AAA authorization

The appliance may need to provide a AAA per-user settings server for certificate users

Client Identity Certificate
Cisco ASA Adaptive Security Appliance
CRL
OCSP
AAA

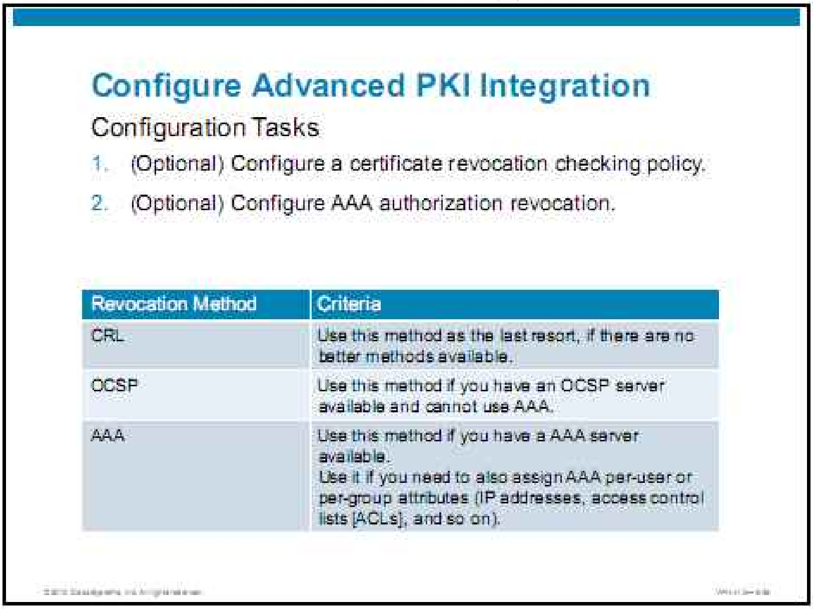
In some cases of certificate-based client authentication, advanced integration with existing PKI is needed. Advanced PKI integration includes configuring a revocation method to reduce a risk of compromised certificates. Certificates are considered compromised when a certificate was issued improperly by a CA or a private key matching a public key on the certificate is thought to be compromised. For example, if the laptop of a user that stores a certificate and a matching private key is lost, the certificate should be revoked. Another example would be revocation of certificates belonging to users who are no longer employed at an organization.

A certificate revocation method can be implemented in the following ways:

- **Configuring certificate revocation lists (CRLs):** A CRL is a list of serial numbers of certificates that have been revoked and are no longer valid. A CRL is generated and published by the CA that issues corresponding certificates and is updated periodically or immediately after a certificate has been revoked. You can configure the Cisco ASA adaptive security appliance to make CRL checks mandatory when authenticating a certificate. The Cisco ASA adaptive security appliance needs a CRL location to verify the certificates of clients. A CRL location can be found in a CRL distribution point (CDP) that is specified in an identity certificate. The security appliance can download a CRL using HTTP, LDAP, or Simple Certificate Enrollment Protocol (SCEP).
- **Configuring Online Certificate Status Protocol (OCSP):** OCSP is a protocol for obtaining the revocation status of digital certificates. OCSP messages are usually communicated over HTTP. You can configure the Cisco ASA adaptive security appliance to make OCSP checks mandatory when authenticating a certificate. The location of the OCSP server on the Cisco ASA adaptive security appliance can be configured as an OCSP URL that is defined in a match certificate rule. The location can be statically configured as an OCSP URL, or it can be specified in the Authority Information Access (AIA) field of the authenticating certificate.

| Note | The OCSP server is being termed as the OCSP responder. |
|---|---|

- **Configuring AAA authorization of the certificate of a user:** You can also revoke user authorization by deploying an external RADIUS server. When the Cisco ASA adaptive security appliance receives the certificate of a user, it sends a predefined field from the certificate as a username and a predefined (common to all users) password to the RADIUS server, which authorizes the user. On the RADIUS server, users with proper usernames (which match predefined fields in the user certificates) and passwords, have to be configured. If you want to revoke user authorization, you have to delete or disable a user account that corresponds to the certificate that you want to revoke.



## Configure Advanced PKI Integration

Configuration Tasks

1. (Optional) Configure a certificate revocation checking policy.
2. (Optional) Configure AAA authorization revocation.

| Revocation Method | Criteria |
|---|---|
| CRL | Use this method as the last resort, if there are no better methods available. |
| OCSP | Use this method if you have an OCSP server available and cannot use AAA. |
| AAA | Use this method if you have a AAA server available.<br>Use it if you need to also assign AAA per-user or per-group attributes (IP addresses, access control lists [ACLs], and so on). |

These are the configuration tasks that are involved in configuring advanced PKI integration:

1. Optionally, configure a certificate revocation checking policy.
2. Optionally, or alternatively, configure AAA user authorization based on certificate identity.

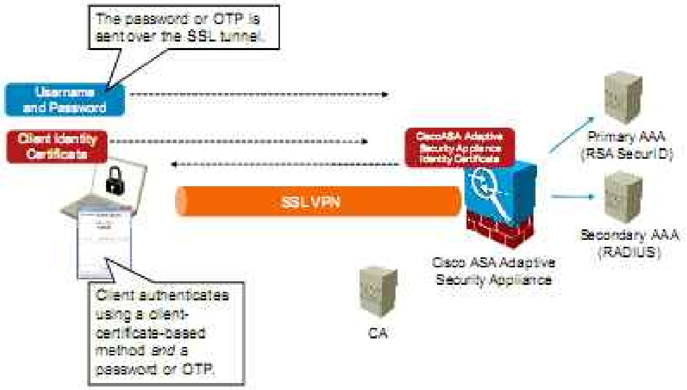
These tasks are identical to those that are used in Cisco Easy VPN deployment, and are therefore not discussed here.

# Deploying Multiple Client Authentication

This topic describes how to configure and verify multiple client authentications.

## Configure Multiple Client Authentication

Overview

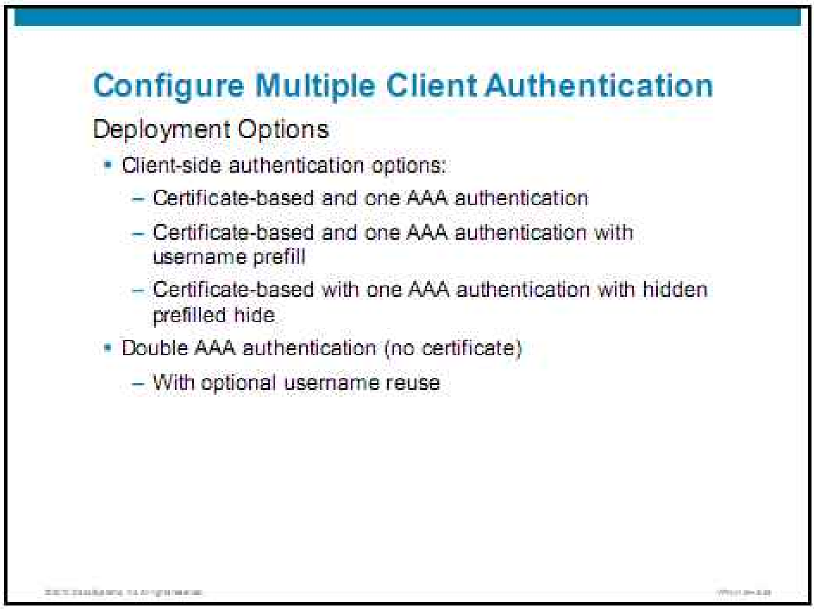


The password or OTP is sent over the SSL tunnel.

Client authenticates using a client-certificate-based method *and* a password or OTP.

Username and Password
Client Identity Certificate
Cisco ASA Adaptive Security Appliance Identity Certificate
SSL VPN
Primary AAA (RSA SecurID)
Secondary AAA (RADIUS)
Cisco ASA Adaptive Security Appliance
CA

Cisco AnyConnect VPN solutions offer multiple client authentication. With multiple authentications, clients can be first authenticated by using a certificate. After the Cisco ASA adaptive security appliance validates a certificate, an SSL tunnel is established. Inside the SSL tunnel, users may have to authenticate again by using a username and a password or a one-time password (OTP). This AAA authentication can be performed against one or two separate databases.



## Configure Multiple Client Authentication

Deployment Options

- Client-side authentication options:
  - Certificate-based and one AAA authentication
  - Certificate-based and one AAA authentication with username prefill
  - Certificate-based with one AAA authentication with hidden prefilled hide
- Double AAA authentication (no certificate)
  - With optional username reuse

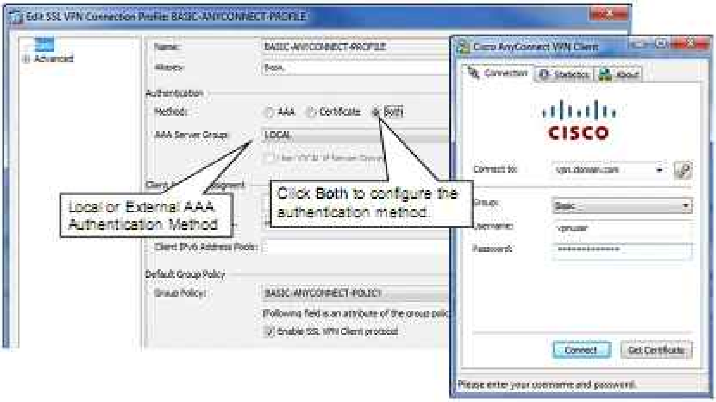
You can deploy one of these multiple authentication combinations:

- Certificate-based and one AAA authentication
- Certificate-based and one AAA authentication, where a username for AAA authentication can be extracted from a certificate subject field (username prefill)
- Certificate-based and one AAA authentication where a username for AAA authentication can be extracted from a certificate subject field and hidden from users
- Double AAA authentication (no certificate) with optional username reuse

All of these options are used to perform client-side authentication. The security appliance authenticates the clients by using any of these methods.

## Configure Multiple Client Authentication

Certificate and One AAA Authentication



Edit SSL VPN Connection Profile: BASIC-ANYCONNECT-PROFILE

Name: BASIC-ANYCONNECT-PROFILE

Aliases: Basic

Authentication

Method: ○ AAA ○ Certificate ● Both

AAA Server Group: LOCAL

Default Group Policy

Group Policy: BASIC-ANYCONNECT-POLICY

Following field is an attribute of the group polic

☑ Enable SSL VPN Client protocol

Cisco AnyConnect VPN Client

Connect to: vpn.domain.com

Group: Basic

Username: vpnuser

Password: **************

Please enter your username and password.

Local or External AAA Authentication Method

Click **Both** to configure the authentication method.

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

To configure certificate-based and one AAA client authentication, complete the following configuration steps in the Cisco ASDM:

**Step 1** Inside the ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

**Step 2** Choose a connection profile and click **Edit** (not shown in the example). The Edit SSL VPN Connection Profile window is displayed.

**Step 1** Make sure that the **Basic** option is selected from the menu on the left.

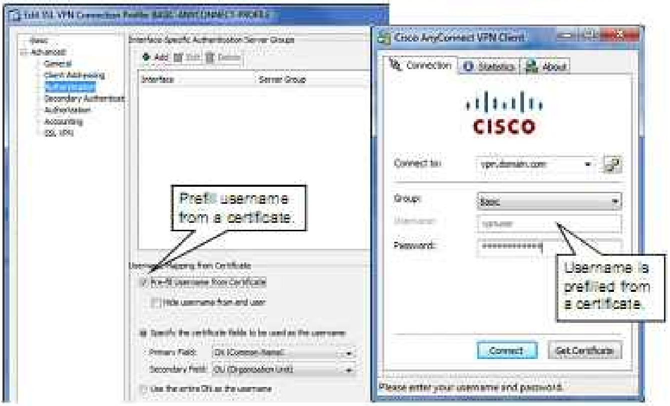
**Step 2** In the Authentication section of the Edit SSL VPN Connection Profile window, choose the **Both** radio button to enable authentication by using certificates and AAA.

**Step 3** From the AAA Server Group drop-down menu, choose either **Local** or a AAA server group to perform the AAA authentication.

The figure shows the Cisco AnyConnect interface in which the user must enter the username and password that is required for the AAA authentication. The AAA authentication is performed after the certificate authentication.

## Configure Multiple Client Authentication

Certificate and One AAA Authentication with Prefill


Edit SSL VPN Connection Profile: BASIC-ANYCONNECT-PROFILE
Basic
Advanced
General
Client Addressing
Authentication
Secondary Authentication
Authorization
Accounting
SSL VPN
Interface-Specific Authentication Server Groups
Add
Edit
Delete
Interface
Server Group
Username Mapping from Certificate
Cisco AnyConnect VPN Client
Connection
Statistics
About
CISCO
Connect
Get Certificate
Prefill username from a certificate.
Username is prefilled from a certificate.

☑ Pre-fill Username from Certificate

☐ Hide username from end user

● Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

Connect to: vpn.domain.com

Group: Basic

Username: Username

Password: ************

Please enter your username and password.

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

The figure illustrates the configuration of the Pre-fill Username from Certificate feature. The security appliance can extract the username from the user identity certificate and use it for AAA authentication.

Complete these steps to enable the username prefill feature:

**Step 1** Choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** to edit the desired connection profile.

**Step 2** Choose the **Authentication** submenu.

**Step 3** Check the **Pre-fill Username from Certificate** check box to specify that the username field should be populated automatically from a specific field in a certificate.

**Step 4** Click the **Specify the Certificate Fields to Be Used as the Username** radio button to select that a username will be derived from a specified certificate field. Multiple options exist:

- Choose a value from the **Primary Field** list. This method is set by default to CN (Common Name). You can augment this selection by defining the secondary field that will be extracted if the primary field does not exist.
- Custom methods.

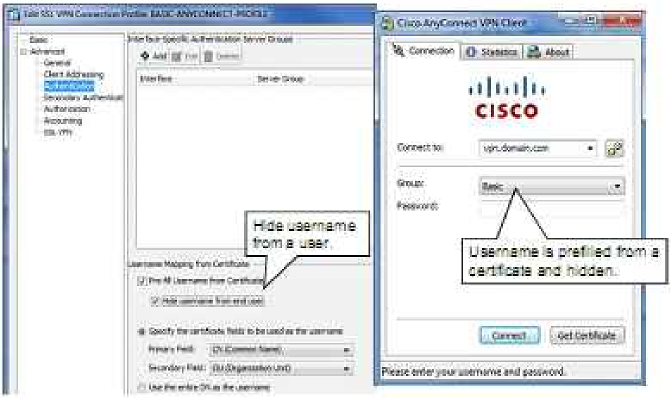
**Step 5** Click **OK** in the Edit SSL VPN Connection Profile.

**Step 6** Click **Apply** to apply the configuration.

When the Cisco AnyConnect client connects to the SSL VPN and selects (or is assigned to) the connection profile that is configured for certificate-based and AAA authentication with the username prefill feature, the Username field in the Authentication tab is filled in and grayed out. The user cannot modify it and is only prompted for the corresponding password. This password may be checked against either the local or an external AAA database, depending on the configuration of the connection profile.

## Configure Multiple Client Authentication

### Certificate and One AAA Authentication with Prefill and Hide



Edit SSL VPN Connection Profile: BASIC-ANYCONNECT-PROFILE

- Basic
- Advanced
  - General
  - Client Addressing
  - Authentication
  - Secondary Authentication
  - Authorization
  - Accounting
  - SSL VPN

Interface-Specific Authentication Server Groups

| Interface | Server Group |
|---|---|

Username Mapping from Certificate

☑ Pre-fill Username from Certificate

☑ Hide username from end user

● Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

Hide username from a user.

Cisco AnyConnect VPN Client

Connect to: vpn.domain.com

Group: Basic

Password:

Username is prefilled from a certificate and hidden.

Please enter your username and password.

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

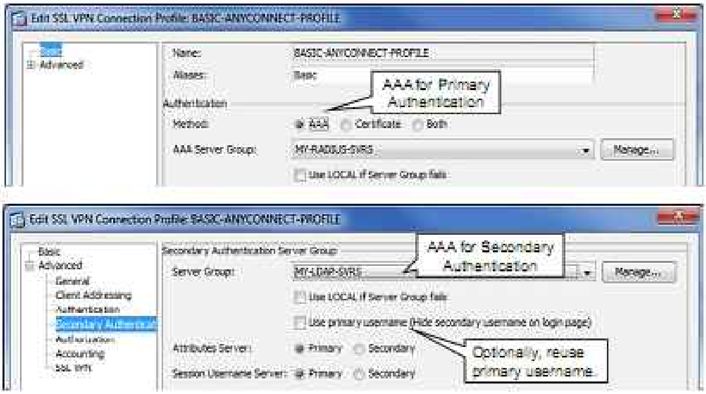
In addition to using the username prefill feature, you may enhance security by hiding the username from the authenticating users. This option improves security in situations when an unauthorized person tries to break into the VPN by using a stolen computer.

To enable the username hide feature, check the **Hide Username from End User** check box in the Authentication menu of the connection profile.

When the username is extracted from the certificate and hidden from the end user, users are only prompted for a password when they connect by using the respective connection profile.

## Configure Multiple Client Authentication

### Double AAA Authentication



Edit SSL VPN Connection Profile: BASIC-ANYCONNECT-PROFILE

Name: BASIC-ANYCONNECT-PROFILE

Aliases: Basic

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: MY-RADIUS-SVRS

□ Use LOCAL if Server Group fails

AAA for Primary Authentication

Edit SSL VPN Connection Profile: BASIC-ANYCONNECT-PROFILE

Secondary Authentication Server Group

Server Group: MY-LDAP-SVRS

□ Use LOCAL if Server Group fails

□ Use primary username (Hide secondary username on login page)

Attributes Server: ● Primary ○ Secondary

Session Username Server: ● Primary ○ Secondary

AAA for Secondary Authentication

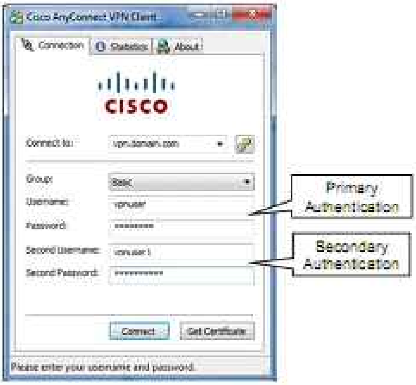
Optionally, reuse primary username.

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

You can also enable double AAA authentication. In this case, you should choose **AAA** instead of **Both** as the authentication method in the Basic menu of the connection profile configuration.

## Configure Multiple Client Authentication

### Double AAA Authentication (Cont.)



Cisco AnyConnect VPN Client

Connect to: vpn.domain.com

Group: Basic

Username: vpnuser

Password: *********

Second Username: vpnuser1

Second Password: **********

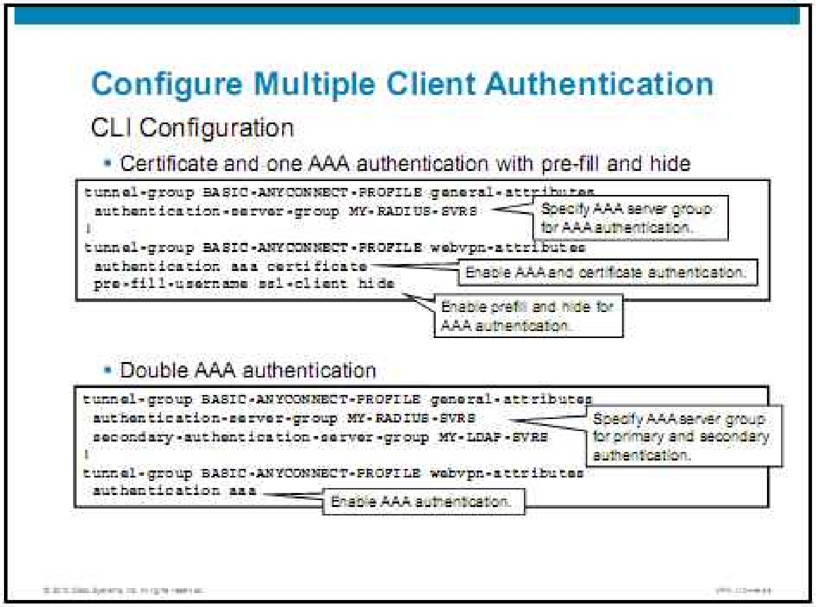
Please enter your username and password.

Primary Authentication

Secondary Authentication

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

The figure shows the Cisco AnyConnect client connecting to a connection profile that is configured for double authentication. The user is prompted to enter a primary username and password and a secondary username and password.



## Configure Multiple Client Authentication

CLI Configuration

- Certificate and one AAA authentication with pre-fill and hide

```
tunnel-group BASIC-ANYCONNECT-PROFILE general-attributes
 authentication-server-group MY-RADIUS-SVRS
!
tunnel-group BASIC-ANYCONNECT-PROFILE webvpn-attributes
 authentication aaa certificate
 pre-fill-username ssl-client hide
```

Specify AAA server group for AAA authentication.

Enable AAA and certificate authentication.

Enable prefill and hide for AAA authentication.

- Double AAA authentication

```
tunnel-group BASIC-ANYCONNECT-PROFILE general-attributes
 authentication-server-group MY-RADIUS-SVRS
 secondary-authentication-server-group MY-LDAP-SVRS
!
tunnel-group BASIC-ANYCONNECT-PROFILE webvpn-attributes
 authentication aaa
```

Specify AAA server group for primary and secondary authentication.

Enable AAA authentication.

To configure certificate and AAA client authentication using the CLI, use the following commands. First, enter tunnel group configuration mode by using the **tunnel-group** command, followed by the tunnel group name and the **general-attributes** keyword. Then, use the **authentication-server-group** command to configure a AAA server group that will be used for primary authentication.

Next, enter tunnel group configuration mode for WebVPN attributes using the **tunnel-group** command, followed by the tunnel group name and **webvpn-attributes** keyword. Use the **pre-fill-username ssl-client hide** command to specify that the username will be extracted from a certificate. Finally, enable AAA and certificate authentication by using the **authentication certificate aaa** command.

To configure double AAA client authentication using the CLI, use the following commands. First, enter tunnel group configuration mode by using the **tunnel-group** command, followed by the tunnel group name and the **general-attributes** keyword. Then, configure AAA server groups that will be used for primary and secondary authentication by using the **authentication-server-group** and **secondary-authentication-server-group** commands, respectively.

Next, enter tunnel group configuration mode for WebVPN attributes by using the **tunnel-group** command, followed by the tunnel group name and the **webvpn-attributes** keyword. Enable AAA authentication by using the **authentication aaa** command.

### 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 |
|---|---|
| **general-attributes** | Specifies attributes for the tunnel group |
| *name* | Specifies the name of the tunnel group |

## 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**]

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

| Parameter | Description |
|---|---|
| *interface_name* | (Optional) Specifies the interface where the IPsec tunnel terminates |
| **LOCAL** | (Optional) Requires authentication against the local user database if all of the servers in the server group have been deactivated due to communication failures |
| *server_group* | Identifies the previously configured authentication server or group of servers |

## secondary-authentication-server-group

To specify a secondary authentication server group to associate with the session when double authentication is enabled, use the **secondary-authentication-server-group** command in tunnel-group general-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

**secondary-authentication-server-group** [*interface_name*] {**none** | **LOCAL** | *groupname* [**LOCAL**]} [**use-primary-username**]}

### secondary-authentication-server-group Parameters

| Parameter | Description |
|---|---|
| *interface_name* | (Optional) Specifies the interface where the IPsec tunnel terminates. |
| **LOCAL** | (Optional) Requires authentication against the local user database if all of the servers in the server group have been deactivated due to communication failures. If the server group name is either LOCAL or NONE, do not use the **LOCAL** keyword here. |
| **none** | (Optional) Specifies the server group name as NONE, indicating that authentication is not required. |
| *groupname* **[LOCAL]** | Identifies the previously configured authentication server or group of servers. Optionally, this group can be the LOCAL group. |
| **use-primary-username** | Use the primary username as the username for the secondary authentication. |

## 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 |
|---|---|
| `webvpn-attributes` | Specifies WebVPN attributes for the tunnel group |
| *name* | Specifies the name of the tunnel group |

## pre-fill-username

To enable extraction of a username from a client certificate for use in authentication and authorization, use the **pre-fill-username** command in tunnel-group webvpn-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

**pre-fill-username** {**ssl-client** | **clientless**}

### pre-fill-username Parameters

| Parameter | Description |
|---|---|
| `ssl-client` | Enables this feature for Cisco AnyConnect VPN Client connections |
| `clientless` | Enables this feature for clientless connections |
| `hide` | Does not display the extracted username to the end user |

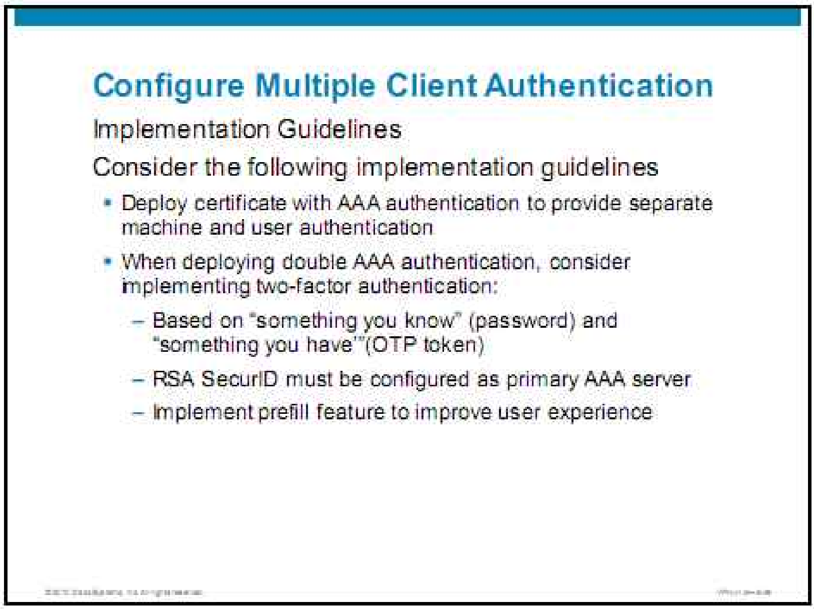
## authentication

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 |
|---|---|
| `aaa` | Provides a username and a password that the adaptive security appliance checks against a previously configured AAA server |
| `certificate` | Provides a certificate during SSL negotiation |



## Configure Multiple Client Authentication

Implementation Guidelines

Consider the following implementation guidelines

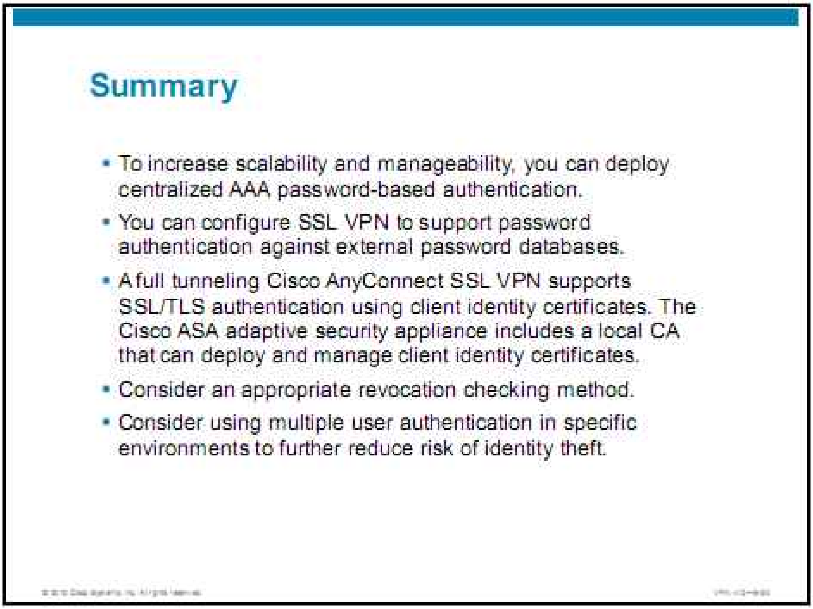
- Deploy certificate with AAA authentication to provide separate machine and user authentication
- When deploying double AAA authentication, consider implementing two-factor authentication:
  - Based on "something you know" (password) and "something you have'"(OTP token)
  - RSA SecurID must be configured as primary AAA server
  - Implement prefill feature to improve user experience

Consider the following configuration guidelines when implementing multiple client authentication:

- Deploy "certificate + AAA" authentication to provide separate machine and user authentication
- When deploying double AAA authentication (with or without certificates), consider implementing two-factor authentication:
  - Based on "something you know" (password) and "something you have" (OTP token).
  - RSA SecurID must be configured as the primary AAA server.
  - Consider implementing the prefill or "use primary username" feature to improve user experience.

# Summary

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



## Summary

- To increase scalability and manageability, you can deploy centralized AAA password-based authentication.
- You can configure SSL VPN to support password authentication against external password databases.
- A full tunneling Cisco AnyConnect SSL VPN supports SSL/TLS authentication using client identity certificates. The Cisco ASA adaptive security appliance includes a local CA that can deploy and manage client identity certificates.
- Consider an appropriate revocation checking method.
- Consider using multiple user authentication in specific environments to further reduce risk of identity theft.

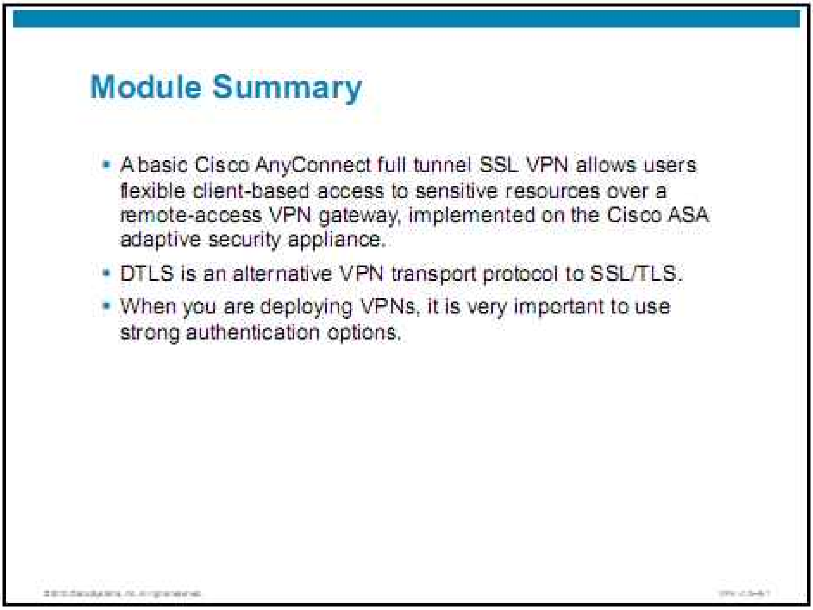
# References

For additional information, refer to these resources:

- *ASA 8.x: AnyConnect SCEP Enrollment Configuration Example* at http://ciscosystems.com/en/US/products/ps6120/products_configuration_example09186a0080b25dc1.shtml
- *ASA 8.x: AnyConnect SSL VPN CAC-SmartCards Configuration for Windows* at http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809a2b93.shtml

# Module Summary

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



## Module Summary

- A basic Cisco AnyConnect full tunnel SSL VPN allows users flexible client-based access to sensitive resources over a remote-access VPN gateway, implemented on the Cisco ASA adaptive security appliance.
- DTLS is an alternative VPN transport protocol to SSL/TLS.
- When you are deploying VPNs, it is very important to use strong authentication options.

## Module 4

# Deployment of Cisco ASA Adaptive Security Appliance Clientless Remote Access VPN Solutions

## Overview

Clientless Secure Sockets Layer (SSL) virtual private network (VPN) solutions provide browser-based access to resources behind the Cisco ASA adaptive security appliance. In clientless SSL VPNs, users can access resources without any special client software. Using clientless SSL VPNs, users can access web-based applications, Common Internet File System (CIFS) file shares, and FTP servers. Using application plug-ins, port forwarding, and smart tunnels, you can access almost any application that uses static TCP ports. The module describes deployment of the basic clientless SSL VPN, as well as advanced application access, and advanced authentication. This module also describes how to customize the clientless SSL VPN portal to the needs of the organization.

## Module Objectives

Upon completing this module, you will be able to implement and maintain a Cisco clientless remote access SSL VPNs 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 basic clientless VPN features of a Cisco ASA adaptive security appliance clientless SSL VPN
- Deploy and manage advanced clientless VPN application access features of a clientless SSL VPN
- Deploy and manage advanced authentication features of a clientless SSL VPN
- Deploy and manage advanced clientless VPN application access features of a clientless SSL VPN

## Lesson 1

# Deploying a Basic Clientless VPN Solution

## Overview

A basic clientless Cisco SSL VPN solution allows users browser-based access to sensitive resources over a remote access Secure Sockets Layer (SSL) virtual private network (VPN) gateway that is implemented on the Cisco ASA adaptive security appliance. A basic Cisco ASA clientless SSL VPN uses basic user authentication with usernames and passwords, basic SSL VPN portal features, and a single access control policy. This lesson enables you to configure, verify, and troubleshoot a basic clientless SSL VPN solution.

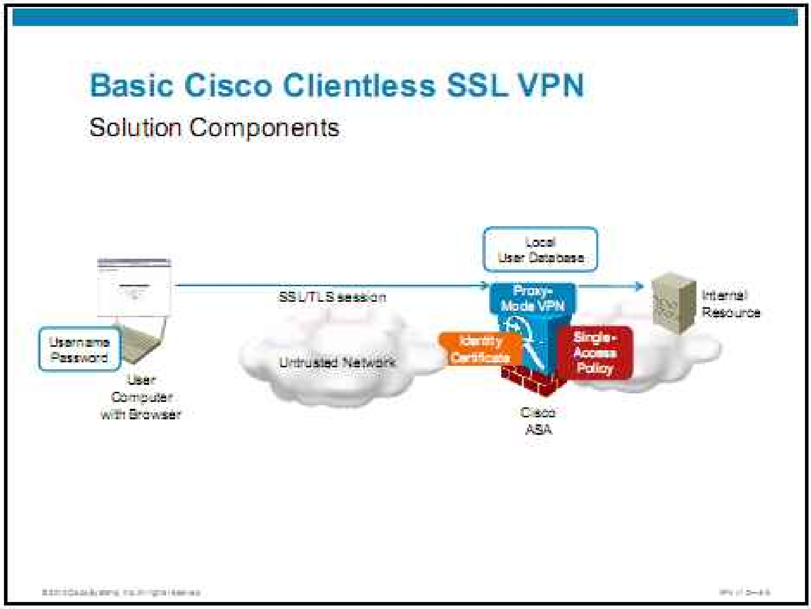
### Objectives

Upon completing this lesson, you will be able to deploy and manage basic clientless VPN features of a Cisco ASA adaptive security appliance clientless SSL VPN. This ability includes being able to meet these objectives:

- Plan the configuration of a clientless SSL VPN solution
- Configure and verify basic Cisco ASA adaptive security appliance gateway features for a clientless SSL VPN solution
- Configure and verify password-based local user authentication in a clientless SSL VPN solution
- Configure and verify basic portal features and access control in a clientless SSL VPN solution
- Troubleshoot VPN session establishment between a browser client and a Cisco ASA adaptive security appliance gateway

# Configuration Choices, Basic Procedure, and Required Input Parameters

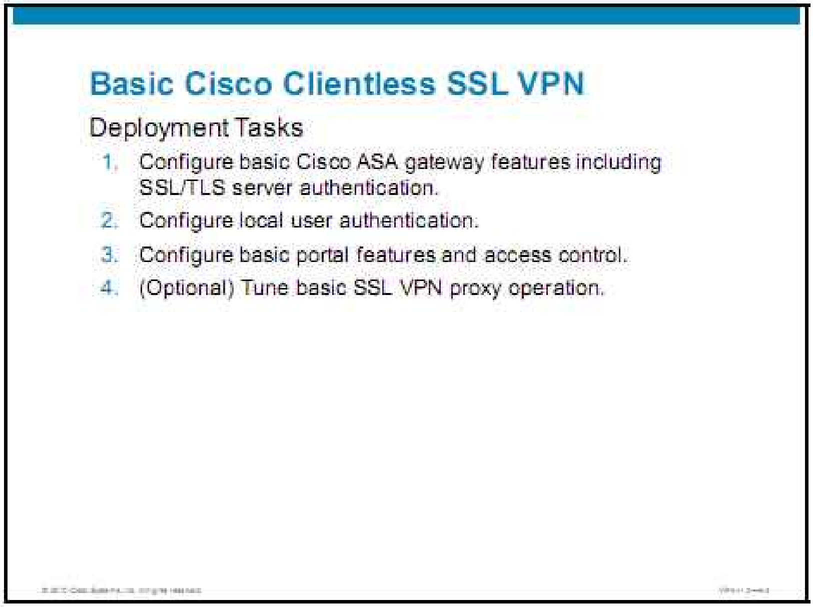
This topic describes how to plan the configuration of a clientless SSL VPN solution.



## Basic Cisco Clientless SSL VPN

Solution Components

In a basic Cisco ASA adaptive security appliance clientless SSL VPN solution, remote users use a standard web browser to establish a Secure Sockets Layer or Transport Layer Security (SSL/TLS) session with the Cisco ASA adaptive security appliance. The basic solution uses bidirectional authentication, where the client authenticates the Cisco ASA adaptive security appliance with a certificate-based authentication method, and the appliance authenticates the user based on a username and password against its local user database. After authentication, the Cisco ASA adaptive security appliance applies a set of authorization rules to the user session, and presents the user with a web portal over which the user can access internal resources only using a browser. In the basic clientless solution, the client can only use some services, such as web application access and browser-based file-share access to internal resources.



## Basic Cisco Clientless SSL VPN

Deployment Tasks

1. Configure basic Cisco ASA gateway features including SSL/TLS server authentication.
2. Configure local user authentication.
3. Configure basic portal features and access control.
4. (Optional) Tune basic SSL VPN proxy operation.

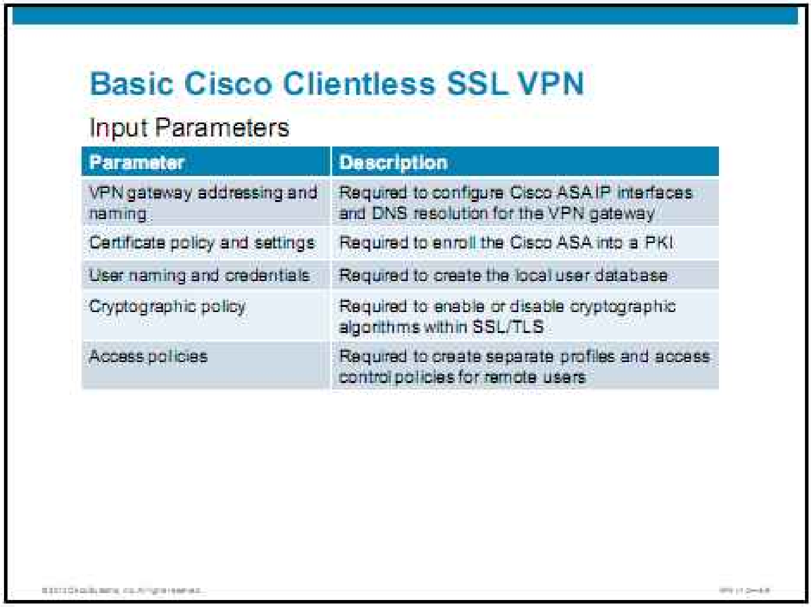
Use the following general deployment tasks to create a basic Cisco ASA clientless SSL VPN:

1. Configure the Cisco ASA adaptive security appliance with basic SSL VPN gateway features, including provisioning the identity certificate of the appliance to enable SSL/TLS server authentication.

2. Configure basic user authentication by configuring the local user database on the Cisco ASA adaptive security appliance to create user accounts with static passwords.

3. Configure basic SSL VPN portal features and basic access control, limiting access to the enterprise network.

4. Tune the configuration of the Cisco ASA adaptive security appliance SSL VPN proxy operations to support potentially problematic applications.



## Basic Cisco Clientless SSL VPN

Input Parameters

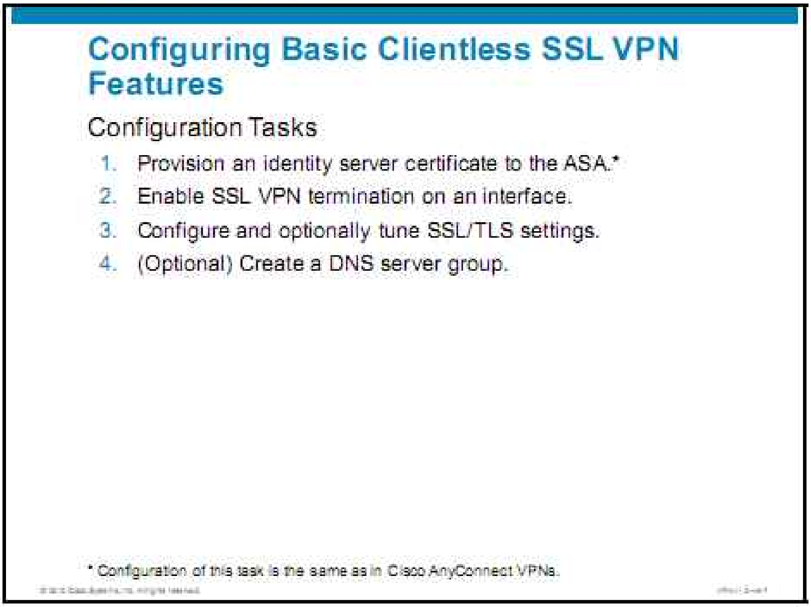
| Parameter | Description |
|---|---|
| VPN gateway addressing and naming | Required to configure Cisco ASA IP interfaces and DNS resolution for the VPN gateway |
| Certificate policy and settings | Required to enroll the Cisco ASA into a PKI |
| User naming and credentials | Required to create the local user database |
| Cryptographic policy | Required to enable or disable cryptographic algorithms within SSL/TLS |
| Access policies | Required to create separate profiles and access control policies for remote users |

Before implementing a basic Cisco ASA clientless SSL VPN, you will need to obtain and analyze several pieces of information that are related to the network and system environment. These input parameters include the following:

- The IP addressing plan that will dictate the SSL VPN gateway IP addressing, and the enterprise naming plan that will dictate the name of the SSL VPN gateway. This data is needed to assign an IP address to the Cisco ASA adaptive security appliance VPN-terminating interface, and to assign a name inside the SSL VPN gateway SSL/TLS identity certificate.
- The enterprise certificate policy and certificate settings to include all relevant fields inside a PKI-provisioned certificate, to enroll the Cisco ASA adaptive security appliance into a PKI (if so desired).
- The enterprise policy of user naming and the enterprise password policy, to create the local user database on the Cisco ASA adaptive security appliance.
- The enterprise cryptographic policy, to choose the optimal SSL/TLS protocol versions and algorithm bundles (cipher suites) for SSL/TLS sessions on the Cisco ASA adaptive security appliance.
- Access policies that dictate which sensitive resources remote users can access. These policies are needed to configure an access control policy on the Cisco ASA adaptive security appliance that will be applied to clientless SSL VPN sessions.

# Configuring Basic Cisco ASA Adaptive Security Appliance SSL VPN Gateway Features

This topic describes how to configure and verify basic Cisco ASA adaptive security appliance gateway features for clientless SSL VPN.



## Configuring Basic Clientless SSL VPN Features

Configuration Tasks

1. Provision an identity server certificate to the ASA.*
2. Enable SSL VPN termination on an interface.
3. Configure and optionally tune SSL/TLS settings.
4. (Optional) Create a DNS server group.

* Configuration of this task is the same as in Cisco AnyConnect VPNs.

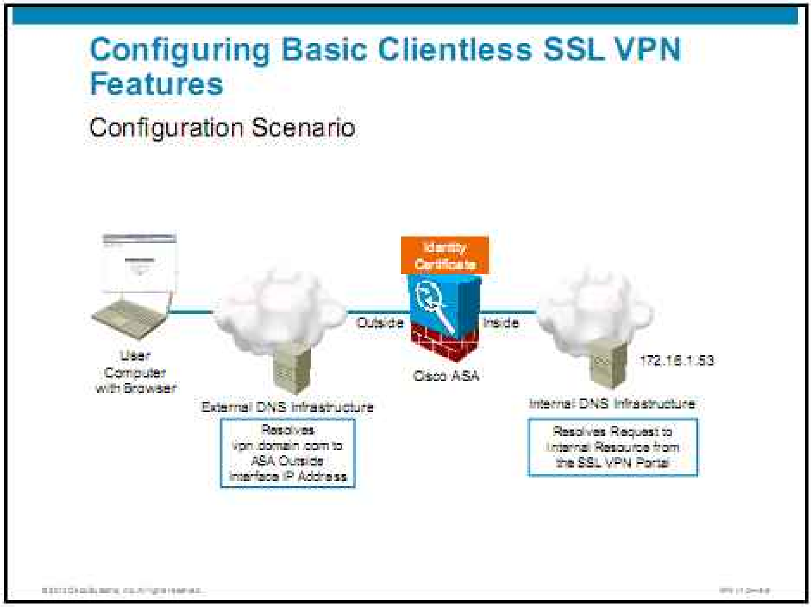
To configure basic Cisco ASA adaptive security appliance SSL VPN gateway features for clientless access, complete the following configuration tasks:

1. Provision an identity server SSL/TLS certificate to the Cisco ASA adaptive security appliance. This task is performed in the same manner as the related task in SSL VPNs that are based on the Cisco AnyConnect VPN.

2. Enable SSL VPN termination on a Cisco ASA adaptive security appliance interface and therefore enable the Cisco ASA adaptive security appliance SSL VPN server function.

3. Configure and optionally tune SSL/TLS settings of the SSL VPN server.

4. Optionally, create a DNS server group if you want to use hostnames instead of IP addresses to access internal resources. The DNS settings enable the security appliance to resolve the hostnames that are specified in the user requests.



## Configuring Basic Clientless SSL VPN Features

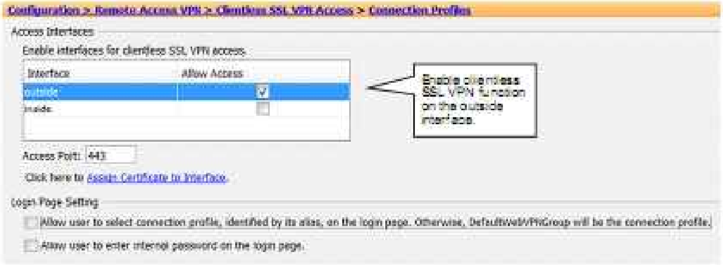
Configuration Scenario

Identity Certificate
Outside
Inside
User Computer with Browser
Cisco ASA
172.16.1.53
External DNS Infrastructure
Resolves vpn.domain.com to ASA Outside Interface IP Address
Internal DNS Infrastructure
Resolves Request to Internal Resource from the SSL VPN Portal

This figure presents the configuration scenario that is used in upcoming configuration tasks. The Cisco ASA adaptive security appliance can either use a self-signed certificate or receive its identity certificate from an external or internal CA server. You will need to configure the external Domain Name System (DNS) infrastructure to resolve the name of the Cisco ASA adaptive security appliance (inside its identity certificate) to its VPN-terminating interface IP address (the IP address of the outside interface in this example). Additionally, you may need the IP addresses of internal DNS servers for the SSL VPN portal to be able to resolve internal URLs.

## Configuring Basic Clientless SSL VPN Features

Task 2: Enable SSL VPN Termination on an Interface



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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

| Interface | Allow Access |
|---|---|
| outside | ☑ |
| inside | ☐ |

Access Port: 443

Click here to Assign Certificate to Interface.

Login Page Setting

☐ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

☐ Allow user to enter internal password on the login page.

Enable clientless SSL VPN function on the outside interface.

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

For detailed configuration guidance on the first configuration task (provisioning the identity certificate), refer to the "Deploying a Basic Cisco AnyConnect Full Tunnel SSL VPN Solution" lesson of this course.

In Task 2, you will globally enable the SSL VPN server function on the Cisco ASA adaptive security appliance, and select the interface or interfaces on which the appliance will accept SSL VPN sessions.

Perform the following steps:

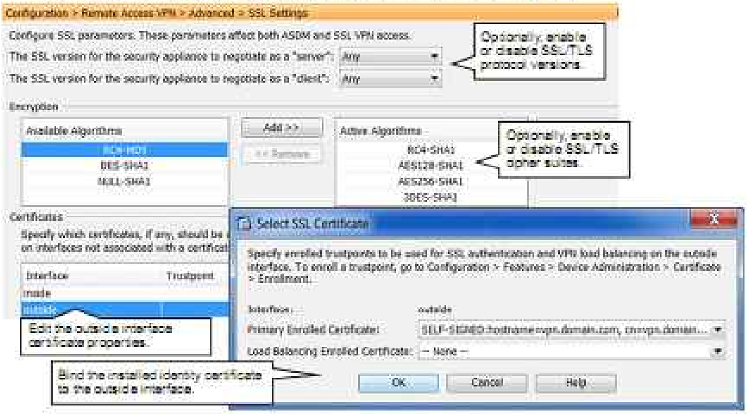
**Step 1** In the Cisco Adaptive Security Device Manager (Cisco ASDM), choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

**Step 1** In the Enable Interfaces for Clientless SSL VPN Access field, check the **Allow Access** check box for the interface on which you want to terminate SSL VPN connections. In this example, these connections are enabled on the "outside" interface.

**Step 2** Click **Apply,** and click **Save** to save your configuration, if necessary.

## Configuring Basic Clientless SSL VPN Features

### Task 3: Configure and Tune SSL/TLS Settings



Configuration > Remote Access VPN > Advanced > SSL Settings

Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

The SSL version for the security appliance to negotiate as a "server": Any

The SSL version for the security appliance to negotiate as a "client": Any

Encryption

| Available Algorithms | Active Algorithms |
|---|---|
| RC4-MD5 | RC4-SHA1 |
| DES-SHA1 | AES128-SHA1 |
| NULL-SHA1 | AES256-SHA1 |
| | 3DES-SHA1 |

Certificates

Specify which certificates, if any, should be … on interfaces not associated with a certificat…

| Interface | Trustpoint |
|---|---|
| inside | |
| outside | |

Select SSL Certificate

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the outside interface. To enroll a trustpoint, go to Configuration > Features > Device Administration > Certificate > Enrollment.

Interface: outside

Primary Enrolled Certificate: SELF-SIGNED:hostname=vpn.domain.com, cn=vpn.domain...

Load Balancing Enrolled Certificate: -- None --

Optionally, enable or disable SSL/TLS protocol versions.

Optionally, enable or disable SSL/TLS cipher suites.

Edit the outside interface certificate properties.

Bind the installed identity certificate to the outside interface.

Configuration > Remote Access VPN > Advanced > SSL Settings

In Task 3, you need to attach the installed identity certificate to an appropriate Cisco ASA adaptive security appliance network interface on which you will configure clientless SSL VPN termination.

Perform the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Advanced > SSL Settings**.

**Step 2** At the top of the SSL Settings window, you can select the SSL and TLS protocol versions that the appliance will support as the SSL/TLS server. For configuration guidance on these settings, refer to this same topic in the "Deploying a Basic Cisco AnyConnect Full Tunnel SSL VPN Solution" lesson of this course.

**Step 3** From the SSL Settings window, in the Encryption area, you can choose the cryptographic algorithm bundles (cipher suites) that the Cisco ASA adaptive security appliance will accept in the initial SSL/TLS negotiation. If you need to change these settings based on a local cryptographic policy, you can enable or disable specific bundles here.

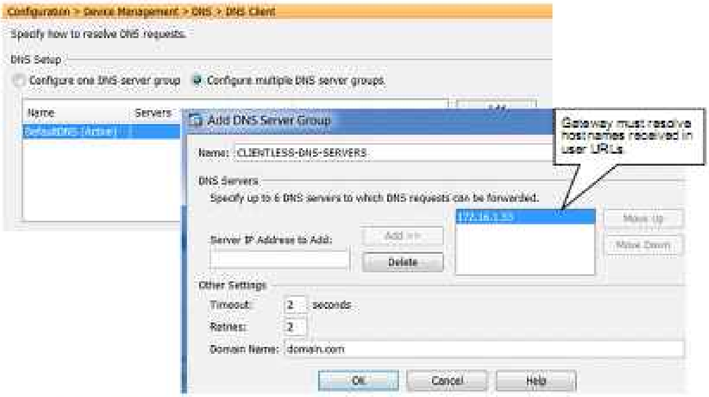
**Step 4** In the SSL Settings window, where the interfaces are listed, click the **Edit** button to edit the interface or interfaces on which the Cisco ASA adaptive security appliance will accept SSL VPN connections.

**Step 5** In the Select SSL Certificate dialog box, choose the **Primary Enrolled Certificate** drop-down list, and choose the installed identity certificate. The example in the figure is using a self-signed identity certificate.

**Step 6** Click **OK** and **Apply**, and then click **Save** to save your configuration, if necessary.

# Configuring Basic Clientless SSL VPN Features

## Task 4: (Optional) Create a DNS Server Group



Configuration > Device Management > DNS > DNS Client

Specify how to resolve DNS requests.

DNS Setup

○ Configure one DNS server group ● Configure multiple DNS server groups

| Name | Servers |
|---|---|
| DefaultDNS (Active) | |

Add DNS Server Group

Name: CLIENTLESS-DNS-SERVERS

DNS Servers

Specify up to 6 DNS servers to which DNS requests can be forwarded.

Server IP Address to Add:

172.16.1.55

Other Settings

Timeout: 2 seconds

Retries: 2

Domain Name: domain.com

Gateway must resolve hostnames received in user URLs.

Configuration > Device Management > DNS > DNS Client

In the optional Task 4, you will create a DNS server group that the Cisco ASA adaptive security appliance will use to resolve internal URLs that are requested by clientless SSL VPN users.

The significance of DNS in clientless SSL VPN is higher than in full tunnel VPNs (Cisco AnyConnect VPN Clients or Easy VPN Clients), because the VPN server resolves hostnames separately from the client. The client specifies the desired resources and the internal hostnames in the URLs that are sent to the gateway. The gateway rewrites the content and resolves the hostnames to reach the internal servers. In full tunnel VPNs, only the VPN clients perform DNS lookup.

You can create multiple DNS server groups, and assign a different DNS server group to each user group. To create a DNS server group, perform the following steps:

**Step 1** Choose **Configuration > Device Management > DNS > DNS Client**.

**Step 2** In the DNS Setup area, click the **Configure Multiple DNS Server Groups** radio button.

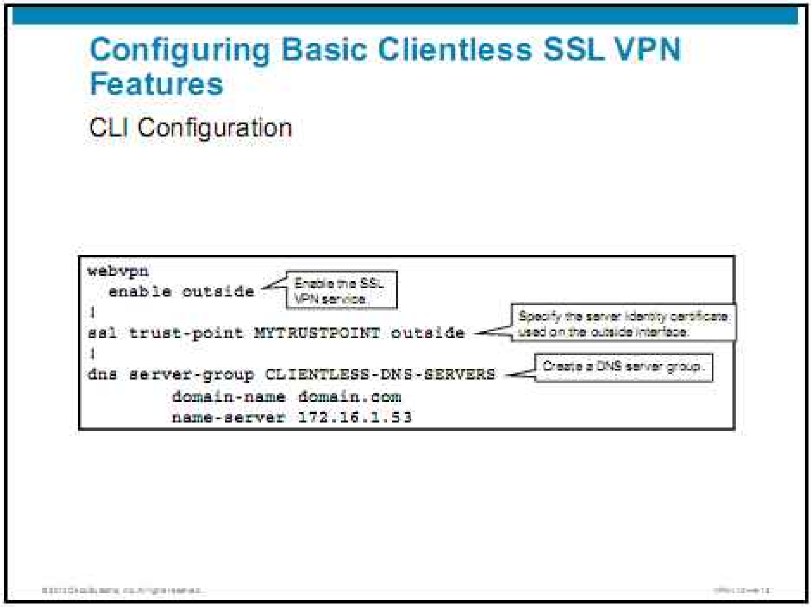
**Step 3** Click **Add** to add a new DNS server group.

**Step 4** In the Add DNS Server Group window, name the new DNS server group by entering the name in the Name field. (This example uses CLIENTLESS-DNS-SERVERS for the name.)

**Step 5** Enter the addresses of all required DNS servers in the Server IP Address to Add field, and click **Add** to add a server to the group.

**Step 6** Specify the local domain suffix in the Domain Name field.

**Step 7** Click **OK** and **Apply**, and then click **Save** to save your configuration, if necessary.



## Configuring Basic Clientless SSL VPN Features

CLI Configuration

```
webvpn
  enable outside
!
ssl trust-point MYTRUSTPOINT outside
!
dns server-group CLIENTLESS-DNS-SERVERS
        domain-name domain.com
        name-server 172.16.1.53
```

Enable the SSL VPN service.

Specify the server identity certificate used on the outside interface.

Create a DNS server group.

The output in the figure shows the CLI commands that are required to configure the basic Cisco ASA adaptive security appliance SSL VPN gateway features using a preprovisioned certificate in the "MYTRUSTPOINT" trustpoint.

In the CLI, enter the SSL VPN server configuration submode on the Cisco ASA adaptive security appliance using the **webvpn** command, and enable the SSL VPN server on the outside interface using the **enable** command.

Next, assign the installed identity certificate of the Cisco ASA adaptive security appliance to the interface using the **ssl trust-point** command.

Finally, create the optional DNS server group using the **dns server-group** command, and inside its configuration submode, use the **domain-name** command to specify the default local domain suffix and the **name-server** command or commands to specify all DNS servers that belong to this group.

## dns server-group

To enter the dns server-group mode, in which you can specify the domain name, name server, number of retries, and timeout values for a DNS server to use for a tunnel group, use the **dns server-group** command in global configuration mode. To remove a particular DNS server group, use the **no** form of this command.

**dns server -group** *name*

### dns server-group Parameters

| Parameter | Description |
|---|---|
| *name* | Specifies the name of the DNS server group configuration that should be used for the tunnel group |

## domain-name (dns server-group)

To set the default domain name, use the **domain-name** command in dns server-group configuration mode. To remove the domain name, use the **no** form of this command. The Cisco ASA adaptive security appliance appends the domain name as a suffix to unqualified names. For example, if you set the domain name to "example.com," and specify a syslog server by the unqualified name "jupiter," then the security appliance qualifies the name to jupiter.example.com.

**domain-name** *name*

### domain-name (dns server-group) Parameters

| Parameter | Description |
|---|---|
| *name* | Sets the domain name, up to 63 characters |

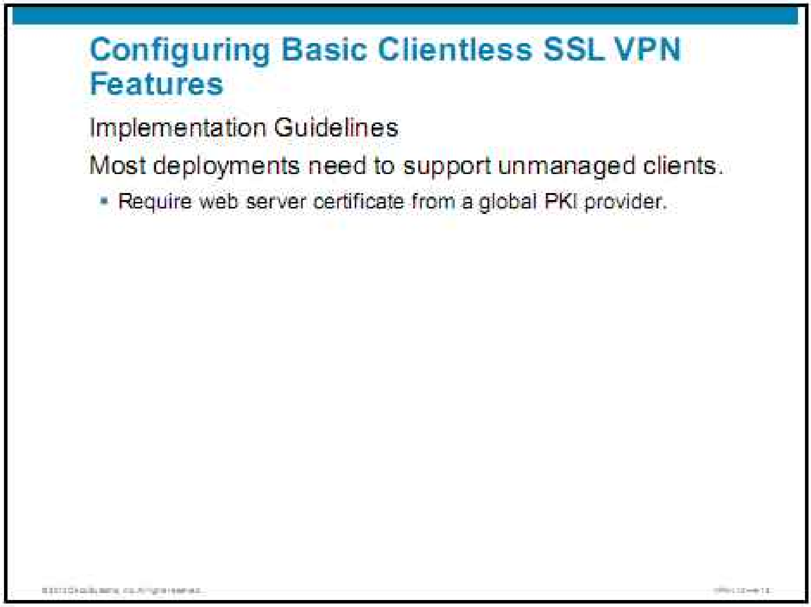
## name-server

To identify one or more DNS servers, use the **name-server** command in dns server-group configuration mode. To remove a server or servers, use the **no** form of this command. The adaptive security appliance uses DNS to resolve server names in your SSL VPN configuration or certificate configuration. Other features that define server names (such as authentication, authorization, and accounting [AAA]) do not support DNS resolution. You must enter the IP address or manually resolve the name to an IP address by using the **name** command.

**name-server** *ip_address* [*ip_address2*] [...] [*ip_address6*]

### name-server Parameters

| Parameter | Description |
|---|---|
| *ip_address* | Specifies the DNS server IP address. You can specify up to 6 addresses as separate commands, or for convenience, up to 6 addresses in one command separated by spaces. If you enter multiple servers in one command, the Cisco ASA adaptive security appliance saves each server in a separate command in the configuration. The appliance then tries each DNS server in order until it receives a response. |



## Configuring Basic Clientless SSL VPN Features

Implementation Guidelines

Most deployments need to support unmanaged clients.

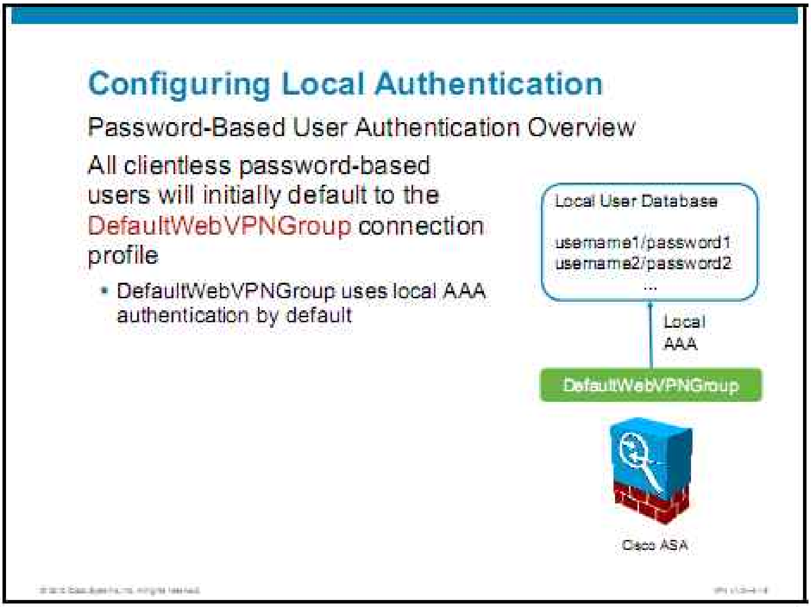
- Require web server certificate from a global PKI provider.

When you implement basic Cisco ASA clientless SSL VPN gateway features, consider this implementation guideline:

- With clientless VPNs, you are likely to support unmanaged VPN clients. If you deploy a self-signed or private public key infrastructure (PKI) certificate, these clients have no built-in mechanism to be able to verify the identity certificate of the Cisco ASA adaptive security appliance, effectively negating all SSL/TLS protection and possibly exposing you to significant risk. If your Cisco ASA adaptive security appliance SSL VPN gateway is accessed by such users, you should install an identity certificate from a global PKI provider on the Cisco ASA adaptive security appliance.

# Configuring Local Password-Based User Authentication

This topic describes how to configure and verify password-based local user authentication in a clientless SSL VPN.



## Configuring Local Authentication

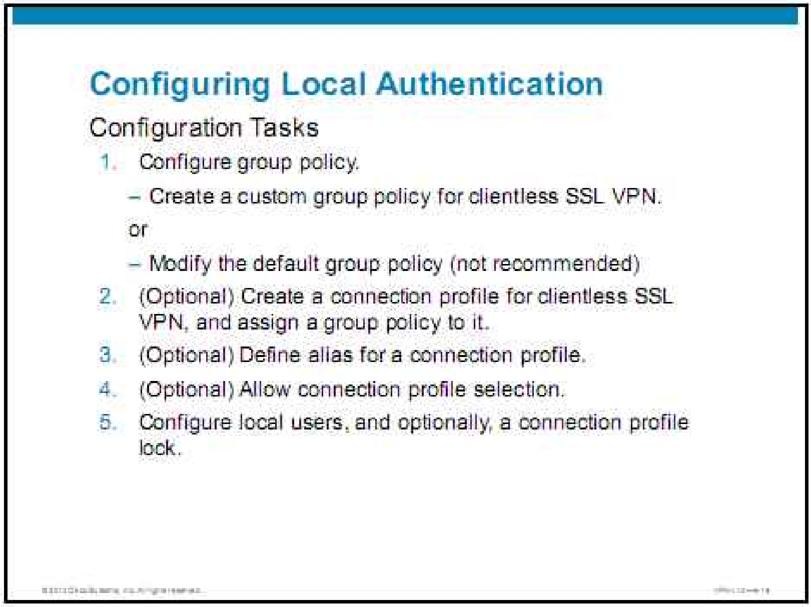
Password-Based User Authentication Overview

All clientless password-based users will initially default to the DefaultWebVPNGroup connection profile

- DefaultWebVPNGroup uses local AAA authentication by default

After configuring basic Cisco ASA adaptive security appliance SSL VPN gateway parameters, the next deployment task is to configure a user authentication method, and prepare the Cisco ASA adaptive security appliance with all the necessary configuration objects to enable later assignment of VPN policies. In this basic SSL VPN clientless solution, you will deploy simple password-based user authentication, using the local user database on the Cisco ASA adaptive security appliance.

When SSL VPN clientless users connect to the Cisco ASA adaptive security appliance, the Cisco ASA adaptive security appliance will initially assign them to the DefaultWebVPNGroup connection profile. This connection profile is by default configured to use the local user database for user authentication.



## Configuring Local Authentication

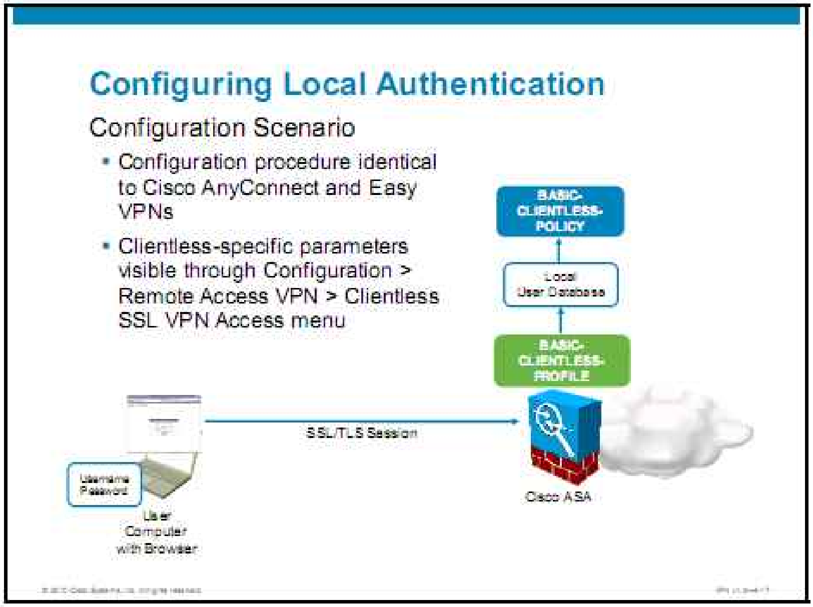
### Configuration Tasks

1. Configure group policy.
   - Create a custom group policy for clientless SSL VPN.

   or
   - Modify the default group policy (not recommended)
2. (Optional) Create a connection profile for clientless SSL VPN, and assign a group policy to it.
3. (Optional) Define alias for a connection profile.
4. (Optional) Allow connection profile selection.
5. Configure local users, and optionally, a connection profile lock.

To configure local user authentication in a clientless SSL VPN solution, perform the following configuration tasks:

1. Configure a group policy using one of two options:
   - Create a custom group policy for clientless SSL VPN.
   - Modify the default group policy. This approach is not recommended, because you may have problems with grouping users later on.
2. Create a connection profile for clientless SSL VPN, and assign the configured group policy to it.
3. Optionally, define an alias for the connection profile. An alias makes a profile selectable to VPN users.
4. Optionally, allow connection profile selection. This option allows the VPN users to connect using a chosen connection profile, if the profile has an alias.
5. Configure local users and, optionally, a connection profile lock. This task is identical to the Cisco AnyConnect and Easy VPN scenarios and will not be covered here.



## Configuring Local Authentication

Configuration Scenario

- Configuration procedure identical to Cisco AnyConnect and Easy VPNs
- Clientless-specific parameters visible through Configuration > Remote Access VPN > Clientless SSL VPN Access menu

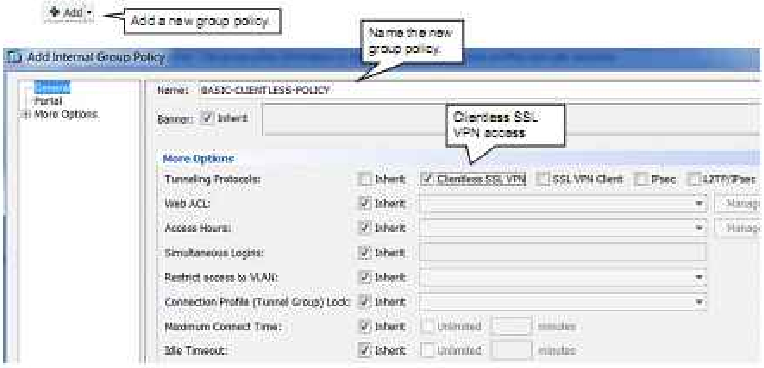
This figure presents the configuration scenario that is used in upcoming configuration tasks. On the Cisco ASA adaptive security appliance, you will create a custom connection profile named BASIC-CLIENTLESS-PROFILE, and a related group policy named BASIC-CLIENTLESS-POLICY. A user named "vpnuser" exists in the local user database.

The configuration procedure that is shown here is identical to Cisco AnyConnect and Easy VPNs. It is presented to illustrate the reusability of configuration components for the various VPN types. The group policies and connection profiles can be configured and edited in either of the two configuration menus:

- **Configuration > Remote Access VPN > Clientless SSL VPN Access**: This menu allows you to view and configure parameters that are specific to clientless SSL VPNs. The group policies and connection profiles that are defined in **Configuration > Remote Access VPN > Network (Client) Access** also appear here.
- **Configuration > Remote Access VPN > Network (Client) Access:** This menu allows you to view and configure parameters specific to full tunnel VPNs (Cisco AnyConnect VPN and IPsec clients). The group policies and connection profiles that are defined in **Configuration > Remote Access VPN > Clientless SSL VPN Access** also appear here.

## Configuring Local Authentication

### Task 1A: Create a Custom Group Policy



Add a new group policy.

Name the new group policy.

Clientless SSL VPN access

Add Internal Group Policy

Name: BASIC-CLIENTLESS-POLICY

Banner: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit ☑ Clientless SSL VPN □ SSL VPN Client □ IPsec □ L2TP/IPsec

Web ACL: ☑ Inherit

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Connection Profile (Tunnel Group) Lock: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

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

In the first configuration task, you will create a custom group policy that you will apply to VPN users. Perform the following steps:

**Step 1** In Cisco ASDM, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**.

**Step 2** Click **Add** to create a new policy.

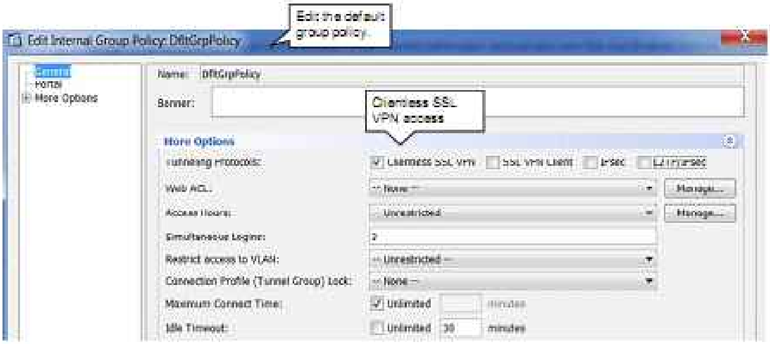
**Step 3** Provide a name for the new group policy (BASIC-CLIENTLESS-POLICY in this example).

**Step 4** Uncheck the **Inherit** check box, check the **Clientless SSL VPN** check box in the Tunneling Protocols option, and uncheck all other tunneling protocols.

**Step 5** Click **OK** and **Apply**, and then click **Save** to save your configuration, if necessary.

## Configuring Local Authentication

### Task 1B: Modify the Default Group Policy



Edit the default group policy.

Clientless SSL VPN access

Edit Internal Group Policy: DfltGrpPolicy

- General
- Portal
- More Options

Name: DfltGrpPolicy

Banner:

**More Options**

Tunneling Protocols: ☑ Clientless SSL VPN □ SSL VPN Client □ IPsec □ L2TP/IPsec

Web ACL: -- None --

Access Hours: -- Unrestricted --

Simultaneous Logins: 3

Restrict access to VLAN: -- Unrestricted --

Connection Profile (Tunnel Group) Lock: -- None --

Maximum Connect Time: ☑ Unlimited minutes

Idle Timeout: □ Unlimited 30 minutes

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

Alternatively, you may modify the default group policy to support clientless SSL VPN connections. Perform the following steps:

**Step 1** In Cisco ASDM, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**, select the **DfltGrpPolicy**, and click the **Edit** button to edit it.

**Step 2** In the Edit Internal Group Policy window, check the **Clientless SSL VPN** check box in the Tunneling Protocols section, and uncheck all other tunneling protocols.

---

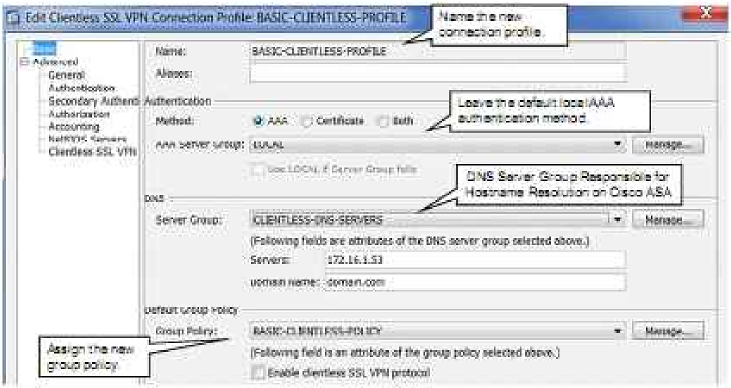
**Note** If your Cisco ASA adaptive security appliance will support other VPN access options, you may need to leave some of other tunneling protocols enabled.

---

**Step 3** Click **OK** and **Apply**, and then click **Save** to save your configuration, if necessary.

## Configuring Local Authentication

### Task 2: Create a Custom Connection Profile



Edit Clientless SSL VPN Connection Profile: BASIC-CLIENTLESS-PROFILE

Name: BASIC-CLIENTLESS-PROFILE

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: CLIENTLESS-DNS-SERVERS

(Following fields are attributes of the DNS server group selected above.)

Servers: 172.16.1.53

Domain Name: domain.com

Default Group Policy

Group Policy: BASIC-CLIENTLESS-POLICY

(Following field is an attribute of the group policy selected above.)

□ Enable clientless SSL VPN protocol

Name the new connection profile.

Leave the default local AAA authentication method.

DNS Server Group Responsible for Hostname Resolution on Cisco ASA

Assign the new group policy.

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

In the second configuration task, you will create a custom connection profile. Perform the following steps:

**Step 1** In Cisco ASDM, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**, and click **Add** to add a new connection profile.

**Step 2** Provide a name for the new connection profile (BASIC-CLIENTLESS-PROFILE in this example).

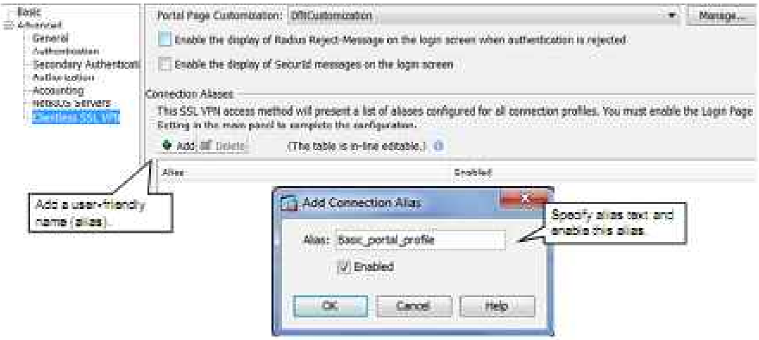
**Step 3** In the Authentication area, leave the authentication method at its default settings (local AAA authentication).

**Step 4** In the DNS section, select the configured DNS server group (CLIENTLESS-DNS-SERVERS) from the Server Group drop-down list.

**Step 5** In the Default Group Policy area, select the custom group policy (BASIC-CLIENTLESS-POLICY in this example) from the Group Policy drop-down list.

## Configuring Local Authentication

### Task 3: Define Alias for Connection Profile



Portal Page Customization: DfltCustomization

□ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

□ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

(The table is in-line editable.)

Alias: Basic_portal_profile

☑ Enabled

Add a user-friendly name (alias).

Specify alias text and enable this alias.

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

Next, you will create an alias for this new profile, using the following steps:

**Step 1** In the same connection profile edit window, navigate to the **Advanced > Clientless SSL VPN** subpane, and click **Add** in the Connection Aliases section.

**Step 2** Assign a name to this connection profile. Use a user-friendly name, because this name will be visible to your VPN users in their browsers. In this example, the name Basic_portal_profile is used.

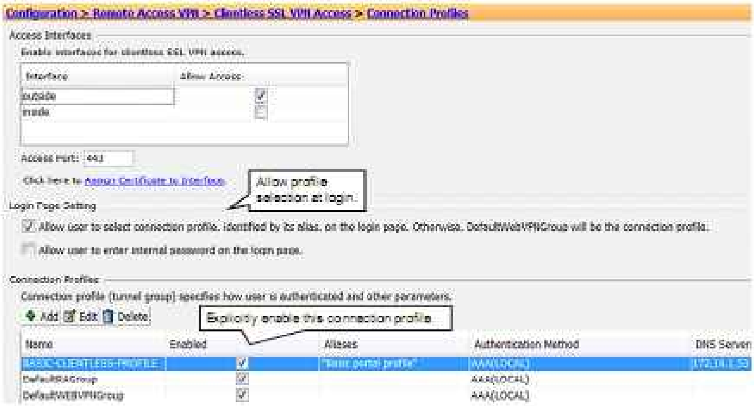
**Step 3** Click **OK** in the Add Connection Alias window.

**Step 4** Click **OK** in the Connection Profile window.

**Step 5** Click **Apply,** and click **Save** to save your configuration if necessary.

## Configuring Local Authentication

### Task 4: Allow Profile Selection



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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

| Interface | Allow Access |
|---|---|
| outside | ☑ |
| inside | □ |

Access Port: 443

Click here to Assign Certificate to Interface.

Login Page Setting

☑ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

□ Allow user to enter internal password on the login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

| Name | Enabled | Aliases | Authentication Method | DNS Server |
|---|---|---|---|---|
| BASIC-CLIENTLESS-PROFILE | ☑ | "Basic portal profile" | AAA(LOCAL) | 172.16.1.53 |
| DefaultRAGroup | ☑ | | AAA(LOCAL) | |
| DefaultWEBVPNGroup | ☑ | | AAA(LOCAL) | |

Allow profile selection at login.

Explicitly enable this connection profile.

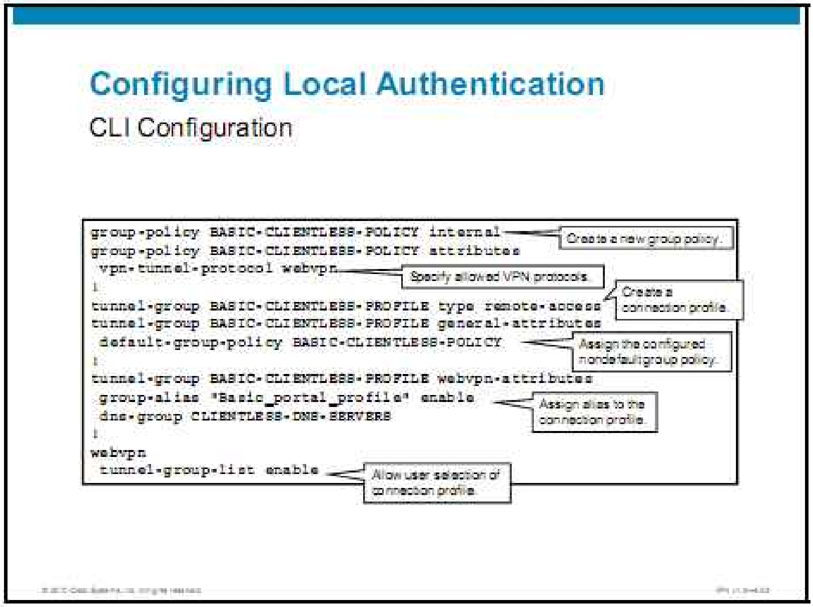
Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles

Finally, you will allow profile selection, and enable the configured profile for use in clientless SSL VPNs. Continue with the following steps:

**Step 1** In the Connection Profiles pane, in the Login Page Setting area, check the **Allow User to Select Connection Profile** check box to allow users to select their connection profile at login. This setting is required. Later in this lesson, you will lock VPN users to a particular profile.

**Step 2** In the Connection Profiles area, check the **Enabled** check box of the newly created connection profile (BASIC-CLIENTLESS-PROFILE here).

**Step 3** Click **Apply,** and click **Save** to save your configuration if necessary.



## Configuring Local Authentication

CLI Configuration

```
group-policy BASIC-CLIENTLESS-POLICY internal
group-policy BASIC-CLIENTLESS-POLICY attributes
 vpn-tunnel-protocol webvpn
!
tunnel-group BASIC-CLIENTLESS-PROFILE type remote-access
tunnel-group BASIC-CLIENTLESS-PROFILE general-attributes
 default-group-policy BASIC-CLIENTLESS-POLICY
!
tunnel-group BASIC-CLIENTLESS-PROFILE webvpn-attributes
 group-alias "Basic_portal_profile" enable
 dns-group CLIENTLESS-DNS-SERVERS
!
webvpn
 tunnel-group-list enable
```

Create a new group policy.

Specify allowed VPN protocols.

Create a connection profile.

Assign the configured nondefault group policy.

Assign alias to the connection profile.

Allow user selection of connection profile.

To enable local authentication for clientless SSL VPN connections, use the following CLI commands. First, use the **group-policy internal** command to create a new internal group policy. Then use the **vpn-tunnel-protocol webvpn** command inside group-policy attributes configuration mode to specify allowed VPN protocols.

Next, create a new, custom connection profile (BASIC-CLIENTLESS-PROFILE) using the **tunnel-group** command, and attach the custom BASIC-CLIENTLESS-POLICY group policy to this connection profile using the **default-group-policy** command in its general-attributes section. Also, in the webvpn-attributes section of the tunnel group, assign a user-friendly connection profile alias to this connection profile using the **group-alias** command, and enable it using the **enable** parameter. Use the **dns-group** command to specify the DNS group that will be used by the Cisco ASA adaptive security appliance to resolve domain names inside a clientless SSL request.

Finally, enter webvpn configuration mode and enable user connection profile selection using the **tunnel-group-list enable** 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 |
|---|---|
| **external server-group** *server_group* | Specifies the group policy as external and identifies the AAA server group for the adaptive security appliance to query for attributes |
| **from** *group-policy_name* | Initializes the attributes of this internal group policy to the values of a preexisting group policy |
| **internal** | Identifies the group policy as internal |
| *name* | 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." |
| **password** *server_password* | 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 |
|---|---|
| *name* | Specifies the name of the group policy |

## vpn-tunnel-protocol

To configure a VPN tunnel type (IP Security [IPSec], Layer 2 Tunneling Protocol [L2TP] over IPSec, SSL VPN client [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 |
|---|---|
| **IPSec** | 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. |
| **l2tp-ipsec** | Negotiates an IPsec tunnel for an L2TP connection. |
| **svc** | Negotiates an SSL VPN tunnel with an SSL VPN client. |
| **webvpn** | Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client. |

## 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 |
|---|---|
| *name* | Specifies the name of the tunnel group. This name can be any string that you choose. If the name is an IP address, it is usually the IP address of the peer. |
| *type* | Specifies the type of tunnel group:<br>■ **remote-access:** Allows a user to connect using either IPsec remote access or WebVPN (portal or tunnel client)<br>■ **ipsec-l2l:** Specifies IPsec LAN-to-LAN, which allows two sites or LANs to connect securely across a public network like the Internet.<br>**Note** The following tunnel group types are deprecated in Cisco ASA Software Version 8.0(2):<br>**– ipsec-ra**: IPsec remote access<br>**– webvpn**: WebVPN<br>The adaptive security appliance converts these to the remote access type. |

## tunnel-group general-attributes

To enter 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 |
|---|---|
| **general-attributes** | Specifies attributes for this tunnel group |
| *name* | 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 |
|---|---|
| *group-name* | 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 |
|---|---|
| **webvpn-attributes** | Specifies WebVPN attributes for this tunnel group |
| *name* | 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 |
|---|---|
| **disable** | Disables the group alias. |
| **enable** | Enables a previously disabled group alias. |
| *name* | Specifies the name of a tunnel group alias. This can be any string that you choose, except that the string cannot contain spaces. |

## dns-group (tunnel-group webvpn configuration mode)

To specify the DNS server to use for a WebVPN tunnel group, use the **dns-group** command in tunnel-group webvpn configuration mode. To restore the default DNS group, use the **no** form of this command.

**dns-group** *name*

### dns-group (tunnel-group webvpn configuration mode) Parameters

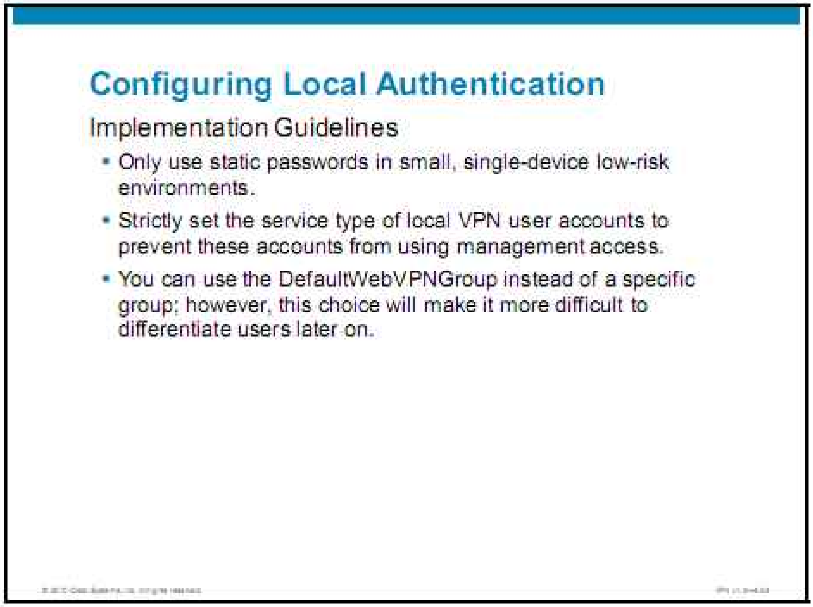
| Parameter | Description |
|---|---|
| *name* | Specifies the name of the DNS server group configuration to use for the tunnel group. |

## 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, as well as the appearance of WebVPN screens that end users see.

**webvpn**



## Configuring Local Authentication

Implementation Guidelines

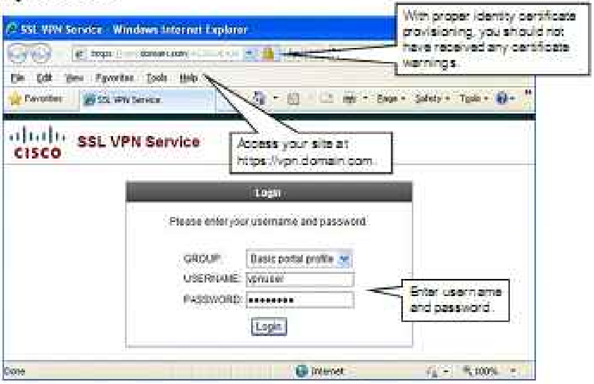
- Only use static passwords in small, single-device low-risk environments.
- Strictly set the service type of local VPN user accounts to prevent these accounts from using management access.
- You can use the DefaultWebVPNGroup instead of a specific group; however, this choice will make it more difficult to differentiate users later on.

Similar to full tunneling SSL VPNs, consider the following implementation guidelines when implementing local AAA authentication in a clientless SSL VPN solution:

- Only use user authentication with static passwords and the local database in small, single gateway, low-risk environments because these passwords are reusable and typically easy to guess.
- Always strictly set the service type of the user to only allow VPN access. This policy is extremely important to prevent unauthorized access to Cisco ASA adaptive security appliance management functions.
- In this topic, all examples used a custom connection profile and a custom group policy. If all of your users share the same authentication method, and access policies, you could also implement local AAA authentication by using only the DefaultWebVPNGroup connection profile and the default group policy.

## Verifying Local Authention

Verify Access



SSL VPN Service - Windows Internet Explorer
File Edit View Favorites Tools Help
Favorites
SSL VPN Service
Page ▾ Safety ▾ Tools ▾
SSL VPN Service
Done
Internet
100%

With proper identity certificate provisioning, you should not have received any certificate warnings.

Access your site at https://vpn.domain.com.

**Login**

Please enter your username and password.

GROUP: Basic portal profile

USERNAME: vpnuser

PASSWORD: ••••••••

Login

Enter username and password.

At this point, you should be able to access the SSL VPN portal, without access restrictions to internal resources.

At this point in your configuration flow, you should already be able to access basic features of the SSL VPN, without any access restrictions for authenticated users.

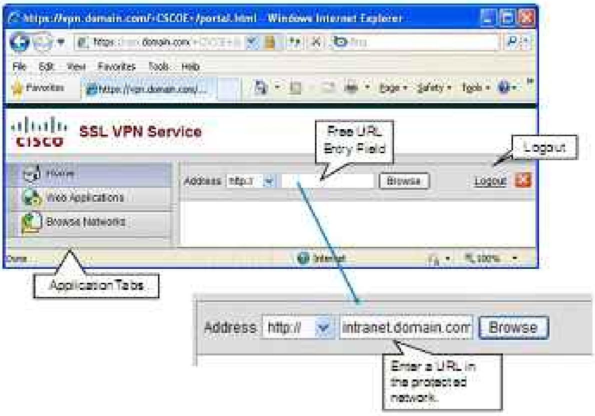
On your client system, open a browser and navigate to the HTTPS URL of the Cisco ASA adaptive security appliance outside interface. In this configuration example, the outside interface of the appliance is reachable at https://vpn.domain.com, and vpn.domain.com is also the canonical name ( that is used inside the Cisco ASA adaptive security appliance identity certificate.

The browser should open the SSL VPN login page without any certificate warnings if the Cisco ASA adaptive security appliance is using an identity certificate from a global PKI provider. If you observe certificate warnings, it is imperative that you remedy this problem before production use.

On the login page, enter the username and password (vpnuser/password) to log into the SSL VPN portal. You can see that the alias of the connection profile is listed in the GROUP drop-down box.

## Verifying Local Authentication

Default Portal User Interface


https://vpn.domain.com/+CSCOE+/portal.html - Windows Internet Explorer
File Edit View Favorites Tools Help
SSL VPN Service
Home
Web Applications
Browse Networks
Address http://
Browse
Logout
Free URL Entry Field
Logout
Application Tabs
Address http:// intranet.domain.com
Browse
Enter a URL in the protected network.

This figure shows the default SSL VPN portal interface as is seen by the clientless SSL VPN user. You can fully customize this page, as you will learn in the upcoming lessons in this course.

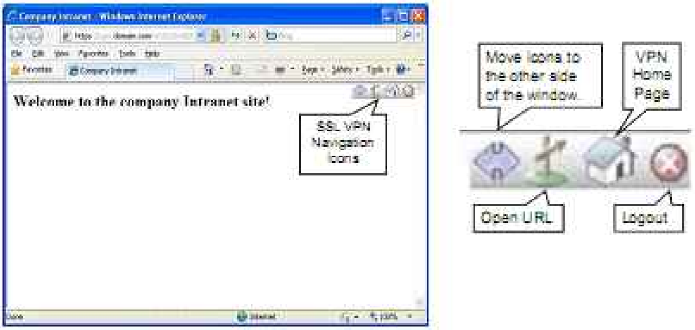
On the left side of the default portal, you can see application tabs that invoke specific views of the portal. The Web Applications view will invoke a portal view that only displays the preconfigured links (bookmarks) to web applications. The Browse Networks view will invoke a portal view that only displays the preconfigured links (bookmarks) to file shares and the file-share browsing interface.

By default, the portal will include a URL entry field, which allows users to enter a URL of their choice. By clicking Browse, the Cisco ASA adaptive security appliance SSL VPN portal will retrieve the requested resource and display it in the browser window.

**Note** The prefix to the URL path in the browser changes depending on whether you require authentication. The security appliance uses /+CSCOE+/ for objects that require authentication, and /+CSCOU+/ for objects that do not. The security appliance displays /+CSCOE+/ objects on the portal page only, while /+CSCOU+/ objects are visible and usable in either the login or the portal pages.

## Verifying Local Authentication

Portal User Interface



Welcome to the company Intranet site!

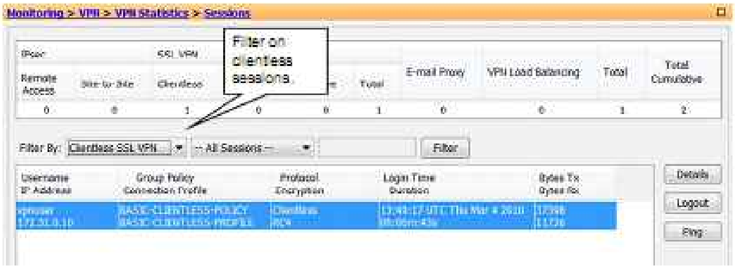
Company Intranet - Windows Internet Explorer
SSL VPN Navigation Icons
Move icons to the other side of the window
VPN Home Page
Open URL
Logout

When you navigate to a resource over clientless SSL VPN, the browser will display navigation icons as a floating toolbar at the top of its content window. You can use these icons anytime to return to the home page, open an URL over the clientless SSL VPN session (if allowed), move the toolbar to the other side of the content window, or close (logout) your SSL VPN session.

**Note** Never use the home page button of the browser during a clientless session because this action will cause you to navigate away from the SSL VPN portal.

## Verifying Local Authentication

Cisco ASDM



Monitoring > VPN > VPN Statistics > Sessions

Filter on clientless sessions.

| IPsec |  | SSL VPN |  |  |  | E-mail Proxy | VPN Load Balancing | Total | Total Cumulative |
|---|---|---|---|---|---|---|---|---|---|
| Remote Access | Site-to-Site | Clientless |  |  | Total |  |  |  |  |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 2 |

Filter By: Clientless SSL VPN ▾ -- All Sessions -- ▾ Filter

| Username<br>IP Address | Group Policy<br>Connection Profile | Protocol<br>Encryption | Login Time<br>Duration | Bytes Tx<br>Bytes Rx |
|---|---|---|---|---|
| vpnuser<br>172.31.0.10 | BASIC-CLIENTLESS-POLICY<br>BASIC-CLIENTLESS-PROFILE | Clientless<br>RC4 | 13:41:17 UTC Thu Mar 4 2010<br>0h:06m:43s | 17398<br>11726 |

Monitoring > VPN > VPN Statistics > Sessions

To verify the clientless connection for your client on the Cisco ASA adaptive security appliance, use Cisco ASDM, and navigate to the **Monitoring > VPN > VPN Statistics > Sessions** pane. Choose **Clientless SSL VPN** in the Filter By field. The VPN session should be displayed in the main pane.

## Verifying Local Authentication

CLI

```
ASA# show vpn-sessiondb webvpn

Session Type: WebVPN

Username     : vpnuser                Index        : 47
Public IP    : 172.31.0.11
Protocol     : Clientless
License      : SSL VPN
Encryption   : RC4                    Hashing      : SHA1
Bytes Tx     : 97718                  Bytes Rx     : 13227
Group Policy : BASIC-CLIENTLESS-POLICY
Tunnel Group : BASIC-CLIENTLESS-PROFILE
Login Time   : 12:47:35 UTC Tue Mar 9 2010
Duration     : 0h:01m:37s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

In the CLI, use the **show vpn-sessiondb webvpn** command to obtain information that is similar to the information from Cisco ASDM.

## 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

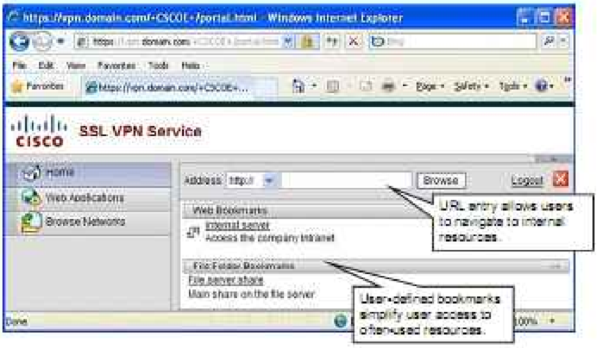
| Parameter | Description |
|---|---|
| `detail` | (Optional) Displays extended details about a session. For example, using the **detail** option for an IPsec session displays additional details such as the Internet Key Exchange (IKE) hashing algorithm, authentication mode, and rekey interval.<br>If you choose **detail**, and the **full** option, the adaptive security appliance displays the detailed output in a machine-readable format. |
| `filter` *`filter_criteria`* | (Optional) Filters the output to display only the information that you specify by using one or more of the filter options. |
| `full` | (Optional) Displays streamed, untruncated output. Output is delineated by \| characters and a \|\| string between records. |
| *`session_type`* | (Optional) To show data for a specific session type, enter one of the following keywords:<br>■ **email-proxy:** Displays email-proxy sessions.<br>■ **index** *indexnumber*: Displays a single session by index number. Specify the index number for the session, 1–750.<br>■ **l2l:** Displays VPN LAN-to-LAN session information.<br>■ **ratio**: Displays VPN session protocol or encryption ratios.<br>■ **remote:** Displays IPsec remote access sessions.<br>■ **summary:** Displays the VPN session summary.<br>■ **svc:** Displays SSL VPN Client sessions.<br>■ **vpn-lb:** Displays VPN Load-Balancing management sessions.<br>■ **webvpn:** Displays information about clientless SSL VPN sessions. |
| `sort` *`sort_criteria`* | (Optional) Sorts the output according to the sort option that you specify. |

# Configuring Basic Portal Features and Access Control

This topic describes how to configure and verify basic portal features and access control in a clientless SSL VPN.

## Configuring Basic Portal Features

URL Entry and Bookmarks



URL entry allows users to navigate to internal resources.

User-defined bookmarks simplify user access to often-used resources.

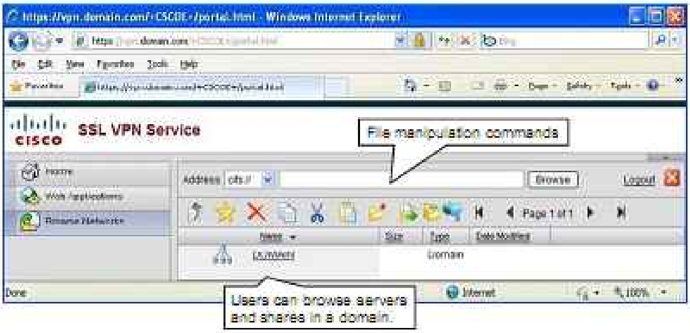
By default, the Cisco ASA adaptive security appliance SSL VPN portal will not restrict users and allows authenticated users access to all internal resources. It also provides several ease-of-use interface features. You can use basic portal tuning to control basic portal appearance by enabling or disabling some of its user interface functions.

This figure shows two main basic features of the Cisco ASA adaptive security appliance SSL VPN portal. The first feature is the URL entry, which allows users to specify the URL of the resource they want to access, and the second is user-defined bookmarks, with which the administrator can specify a list of often-used resources for users to navigate too quickly. When a user logs in to the SSL VPN portal, all bookmarks that are enabled in the group policy of the user are displayed on the portal home page. In addition to the bookmark list, the URL entry field is displayed at the top of the interface. By tuning portal functions, you can enable or disable either of these two features.

These are the protocols that can be used to access resources using URL entry or bookmarks: HTTP, HTTPS, CIFS, and FTP.

## Configuring Basic Portal Features

### Network File Server Access

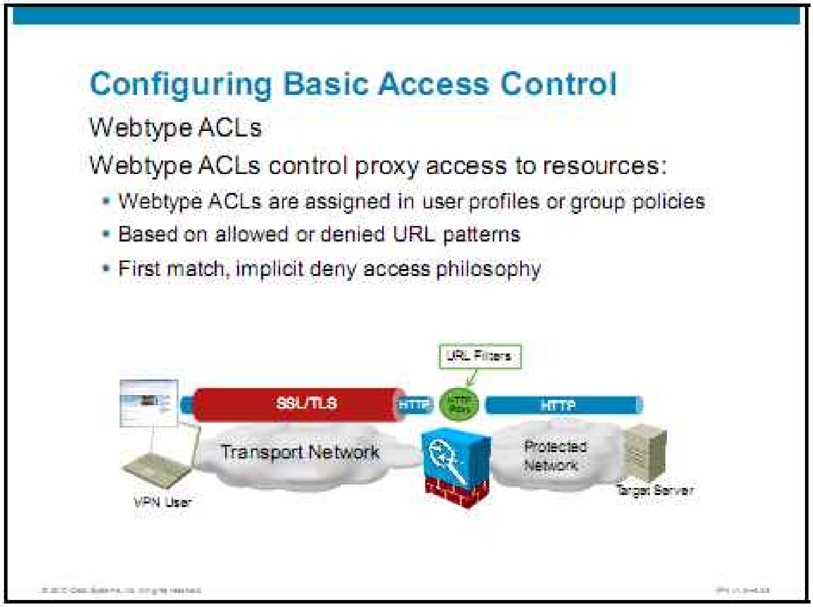


File manipulation commands

Users can browse servers and shares in a domain.

Another basic SSL VPN portal feature is the ability to allow users to access Common Internet File System (CIFS) file shares, and browse a CIFS network using a browser interface. This ability allows for easy interoperability with Microsoft Windows Server file servers, by presenting a Windows Explorer-like user interface within the browser. Using portal tuning features, you can permit or deny access to this file browsing interface.

The same user interface is also presented when you access an FTP server using FTP protocol.



## Configuring Basic Access Control

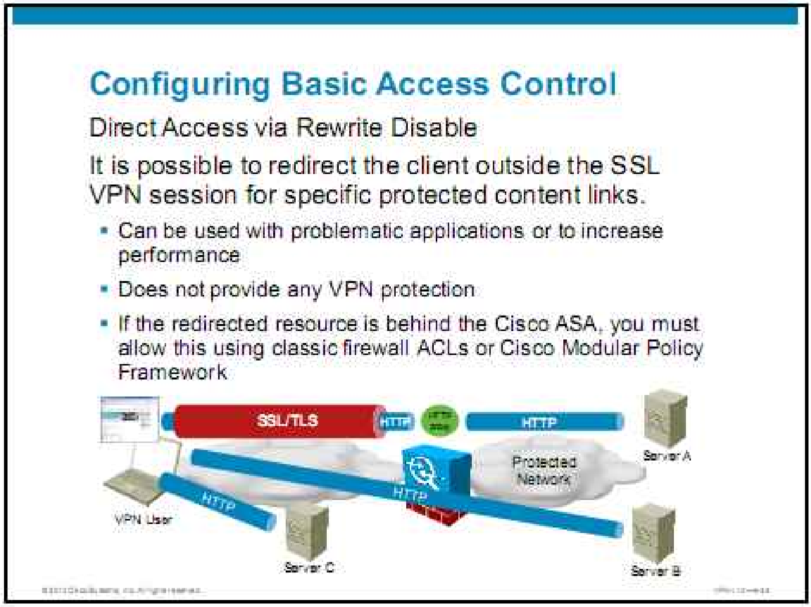
Webtype ACLs

Webtype ACLs control proxy access to resources:

- Webtype ACLs are assigned in user profiles or group policies
- Based on allowed or denied URL patterns
- First match, implicit deny access philosophy

The Cisco ASA clientless SSL VPN feature does not use the Cisco ASA adaptive security appliance interface access control lists (ACLs) and Cisco Modular Policy Framework (MPF) access control model, but enforces its own access control by using webtype ACLs. Webtype ACLs are per-user or per-group ACLs that permit or deny access to URLs reachable over the SSL VPN portal. You can use URL patterns to specify the allowed or denied URLs, and use multiple rules inside a webtype ACL. Webtype ACLs use the same evaluation logic as classic Cisco ASA adaptive security appliance ACLs: the first matched rule dictates the permit or deny action, and there is an implicit deny-all statement at the end of the ACL.

**Note** Note that enabling or disabling portal features such as URL entry and bookmarks does not prevent the user from accessing internal resources, but only removes the relevant user interface options. If users know how to properly construct the rewritten internal URL and enter it in the browser Address field, they can still access the resource behind the Cisco ASA adaptive security appliance, if properly authenticated. Therefore, you *must* deploy webtype ACLs if you want to reliably control access to internal resources.



## Configuring Basic Access Control

Direct Access via Rewrite Disable

It is possible to redirect the client outside the SSL VPN session for specific protected content links.

- Can be used with problematic applications or to increase performance
- Does not provide any VPN protection
- If the redirected resource is behind the Cisco ASA, you must allow this using classic firewall ACLs or Cisco Modular Policy Framework

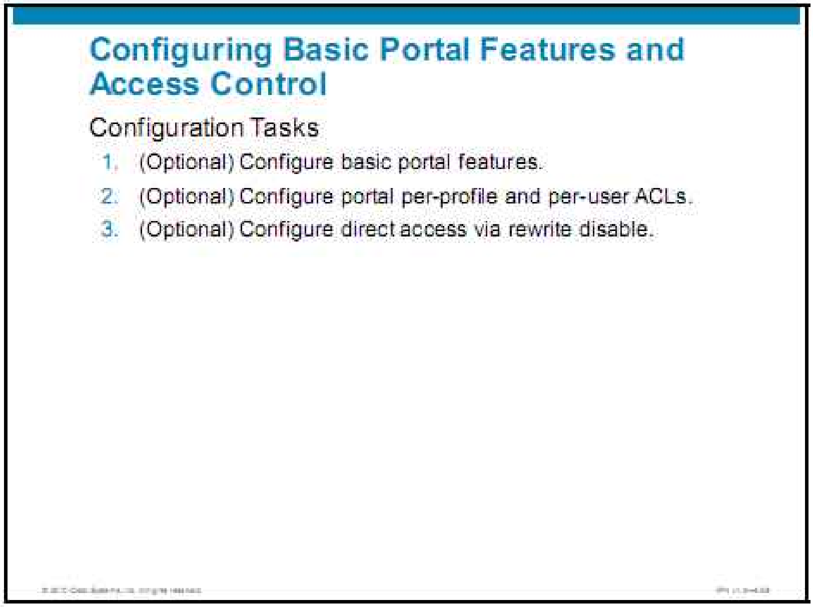
Just as full tunnel VPNs can be configured to allow some traffic to bypass the tunnel, you can configure clientless SSL VPNs in a similar manner. You can use such direct access for servers that are hosting problematic content that the Cisco ASA adaptive security appliance has problems rewriting. You can also use direct access to increase performance by avoiding access via the proxy.

**Note** Note that in clientless SSL VPNs, you can always bypass the SSL VPN session to access resources in the transport network (that is, not behind the Cisco ASA adaptive security appliance) by just opening another browser session and navigating directly to the resources.

Direct access via rewrite disable is useful for clientless VPNs to directly access resources that are linked to protected content that is retrieved over the portal. Normally, any links in documents that you retrieve over the SSL VPN portal will be rewritten by the Cisco ASA adaptive security appliance, which will force the browsing session of the user to always access these links over the SSL VPN portal. You can specify that certain links should not be rewritten, causing the browser of the client to directly access the destination server, bypassing the SSL VPN gateway proxy function.

**Note** Note that resources that you access directly are not protected by the SSL VPN encapsulation.

If the bypassed resource is located in the network outside the Cisco ASA adaptive security appliance SSL VPN gateway, access to that resource requires no further configuration. However, if the resource that is configured for direct access is behind the Cisco ASA adaptive security appliance SSL VPN gateway, you will have to modify Cisco ASA adaptive security appliance interface ACLs or MPF rules to enable such direct access. This direct access is no different from any other access through the Cisco ASA adaptive security appliance, and it is subject to the classic firewall access policy.



## Configuring Basic Portal Features and Access Control

### Configuration Tasks

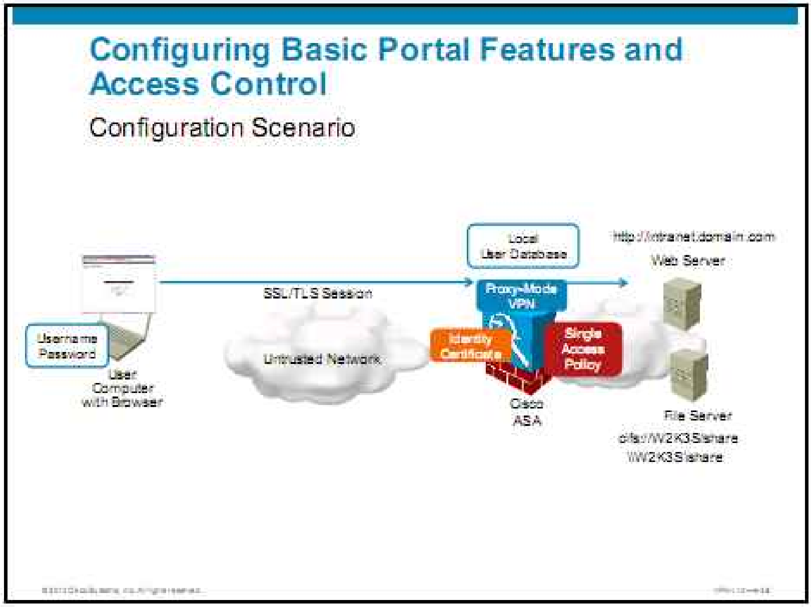
1. (Optional) Configure basic portal features.
2. (Optional) Configure portal per-profile and per-user ACLs.
3. (Optional) Configure direct access via rewrite disable.

To configure basic portal features and access control in a basic clientless solution, you will perform some of the following configuration tasks:

1. Optionally, you can enable, disable, and tune the basic SSL VPN portal user-interface features.

2. Optionally, configure per-user or per-group-policy webtype ACLs to implement per-user or per-group access policies.

3. Optionally, configure direct access via rewrite disable feature to enable remote clients to directly access specific resources.



## Configuring Basic Portal Features and Access Control

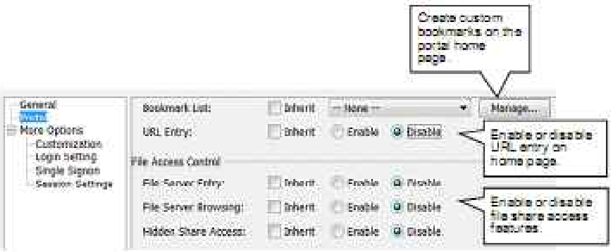
Configuration Scenario

This figure presents the configuration scenario that is used in upcoming configuration tasks. Remote users will only be allowed to access a single web server (http://intranet.domain.com) in the protected network, and a single file server (cifs://W2K3S). You should create predefined bookmarks to access the web server home page and the file share named "share" on the W2K3S file server. To browse the W2K3S server and possibly the rest of the Windows domain, you will configure the Cisco ASA adaptive security appliance to consult the internal Microsoft Windows name server (WINS/NetBIOS name service) to resolve CIFS hostnames.

You will also configure direct access to all servers in the Cisco.com domain, disabling the rewrite if links to Cisco.com are present in the content that is retrieved over the SSL VPN portal.

## Configuring Basic Portal Features and Access Control

Task 1: (Optional) Configure Basic Portal Features



Bookmark List: □ Inherit -- None --

URL Entry: □ Inherit ○ Enable ● Disable

File Access Control

File Server Entry: □ Inherit ○ Enable ● Disable

File Server Browsing: □ Inherit ○ Enable ● Disable

Hidden Share Access: □ Inherit ○ Enable ● Disable

Create custom bookmarks on the portal home page.

Enable or disable URL entry on home page.

Enable or disable file share access features.

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

In the first task, you will control some basic SSL VPN portal user interface features, namely, the presence of predefined bookmarks on the portal home page for a specific user group, the ability for users to freely enter URLs on the portal, and file share access features.

Complete the following steps:

**Step 1** In Cisco ASDM, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**, and click **Edit** to edit the group policy that applies to a user group (in this case, the BASIC-CLIENTLESS-POLICY).

**Step 2** Inside the **Edit Internal Group Policy** window, navigate to the Portal subpage.

**Step 3** If you want to create a bookmark list for this policy, click **Manage** in the Bookmark List row. The process of bookmark list creation is explained in the next pages of this topic.

**Step 4** If you want to enable or disable URL entry for this policy, click the **Enable** or **Disable** radio button in the URL Entry row.

**Step 5** If you want to enable or disable the possibility for users to enter a path to an internal file share in the SSL VPN portal Browse Networks view, click the **Enable** or **Disable** radio button in the File Server Entry row.

**Step 6** If you want to enable or disable the possibility for users to browse the file server network in the SSL VPN portal Browse Networks view, click the **Enable** or **Disable** radio button in the File Server Browsing row.

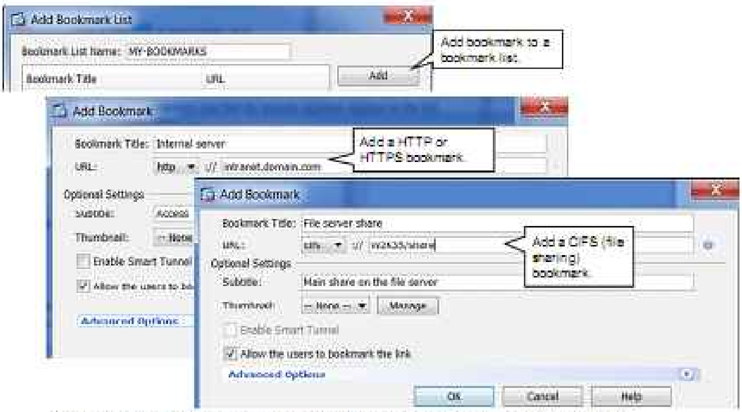
**Step 7** If you want to allow or deny access to hidden CIFS shares (shares whose name ends in the $ characters), click the **Enable** or **Disable** radio button in the Hidden Share Access row.

**Step 8** Click **OK** in the Edit Internal Group Policy window.

**Step 9** Click **Apply,** and click **Save** to save your configuration, if needed.

## Configuring Basic Portal Features and Access Control

### Task 1: (Optional) Configure Basic Portal Features



Bookmark List Name: MY-BOOKMARKS

Bookmark Title | URL

Add bookmark to a bookmark list.

Bookmark Title: Internal server

URL: http :// intranet.domain.com

Add a HTTP or HTTPS bookmark.

Optional Settings

Subtitle: Access

Thumbnail: -- None

□ Enable Smart Tunnel

☑ Allow the users to bo

Bookmark Title: File server share

URL: cifs :// W2K3S/share

Add a CIFS (file sharing) bookmark.

Optional Settings

Subtitle: Main share on the file server

Thumbnail: -- None --

□ Enable Smart Tunnel

☑ Allow the users to bookmark the link

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

A bookmark list is a set of URLs that is configured to be displayed in the clientless SSL VPN portal for a group of users sharing the same group policy. By default, there are no configured bookmark lists, and the network administrator must configure them.

To create a bookmark list inside a group policy, complete the following steps:

**Step 1** Inside the Edit Internal Group Policy window, click **Manage** to create a new bookmark list.

**Step 2** Click **Add** to add a bookmark list.

**Step 3** Configure the bookmark list name (MY-BOOKMARKS in this example) and click **Add** to create individual bookmarks for this list. The Add Bookmark Entry window appears. The creation of a bookmark entry is covered next.

To create a web application (HTTP or HTTPS) bookmark in the bookmark list, complete the following steps:

**Step 1** Configure a name for the bookmark in the **Bookmark Title** field.

**Step 2** Configure the URL value for the bookmark as HTTP or HTTPS.

**Step 3** Configure the server HTTP or HTTPS URL to be used with the bookmark entry.

**Step 4** Optionally, configure the bookmark subtitle. The subtitle will appear under the bookmark entry on the web portal.

**Step 5** Optionally, configure the thumbnail picture to be used with this bookmark entry.

**Step 6** Click **OK**, **OK**, and **Apply,** and click **Save** to save your configuration, if needed.

**Note** To use thumbnails with bookmarks, they must first be uploaded to the Cisco ASA adaptive security appliance.

In this figure, a web application bookmark named "Internal server" has been created. The bookmark has been given an URL of http://intranet.domain.com.

To create a file share (CIFS) bookmark in the bookmark list, complete the following steps:

**Step 1** Configure a name for the bookmark in the **Bookmark Title** field.

**Step 2** Configure the URL value for the bookmark as CIFS.

**Step 3** Configure the server CIFS URL to be used with the bookmark entry.

**Step 4** Optionally, configure the bookmark subtitle. The subtitle will appear under the bookmark entry on the web portal.

**Step 5** Optionally, configure the thumbnail to be used with this bookmark entry.

**Step 6** Click **Ok**, **Ok**, and **Apply**, and click **Save** to save your configuration, if needed.

In this figure, a CIFS bookmark named "File server share" has been created. The target CIFS URL is cifs://W2K3S/share.

If you are using CIFS file share access, especially if you are not using bookmarks and want users to browse the network, you must configure appropriate CIFS name servers that the Cisco ASA adaptive security appliance will consult to obtain a list of file servers in a domain, together with their IP addresses. To configure a list of CIFS name servers, you should edit the relevant connection profile to which your users belong.

Perform the following steps (not shown in the figure):

**Step 1** Edit the connection profile to which your users belong.

**Step 2** Inside **the Edit Clientless SSL VPN Connection Profile** window, navigate to the **Advanced > NetBIOS Server** subpane.

**Step 3** Click **Add** to add a CIFS name server.

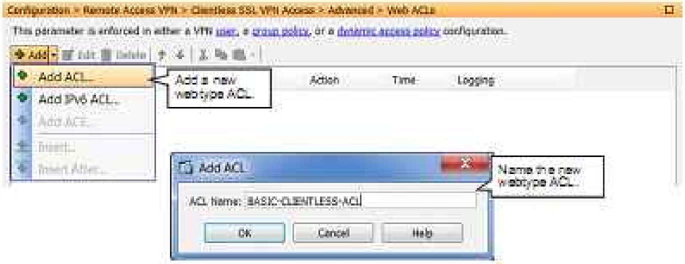
**Step 4** In the Add NetBIOS Server window, specify the IP address of the CIFS name server.

**Note** It is recommended that you add more than one CIFS name server for redundancy.

**Step 5** Click **OK**, **OK**, and **Apply**, and click **Save** to save your configuration, if needed.

## Configuring Basic Portal Features and Access Control

### Task 2: Configure per-Group and per-User ACLs


Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs
This parameter is enforced in either a VPN user, a group policy, or a dynamic access policy configuration.
Add
Edit
Delete
Add ACL...
Add IPv6 ACL...
Add ACE...
Insert...
Insert After...
Action
Time
Logging
Add ACL
OK
Cancel
Help

ACL Name: BASIC-CLIENTLESS-ACL

Add a new webtype ACL.

Name the new webtype ACL.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs

In the second task, you will configure a webtype ACL to limit access to internal resources, and apply the webtype ACL to a group policy that applies to your user group (connection profile).

To create a new webtype ACL, perform the following steps:

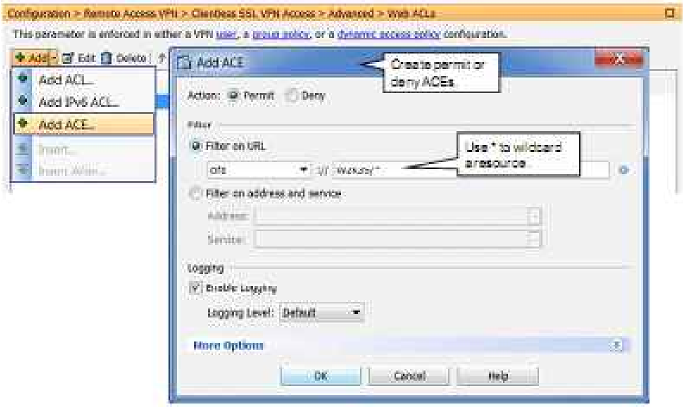
**Step 1** In Cisco ASDM, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**. An ACL manager window for webtype ACLs will open.

**Step 2** Choose **Add > Add ACL** to add a new webtype ACL.

**Step 3** In the Add ACL window, choose a unique name for the new webtype ACL.

## Configuring Basic Portal Features and Access Control

Task 2: Configure per-Group and per-User ACLs (Cont.)


Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs
This parameter is enforced in either a VPN user, a group policy, or a dynamic access policy configuration.
Add
Edit
Delete
Add ACL...
Add IPv6 ACL...
Add ACE...
Insert...
Insert After...
Add ACE
Filter
Address:
Service:
Logging
More Options
OK
Cancel
Help

Action: ● Permit ○ Deny

● Filter on URL: cifs ://W2K3S/*

○ Filter on address and service

☑ Enable Logging

Logging Level: Default

Create permit or deny ACEs

Use * to wildcard a resource

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs

**Step 4** Choose the newly created ACL in the ACL pane, and choose **Add > Add ACE** to add a rule (access control entry [ACE]) to the new webtype ACL.

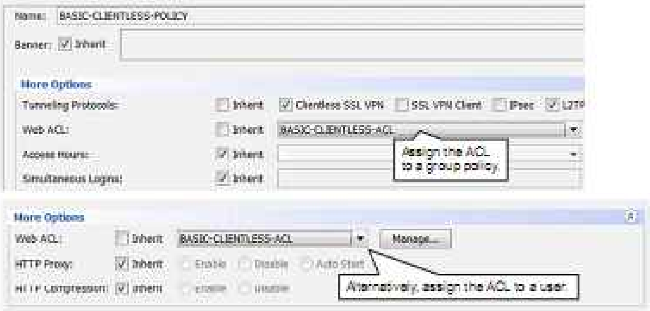
**Step 5** In the **Add ACE** window, enter the conditions that will control access to internal resources:

- Click the **Permit** or **Deny** radio button in the Action area.
- In the Filter area, click the **Filter on URL** radio button, and specify the URL pattern that you want to filter on. You can use the * character to make a resource a wildcard. In this example, the first ACE will allow all access to the intranet.domain.com web server, and the second ACE will allow access to any share on the W2K3S CIFS server.
- In the Logging area, you can enable specific logging for this ACE, similarly to the process for classic Cisco ASA adaptive security appliance ACLs.

**Step 6** Click **OK** and **Apply**, and click **Save** to save your configuration, if necessary.

## Configuring Basic Portal Features and Access Control

### Task 2: Configure per-Group and per-User ACLs (Cont.)



Name: BASIC-CLIENTLESS-POLICY

Banner: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit ☑ Clientless SSL VPN □ SSL VPN Client □ IPsec ☑ L2TP

Web ACL: □ Inherit BASIC-CLIENTLESS-ACL

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Assign the ACL to a group policy.

More Options

Web ACL: □ Inherit BASIC-CLIENTLESS-ACL Manage...

HTTP Proxy: ☑ Inherit ○ Enable ○ Disable ○ Auto Start

HTTP Compression: ☑ Inherit ○ Enable ○ Disable

Alternatively, assign the ACL to a user.

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

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

To apply the newly created webtype ACL to a group policy (and therefore one or more connection profiles), or to a user account, perform the following steps:

**Step 1** Choose **Configuration > Remote Access > Clientless SSL VPN Access > Group Policies** and edit a group policy that you want to assign the webtype ACL to (in this example, this is the BASIC-CLIENTLESS-POLICY group policy).

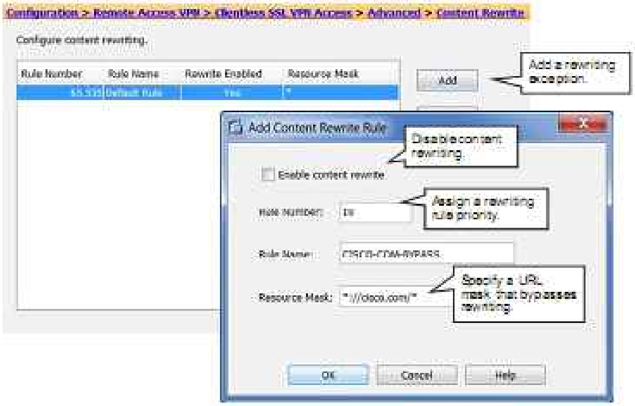
**Step 2** Expand the **More Options** area, uncheck the **Inherit** check box, and select the newly created webtype ACL in the Web ACL field.

**Step 3** Click **OK** and **Apply**, and click **Save** to save your configuration if needed.

Alternatively, if you need to apply this ACL only to a specific user, edit the profile of the user by choosing Configuration > Remote Access > AAA/Local Users > Local Users > Edit, and navigating to the VPN Policy > Clientless SSL VPN > More Options section of the profile of the user**.** Uncheck the **Inherit** check box, and select the newly created webtype ACL in the Web ACL field.

## Configuring Basic Portal Features and Access Control

### Task 3: Configure Direct Access via Rewrite Disable



Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Rewrite

Configure content rewriting.

| Rule Number | Rule Name | Rewrite Enabled | Resource Mask |
|---|---|---|---|
| 65,535 | Default Rule | Yes | * |

Add a rewriting exception.

Add Content Rewrite Rule

Disable content rewriting.

☐ Enable content rewrite

Rule Number: 10

Assign a rewriting rule priority.

Rule Name: CISCO-COM-BYPASS

Resource Mask: *://cisco.com/*

Specify a URL mask that bypasses rewriting.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Rewrite

In the optional Task 3, you can configure direct access and specify that the Cisco ASA adaptive security appliance SSL VPN proxy-rewriting engine should not rewrite specific URL patterns that are found inside protected content. In this example, any content referencing Cisco.com sites should not have these links rewritten. This configuration allows clientless users to click these links inside their SSL VPN session, and open direct connections to these sites.

To configure such direct access by disabling specific content rewriting functions, perform the following steps:

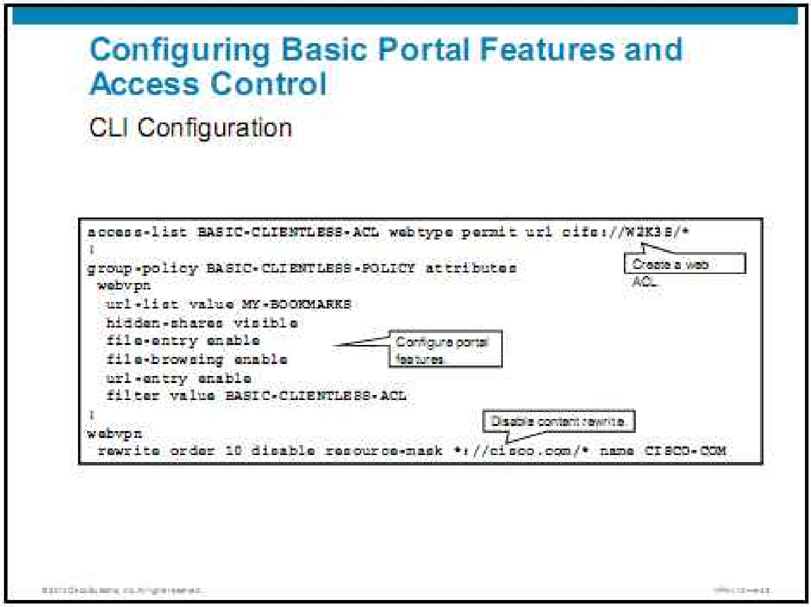
**Step 1** Choose **Configuration > Remote Access > Clientless SSL VPN Access > Advanced > Content Rewrite.**

**Step 2** Click **Add** to add a rewriting exception rule.

**Step 3** In the Add Content Rewrite Rule window, uncheck the **Enable Content Rewrite** check box, specify a rule number (if you have multiple rules, they are evaluated in order according to their sequence number), and assign the rule a user-friendly name.

**Step 4** In the Resource Mask field, specify the URL patterns that the Cisco ASA adaptive security appliance should not rewrite. In this example, the URL pattern is "*://cisco.com/*", meaning that any link using any protocol to the Cisco.com domain inside protected content should be left unmodified.

**Step 5** Click **OK** and **Apply**, and click **Save** to save your configuration if needed.



## Configuring Basic Portal Features and Access Control

CLI Configuration

```
access-list BASIC-CLIENTLESS-ACL webtype permit url cifs://W2K3S/*
!
group-policy BASIC-CLIENTLESS-POLICY attributes
 webvpn
  url-list value MY-BOOKMARKS
  hidden-shares visible
  file-entry enable
  file-browsing enable
  url-entry enable
  filter value BASIC-CLIENTLESS-ACL
!
webvpn
 rewrite order 10 disable resource-mask *://cisco.com/* name CISCO-COM
```

Create a web ACL.

Configure portal features.

Disable content rewrite.

This output shows the CLI commands that are required to configure the basic portal features and access control in clientless SSL VPNs.

Enter group-policy attributes configuration mode, and enter its webvpn submode. In this submode, use the **url-list** command to assign a bookmark list to the group policy. Use the **hidden-shares** command to allow or deny access to hidden CIFS shares and the **file-entry** command to allow or deny users to freely enter CIFS URLs in the Browse Networks view. Use the **file-browsing** command to allow free browsing of file servers and shares and the **url-entry** command to allow or deny free entry of URLs on the portal home page.

**Note** The bookmark lists cannot be configured using the CLI, because they are saved as XML files in the Cisco ASA adaptive security appliance flash file system (FFS).

To configure webtype ACLs and apply them to a group policy, first configure a webtype ACL using the **access-list** *name* **webtype** command. You can apply this webtype ACL to a group policy by using the **filter value** command in the webvpn submode of the group-policy attributes configuration mode.

To configure direct access by making content rewriting exceptions, enter the SSL VPN server configuration submode on the Cisco ASA adaptive security appliance using the **webvpn** command. Use the **rewrite** command to specify a new content rewriting exception rule, with a particular sequence number, specifying a resource mask, and using a user-friendly rule name.

### url-list (group-policy webvpn)

To apply a list of WebVPN servers and URLs to a particular user or group policy, use the **url-list** command in group-policy webvpn configuration mode or in username webvpn configuration mode. To remove a list, including a null value that is created by using the **url-list none command,** use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a URL list, use the **url-list none** command. Using the command a second time overrides the previous setting.

**url-list** {**value** *name* | **none**} [*index*]

### url-list (group-policy webvpn) Parameters

| Parameter | Description |
|---|---|
| *index* | Indicates the display priority on the home page. |
| **none** | Sets a null value for URL lists. Prevents inheriting a list from a default or specified group policy. |
| **value** *name* | Specifies the name of a previously configured list of URLs. To configure such a list, use the **url-list** command in global configuration mode. |

## hidden-shares

To control the visibility of hidden shares for CIFS files, use the **hidden-shares** command in group-policy webvpn configuration mode. To remove the hidden shares option from the configuration, use the **no** form of this command.

**hidden-shares {none | visible}**

### hidden-shares Parameters

| Parameter | Description |
|---|---|
| **none** | Specifies that no configured hidden shares are visible or accessible to users |
| **visible** | Reveals hidden shares, making them accessible to users |

## file-entry

To enable or disable the ability of a user to enter file server names to access, use the **file-entry** command in group-policy webvpn configuration mode.

**file-entry {enable | disable}**

### file-entry Parameters

| Parameter | Description |
|---|---|
| **enable \| disable** | Enables or disables the ability to enter file server names to access |

## file-browsing

To enable or disable CIFS or FTP file browsing for file servers or shares, use the **file-browsing** command in group-policy webvpn configuration mode.

**file-browsing {enable | disable}**

### file-browsing Parameters

| Parameter | Description |
|---|---|
| **enable \| disable** | Enables or disables the ability to browse for file servers or shares |

## url-entry

To enable or disable the ability to enter any HTTP or HTTPS URL on the portal page, use the **url-entry** command in group-policy webvpn configuration mode.

**url-entry {enable | disable}**

### url-entry Parameters

| Parameter | Description |
|---|---|
| `enable \| disable` | Enables or disables the ability to browse for file servers or shares |

## 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 group-policy 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 |
|---|---|
| `none` | Indicates that there is no webtype access list. Sets a null value, which disallows an access list. Prevents inheriting an access list from another group policy. |
| `value ACLname` | Provides the name of the previously configured access list. |

## access-list webtype

To add an access list 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* | **any**] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

### access-list webtype Parameters

| Parameter | Description |
|---|---|
| `any` | (Optional) Specifies all URLs. |
| `deny` | Denies access if the conditions are matched. |
| `id` | Name or number of an access list. |
| `interval secs` | (Optional) Specifies the time interval at which to generate system log message 106100. Valid values are from 1 to 600 sec. |
| `log [[disable \| default] \| level]` | (Optional) Specifies that system log message 106100 is generated for the ACE. See the **log** command for information. |
| `oper` | Compares *ip_address* ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). |
| `permit` | Permits access if the conditions are matched. |
| `time_range name` | (Optional) Specifies a keyword for attaching the time-range option to this access list element. |
| `url` | Specifies the use of a URL for filtering. |
| `url_string` | (Optional) Specifies the URL that is to be filtered. |

## rewrite

To disable content rewriting of a particular application or type of traffic over a WebVPN connection, use the **rewrite** command in webvpn mode. To eliminate a rewrite rule, use the **no** form of this command with the rule number, which uniquely identifies the rule. To eliminate all rewriting rules, use the **no** form of the command without the rule number.

By default, the adaptive security appliance rewrites, or transforms, all WebVPN traffic.

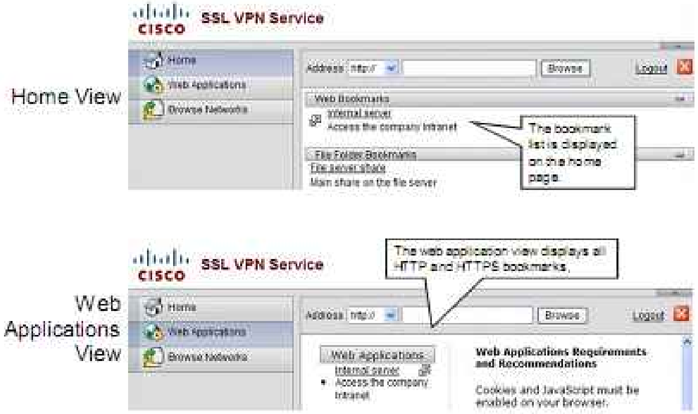
**rewrite order** *integer* {**enable** | **disable**} **resource-mask** *string* [**name** *resource name*]

### rewrite Parameters

| Parameter | Description |
|---|---|
| **disable** | Defines this rewrite rule as a rule that disables content rewriting for the specified traffic. When you disable content rewriting, traffic does not go through the security appliance. |
| **enable** | Defines this rewrite rule as a rule that enables content rewriting for the specified traffic. |
| *integer* | Sets the order of the rule among all the configured rules. The range is 1–65,534. |
| **name** | (Optional) Identifies the name of the application or resource to which the rule applies. |
| **order** | Defines the order in which the adaptive security appliance applies the rule. |
| **resource-mask** | Identifies the application or resource for the rule. |
| *resource name* | (Optional) Specifies the application or resource to which the rule applies. Maximum, 128 bytes. |
| **string** | Specifies the name of the application or resource to match that can contain a regular expression. You can use the following wildcards:<br>■ *****—Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string.<br>■ **?**—Matches any single character.<br>■ **[!seq]**—Matches any character not in sequence.<br>■ **[seq]**—Matches any character in sequence.<br>Maximum, 300 bytes. |

## Verifying Basic Portal Features and Access Control

### User Portal Verification



Access the company intranet

Main share on the file server

The bookmark list is displayed on the home page.

The web application view displays all HTTP and HTTPS bookmarks.

- Access the company intranet

**Web Applications Requirements and Recommendations**

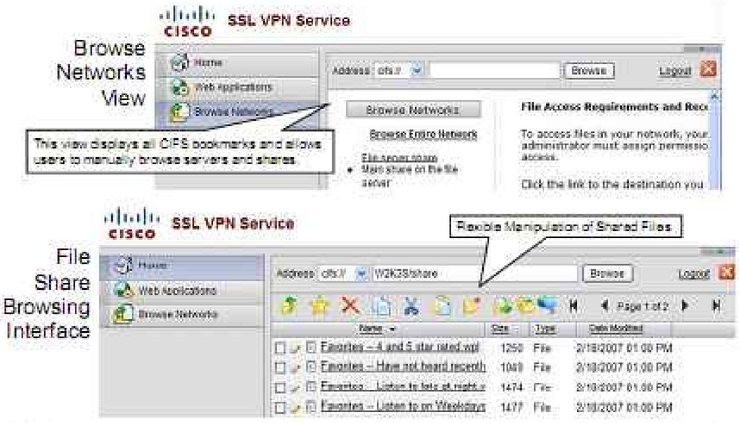
Cookies and JavaScript must be enabled on your browser.

To verify portal feature configuration and access control, you can start a clientless SSL VPN session and log in to the portal.

The top portion of the figure shows the default, Home view of the portal, displaying the two preconfigured web application and CIFS bookmarks. The URL entry function is also enabled. The bottom portion of the figure shows the Web Applications view of the portal, displaying only the preconfigured HTTP and HTTPS bookmarks.

## Verifying Basic Portal Features and Access Control

### User Portal Verification (Cont.)



This view displays all CIFS bookmarks and allows users to manually browse servers and shares.

To access files in your network, your administrator must assign permissio access.

Click the link to the destination you

Flexible Manipulation of Shared Files

| Name | Size | Type | Date Modified |
|---|---|---|---|
| Favorites – 4 and 5 star rated.wpl | 1250 | File | 2/10/2007 01:00 PM |
| Favorites – Have not heard recently | 1049 | File | 2/10/2007 01:00 PM |
| Favorites – Listen to late at night.v | 1474 | File | 2/10/2007 01:00 PM |
| Favorites – Listen to on Weekdays | 1477 | File | 2/10/2007 01:00 PM |

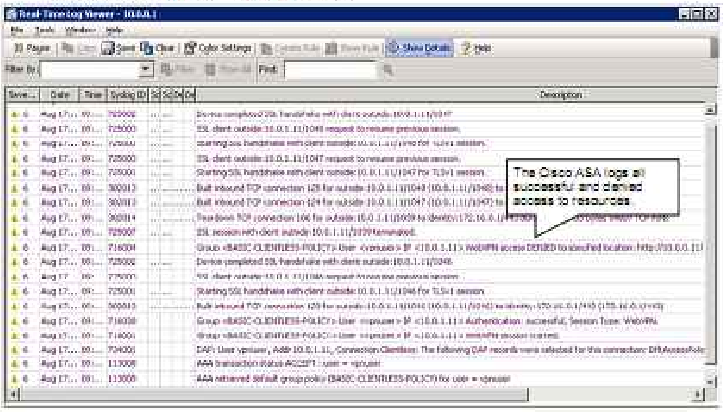
The Browse Networks view shows the preconfigured CIFS bookmark, as well as allowing CIFS URL entry and the browsing functionality through the Browse Entire Network link.

If you access a share by clicking its CIFS bookmark, entering a CIFS path in the CIFS URL entry field, or navigating to a share through the network share browser, the Cisco ASA adaptive security appliance will open a file share interface as seen on the right side of the SSL VPN window in the lower portion of the figure. This interface allows users to flexibly manipulate files, offering the following menu buttons:

- Up One Level
- Favorites
- Delete File
- Copy File
- Cut File
- Paste File
- New Folder
- Upload File
- Network
- Web Folder

# Verifying Basic Portal Features and Access Control

## Access Control Verification



Real-Time Log Viewer - 10.0.0.1

File Tools Window Help
Pause Copy Save Clear Color Settings Create Rule Show Rule Show Details Help
Filter By: Filter Show All Find:

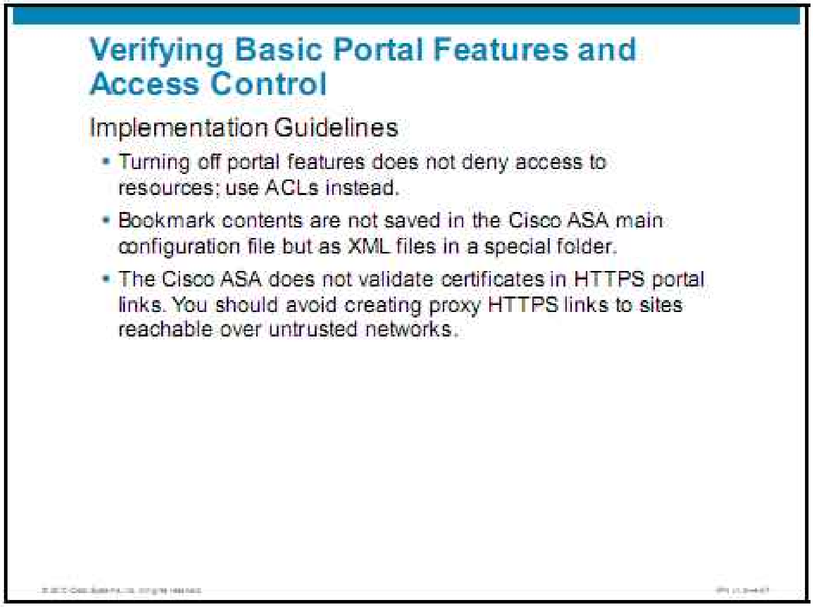
```
Seve... Date     Time   Syslog ID Sc Sc De De Description
6       Aug 17... 09:... 725002                Device completed SSL handshake with client outside:10.0.1.11/1047
6       Aug 17... 09:... 725003                SSL client outside:10.0.1.11/1048 request to resume previous session.
6       Aug 17... 09:... 725001                Starting SSL handshake with client outside:10.0.1.11/1048 for TLSv1 session.
6       Aug 17... 09:... 725003                SSL client outside:10.0.1.11/1047 request to resume previous session.
6       Aug 17... 09:... 725001                Starting SSL handshake with client outside:10.0.1.11/1047 for TLSv1 session.
6       Aug 17... 09:... 302013                Built inbound TCP connection 125 for outside:10.0.1.11/1048 (10.0.1.11/1048) to
6       Aug 17... 09:... 302013                Built inbound TCP connection 124 for outside:10.0.1.11/1047 (10.0.1.11/1047) to
6       Aug 17... 09:... 302014                Teardown TCP connection 106 for outside:10.0.1.11/1039 to identity:172.16.0.1/443 [illegible] TCP FINs
6       Aug 17... 09:... 725007                SSL session with client outside:10.0.1.11/1039 terminated.
6       Aug 17... 09:... 716004                Group <BASIC-CLIENTLESS-POLICY> User <vpnuser> IP <10.0.1.11> WebVPN access DENIED to specified location: http://10.0.0.11/
6       Aug 17... 09:... 725002                Device completed SSL handshake with client outside:10.0.1.11/1046.
6       Aug 17... 09:... 725003                SSL client outside:10.0.1.11/1046 request to resume previous session.
6       Aug 17... 09:... 725001                Starting SSL handshake with client outside:10.0.1.11/1046 for TLSv1 session.
6       Aug 17... 09:... 302013                Built inbound TCP connection 120 for outside:10.0.1.11/1046 (10.0.1.11/1046) to identity:172.16.0.1/443 (172.16.0.1/443)
6       Aug 17... 09:... 716038                Group <BASIC-CLIENTLESS-POLICY> User <vpnuser> IP <10.0.1.11> Authentication: successful, Session Type: WebVPN.
6       Aug 17... 09:... 716001                Group <BASIC-CLIENTLESS-POLICY> User <vpnuser> IP <10.0.1.11> WebVPN session started.
6       Aug 17... 09:... 734001                DAP: User vpnuser, Addr 10.0.1.11, Connection Clientless: The following DAP records were selected for this connection: DfltAccessPolic
6       Aug 17... 09:... 113008                AAA transaction status ACCEPT : user = vpnuser
6       Aug 17... 09:... 113009                AAA retrieved default group policy (BASIC-CLIENTLESS-POLICY) for user = vpnuser
```

The Cisco ASA logs all successful and denied access to resources.

Monitoring > Logging > Real-Time Log Viewer

VPN v1.0—4-44

You can verify the correctness of your webtype ACLs by attempting to access URLs that should be allowed or denied. The Cisco ASA adaptive security appliance will, by default, log all resource accesses through the SSL VPN portal. In this example, the Cisco ASDM Real-Time Low Viewer shows accounting records that show a successful (GRANTED) and unsuccessful (DENIED) attempt to access the webtype-ACL-protected internal network.



## Verifying Basic Portal Features and Access Control

Implementation Guidelines

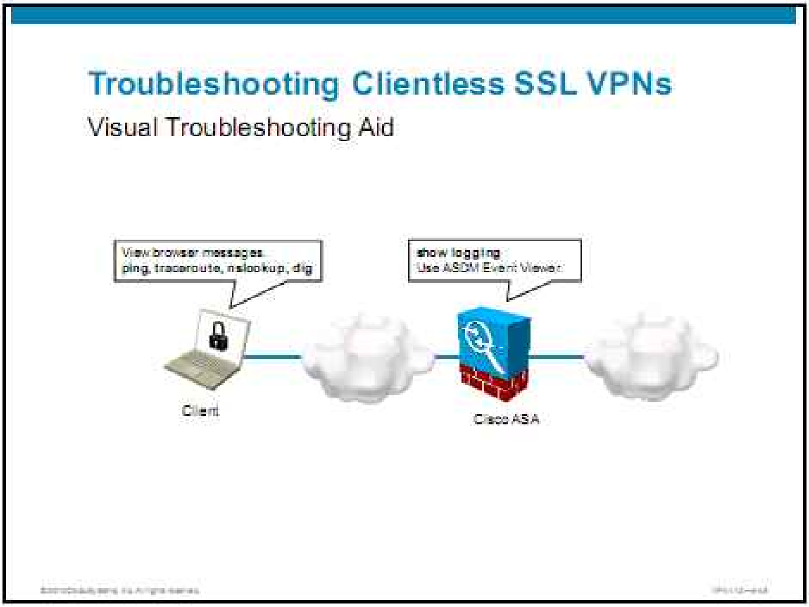
- Turning off portal features does not deny access to resources; use ACLs instead.
- Bookmark contents are not saved in the Cisco ASA main configuration file but as XML files in a special folder.
- The Cisco ASA does not validate certificates in HTTPS portal links. You should avoid creating proxy HTTPS links to sites reachable over untrusted networks.

When you implement basic Cisco ASA adaptive security appliance clientless portal functions and access control, consider the following implementation guidelines:

- Disabling portal user interface functions does not prevent access to internal resources if the user has bookmarked a link, or knows how to construct a rewritten URL. Webtype ACLs are the only reliable method to restrict access to internal resources.
- Bookmark list contents are not saved in the Cisco ASA adaptive security appliance main configuration file, but inside separate XML files. If you need to back up the Cisco ASA adaptive security appliance configuration or migrate the configuration to a different appliance, you will need to migrate these XML files as well.
- If you access HTTPS resources over the SSL VPN portal, the Cisco ASA adaptive security appliance SSL VPN proxy does not validate the certificate of the HTTPS server against a root certificate. Although this lack of validation is usually not an issue if the connection between the Cisco ASA security appliance and the target server is over a trusted network, accessing HTTPS servers over untrusted networks can expose the HTTPS session to significant risk. The risk is significant because man-in-the-middle attacks cannot be detected by the user. Therefore, avoid allowing clientless SSL VPN users to access HTTPS sites over the SSL VPN portal, if these sites are reachable over untrusted transport networks.

# Troubleshooting Clientless SSL VPNs

This topic describes how to troubleshoot VPN session establishment between a browser client and a Cisco ASA adaptive security appliance clientless SSL VPN gateway.



## Troubleshooting Clientless SSL VPNs

Visual Troubleshooting Aid

View browser messages
ping, traceroute, nslookup, dig

show logging
Use ASDM Event Viewer

When troubleshooting clientless SSL VPN session establishment, you should perform troubleshooting tasks on both the client and the Cisco ASA adaptive security appliance, if possible. This figure shows some most useful troubleshooting commands and actions that you can use on involved components.

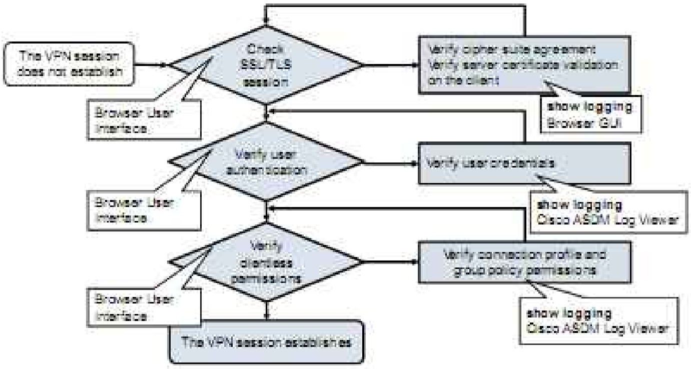
On the client, you can use operating system utilities to determine the reason for connectivity or name resolution issues. Here are some examples of these utilities:

- The ping utility to determine Layer 3 reachability of the Cisco ASA adaptive security appliance from the client
- The traceroute utility to troubleshoot Layer 3 path problems between the client and the Cisco ASA adaptive security appliance
- The nslookup and dig utilities to troubleshoot name resolution, if the browser cannot resolve the URL for the SSL VPN portal

Note that the Cisco ASA adaptive 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.

## Troubleshooting Clientless SSL VPNs

### Troubleshooting Flow


The VPN session does not establish
Check SSL/TLS session
Browser User Interface
Verify cipher suite agreement
Verify server certificate validation on the client
show logging
Browser GUI
Verify user authentication
Browser User Interface
Verify user credentials
show logging
Cisco ASDM Log Viewer
Verify clientless permissions
Browser User Interface
Verify connection profile and group policy permissions
show logging
Cisco ASDM Log Viewer
The VPN session establishes

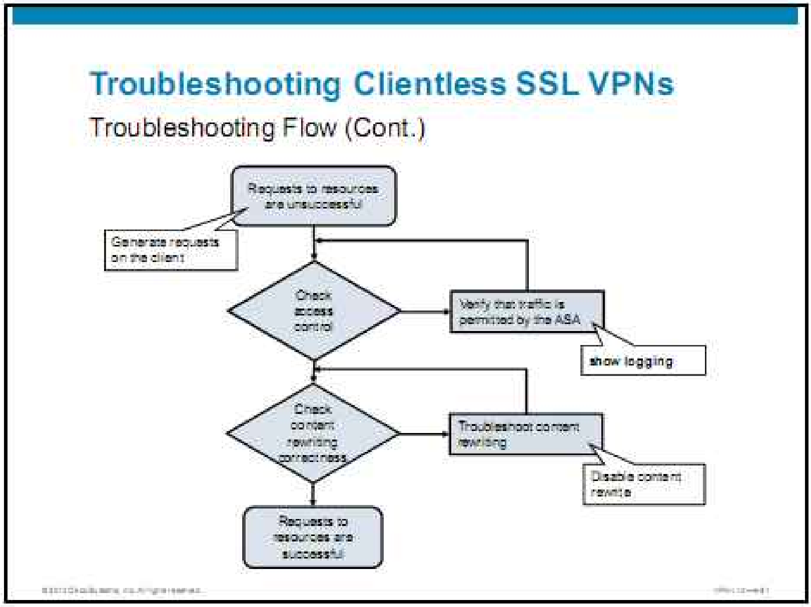
If you are encountering clientless session establishment issues, you may follow these steps to troubleshoot the issue:

**Step 1** First, check that the SSL/TLS session initially establishes, and that there are no negotiation problems that are related to the use of incompatible protocol versions or cipher suites. You can observe these issues in the browser GUI, but you will obtain more detailed and specific information by examining Cisco ASA adaptive security appliance syslog messages.

**Step 2** If the SSL/TLS negotiation completes with no errors, check if user authentication works and the user is supplying the correct credentials. The Cisco ASA adaptive security appliance will clearly indicate these issues in its syslog messages.

**Step 3** Next, check whether the connection profile and the associated group policy allow clientless SSL VPN connections. The Cisco ASA adaptive security appliance will clearly indicate these issues in its syslog messages.

If these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.



## Troubleshooting Clientless SSL VPNs

Troubleshooting Flow (Cont.)

Requests to resources are unsuccessful

Generate requests on the client

Check access control

Verify that traffic is permitted by the ASA

show logging

Check content rewriting correctness

Troubleshoot content rewriting

Disable content rewrite

Requests to resources are successful

If you your SSL VPN session establishes, but there is no connectivity over the SSL VPN portal, you may follow these steps to troubleshoot the issue:

**Step 1** Verify that the Cisco ASA adaptive security appliance is not denying traffic from the SSL VPN tunnel. Examine the Cisco ASA adaptive security appliance syslog to see messages about permitted or denied packets.

**Step 2** Next, if you are using direct access through content rewriting, check that your content rewriting rules are not too general, which would force access to internal resources outside the SSL VPN session. You can observe this in the browser, which will attempt to contact internal hosts directly, instead of over the SSL VPN session.

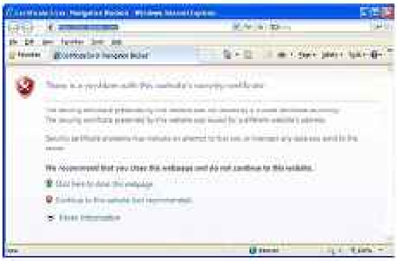
**Step 3** Finally, you can verify the HTML content that is returned to the browser by the SSL VPN portal.

If these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.

## Troubleshooting Clientless SSL VPNs

### Client-Side Issues: Certificates

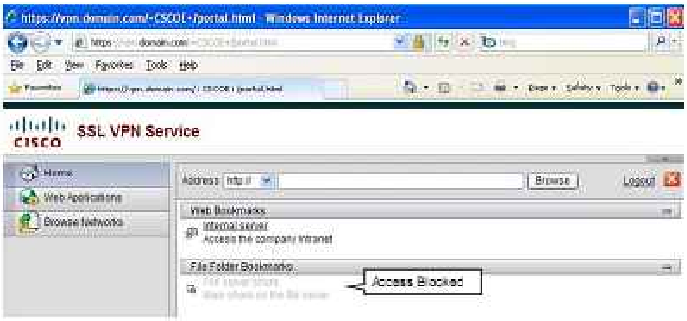
- A certificate warning can appear because of:
  - Unverifiable Cisco ASA identity certificate
  - A name mismatch between certificate CN and VPN URL in the browser
  - An expired Cisco ASA identity certificate
- You should never see this issue in production use



As with Cisco AnyConnect full tunneling VPN, the most common client issue that you may encounter in a clientless SSL VPN is a certificate warning at VPN session establishment. You should never see these issues appearing during production use of the network. Refer to the "Deploying a Basic Cisco AnyConnect Full Tunnel SSL VPN Solution" lesson in this course to obtain guidelines for resolving these issues.

## Troubleshooting Clientless SSL VPNs

### Gateway-Side Issues: Access Control

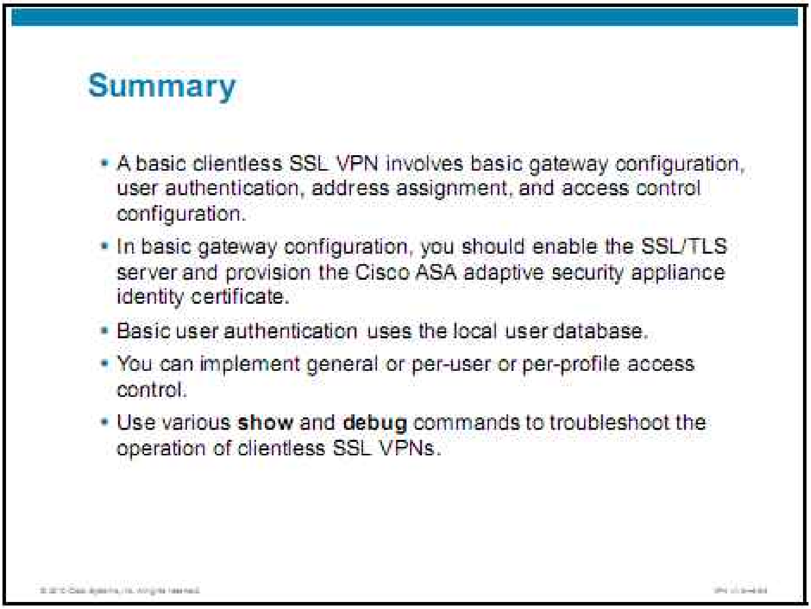


Access Blocked

If you have misconfigured your webtype ACLs to deny traffic that should not be denied, you can observe denied access in the Cisco ASA adaptive security appliance logging output. Another, even simpler method of ACL verification is to observe the predefined bookmarks in the SSL VPN portal. If you have misconfigured your ACLs, the bookmarks that are not reachable because access to these resources is not permitted are dimmed in the portal.

# Summary

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



## Summary

- A basic clientless SSL VPN involves basic gateway configuration, user authentication, address assignment, and access control configuration.
- In basic gateway configuration, you should enable the SSL/TLS server and provision the Cisco ASA adaptive security appliance identity certificate.
- Basic user authentication uses the local user database.
- You can implement general or per-user or per-profile access control.
- Use various **show** and **debug** commands to troubleshoot the operation of clientless SSL VPNs.

# Lesson 2

# Deploying Advanced Application Access for Clientless SSL VPN

## Overview

Many enterprise applications are not web-based, and use other standard or proprietary protocols to communicate over IP networks. Clientless Secure Sockets Layer (SSL) virtual private network (VPN) gateways must therefore provide some alternative possibilities for users to access these application resources. This lesson discusses application plug-ins, Cisco smart tunnels, port forwarding, and the Secure Sockets Layer and Transport Layer Security (SSL/TLS) email proxy features of the Cisco ASA adaptive security appliance SSL VPN gateway, which provide clientless access to a wide range of thin- and thick-client applications. In the lesson, you will learn how to configure, verify, and troubleshoot these access features.

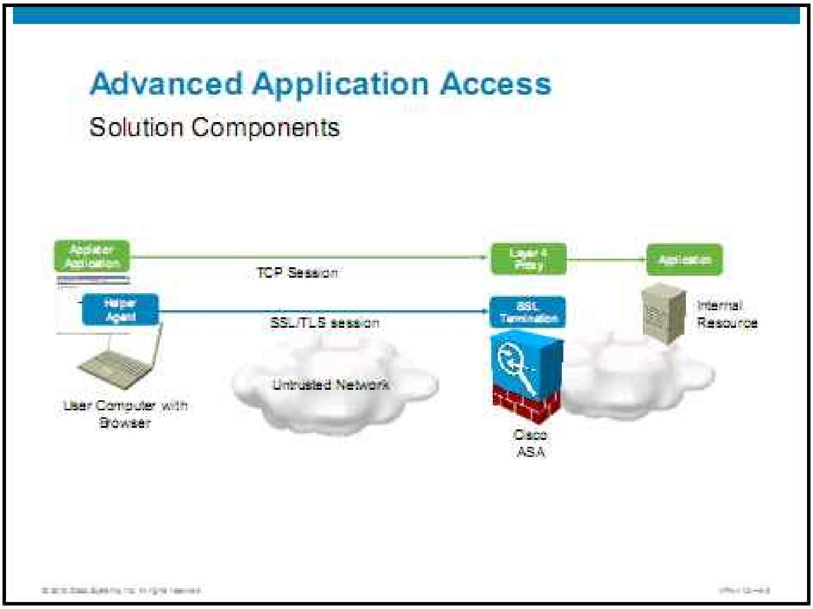
### Objectives

Upon completing this lesson, you will be able to deploy and manage advanced clientless VPN application access features of a clientless Cisco SSL VPN. This ability includes being able to meet these objectives:

- Plan the deployment of clientless SSL VPN application access features
- Configure application plug-ins
- Configure and verify smart tunnels in clientless SSL VPN
- Configure and verify port forwarding in clientless SSL VPN
- Troubleshoot advanced application access in clientless SSL VPN

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic describes how to plan the deployment of clientless SSL VPN application access features.

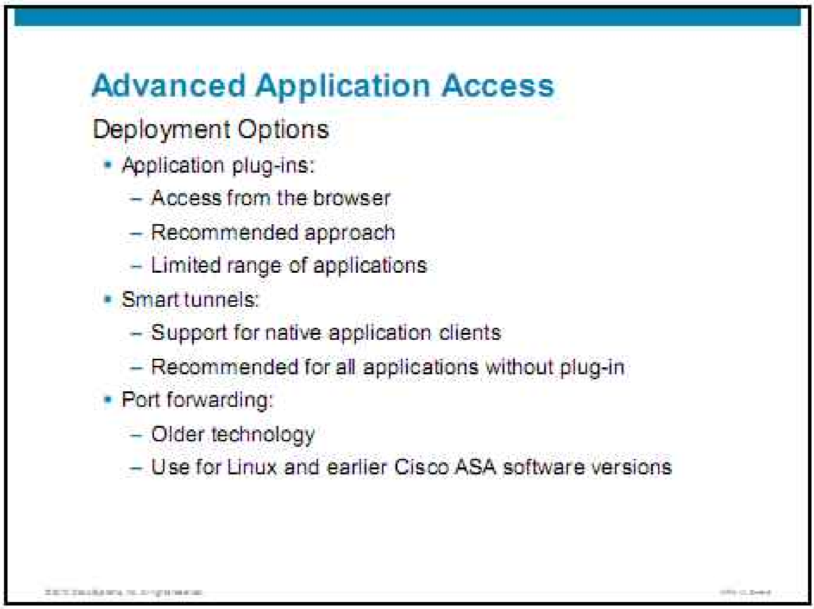


## Advanced Application Access

Solution Components

The SSL VPN rewriting proxy in the Cisco ASA adaptive security appliance provides clientless, transparent access to web and Common Internet File System (CIFS) resources behind the Cisco ASA adaptive security appliance to clients only using a web browser. To provide access to other enterprise applications, including terminal access, database clients, or instant messaging applications, the Cisco ASA adaptive security appliance provides several methods of relaying data over the SSL VPN gateway without the requirement for an SSL VPN client installation.

To enable such advanced application access methods, the Cisco ASA adaptive security appliance loads some additional software in the web-browsing session of the client. This software acts as a lightweight client or a helper relay agent that enables additional communications over an SSL VPN session. The Cisco ASA adaptive security appliance does not require any other components to enable advanced application access.



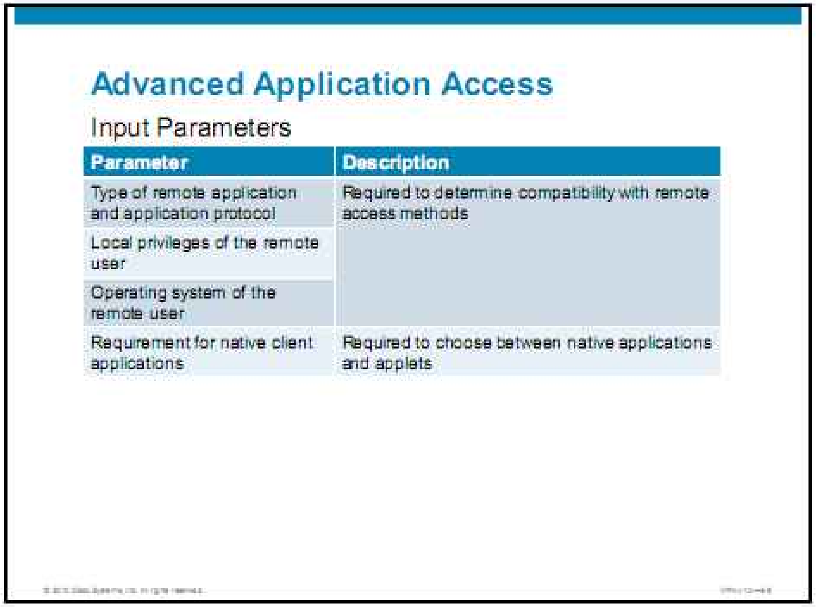
## Advanced Application Access

Deployment Options

- Application plug-ins:
  - Access from the browser
  - Recommended approach
  - Limited range of applications
- Smart tunnels:
  - Support for native application clients
  - Recommended for all applications without plug-in
- Port forwarding:
  - Older technology
  - Use for Linux and earlier Cisco ASA software versions

You can choose several options when deploying advanced application access:

- Application plug-ins provide users with thin application client access to enterprise resources. This is the recommended approach but it supports only a limited set of applications.
- Cisco Smart Tunnels provide users with native application client access to enterprise resources. This approach is the recommended approach for all applications that do not have a plug-in.
- Port forwarding provides users with native application client access to enterprise resources. This method should only be used if smart tunnels cannot be deployed, such as on Linux workstations or when running older Cisco ASA adaptive security appliance software versions.



## Advanced Application Access

Input Parameters

| Parameter | Description |
|---|---|
| Type of remote application and application protocol | Required to determine compatibility with remote access methods |
| Local privileges of the remote user | |
| Operating system of the remote user | |
| Requirement for native client applications | Required to choose between native applications and applets |

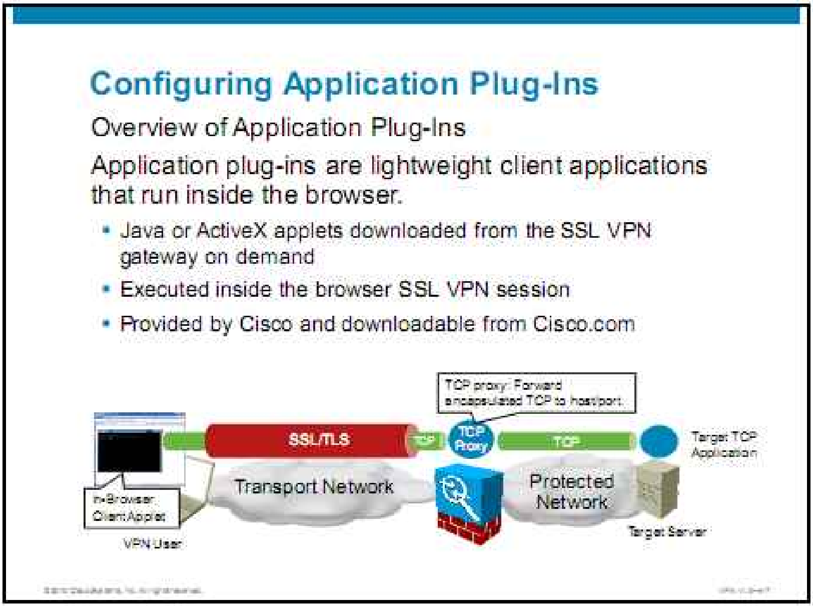
Before you deploy advanced application access, you will need to gather some input parameters about remote systems that are being used by the remote user. Gather the following information:

- The type of applications and application protocols that are used by remote users, that you will need to support over a clientless SSL VPN session.
- The local privileges of the remote user, who may use a limited account without administrative rights on the remote system.
- The operating system that is used by remote users.

  These three pieces of information will allow you to determine the application and operating system compatibility with advanced access methods. They will allow you to choose the most optimal method for a particular environment.
- The requirement for the use of native applications, versus thin applications with reduced functionality, which can be provisioned by the SSL VPN gateway. Some users may require advanced application features (such as a specific terminal emulation) that thin application clients do not provide.

# Configuring Application Plug-Ins

This topic describes how to configure application plug-ins on the Cisco ASA adaptive security appliance SSL VPN gateway.



## Configuring Application Plug-Ins

Overview of Application Plug-Ins

Application plug-ins are lightweight client applications that run inside the browser.

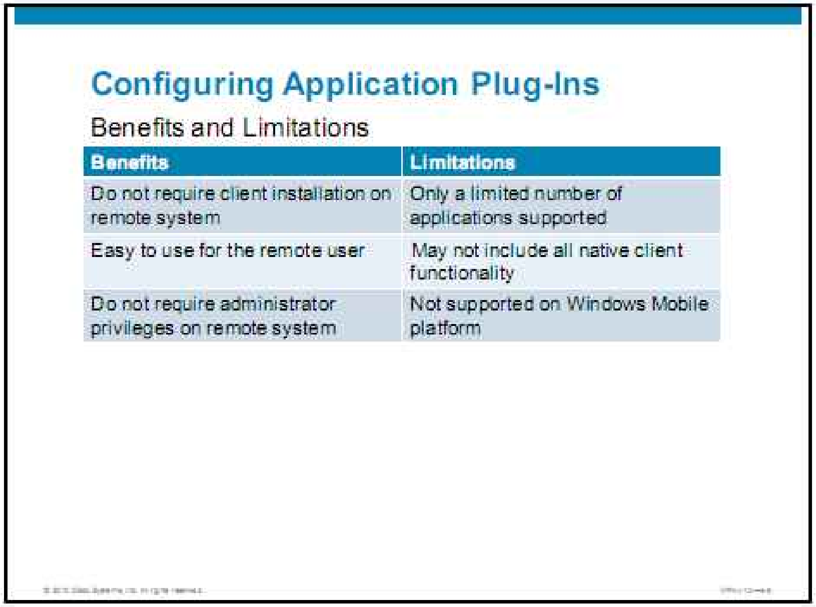
- Java or ActiveX applets downloaded from the SSL VPN gateway on demand
- Executed inside the browser SSL VPN session
- Provided by Cisco and downloadable from Cisco.com

Application plug-ins are light-client applications that provide basic application functionality inside the browser of a user. These plug-ins are downloaded on demand from the SSL VPN gateway, and all their communications with internal protected resources is transparently encapsulated within the SSL VPN session. The user does not have to use any local applications, but instead uses the thin application plug-ins only.

This figure illustrates plug-in-based application access:

1. A user connects and authenticates to the SSL VPN portal and then runs an application plug-in that allows access to a server that is running on the internal network.
2. The application plug-in runs inside the browser, and reuses the SSL session of the browser with the SSL VPN gateway to forward a TCP connection inside it.
3. The SSL VPN gateway extracts the TCP session from the SSL VPN session, establishes a TCP connection with the destination server, and acts as a data relay between the two TCP sessions.

The application plug-ins are distributed by Cisco through the Cisco ASA adaptive security appliance (remote access plug-ins) software download page, and need to be imported into the appliance. Each plug-in contains multiple files that are packed into a JAR (Java Archive) file.



## Configuring Application Plug-Ins

Benefits and Limitations

| Benefits | Limitations |
|---|---|
| Do not require client installation on remote system | Only a limited number of applications supported |
| Easy to use for the remote user | May not include all native client functionality |
| Do not require administrator privileges on remote system | Not supported on Windows Mobile platform |

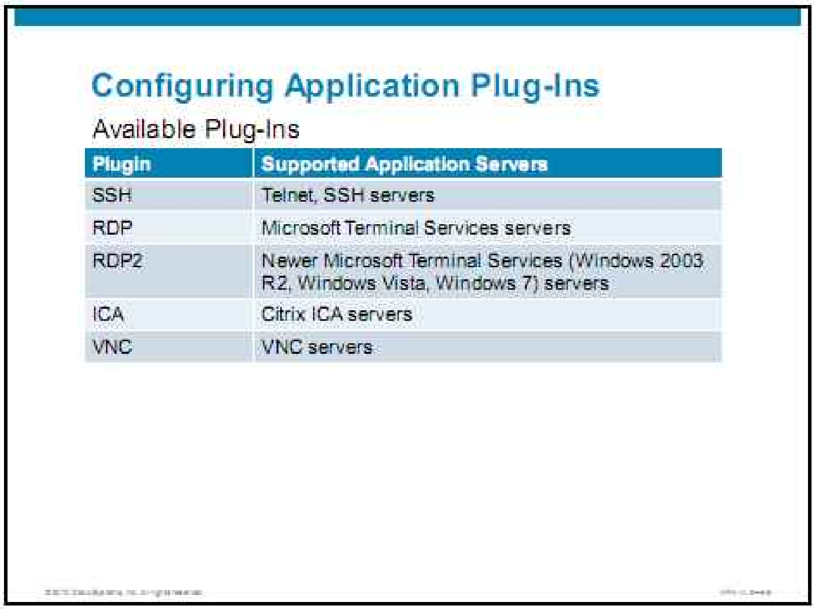
The benefits of application plug-ins are as follows:

- They do not require any installation on the remote system, because they run as Java or ActiveX applets inside the browser.
- They are easy to use for the remote user, because they start virtually automatically and are preconfigured for use.
- They do not require administrator privileges on the remote system. (Microsoft ActiveX applets may require additional privileges, but a Java alternative can be used instead.)

The limitations of application plug-ins are as follows:

- There is only a limited number of plug-ins available, mostly to support interactive terminal access.
- The plug-ins do not contain all the functionality that their thick-client equivalents include, and may not support some features that are required by your users.
- Application plug-ins are not supported on the Windows Mobile platform, and generally not supported on platforms that do not support Java.

**Note** Per the GNU General Public License (GPL), Cisco redistributes the plug-ins without having made any changes to them. Per the GNU GPL, Cisco cannot directly enhance these plug-ins. Cisco does not provide direct support for or recommend any particular plug-ins that are not redistributed by Cisco.



## Configuring Application Plug-Ins

Available Plug-Ins

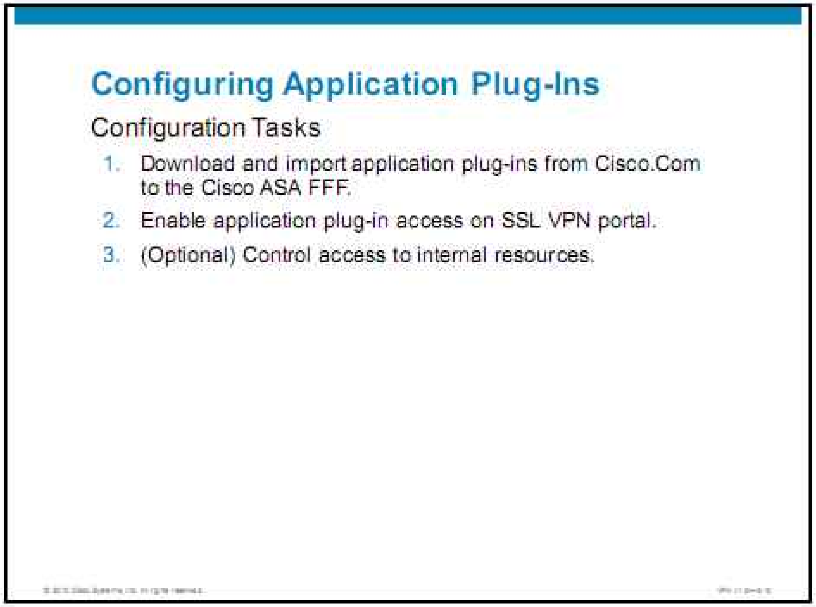
| Plugin | Supported Application Servers |
|---|---|
| SSH | Telnet, SSH servers |
| RDP | Microsoft Terminal Services servers |
| RDP2 | Newer Microsoft Terminal Services (Windows 2003 R2, Windows Vista, Windows 7) servers |
| ICA | Citrix ICA servers |
| VNC | VNC servers |

Cisco provides the following application plug-ins for download on Cisco.com:

- The SSH plug-in provides a standard terminal emulator with support for the Telnet and Secure Shell (SSH) (version 1 and 2) protocols. You can control the SSH version by providing command-line parameters to the application plug-in in its URL.
- The RDP plug-in provides a Microsoft Remote Desktop Protocol (RDP) client to connect to older versions of Microsoft Terminal Services servers.
- The RDP2 plug-in provides a Microsoft Remote Desktop Protocol (RDP) client to connect to newer versions of Microsoft Terminal Services (Windows 2003 Server R2, Windows Vista, and Windows 7) servers. The ActiveX version of the plug-in also supports advanced functionality, such as sharing of remote drives or printers on the terminal server. You can control this functionality by providing command-line parameters to the application plug-in in its URL.

**Note** You can import RDP and RDP2 plug-ins to make both of them available to clientless users.

- The ICA plug-in provides an Independent Computing Architecture (ICA) client to connect to Citrix WinFrame, XenApp, and XenDesktop terminal services.
- The VNC plug-in provides a Virtual Network Computing (VNC) client to connect to VNC display servers. The VNC plug-in does not support encryption over the internal network.



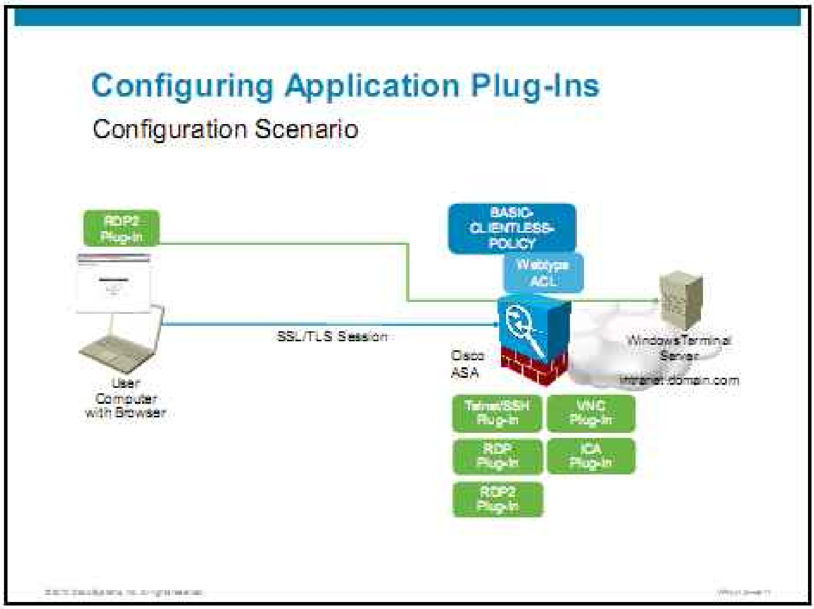
## Configuring Application Plug-Ins

Configuration Tasks

1. Download and import application plug-ins from Cisco.Com to the Cisco ASA FFF.
2. Enable application plug-in access on SSL VPN portal.
3. (Optional) Control access to internal resources.

To configure application plug-in-based access through a Cisco ASA adaptive security appliance SSL VPN gateway, you will perform the following configuration tasks:

1. Download and import application plug-in files from Cisco.com to the Cisco ASA adaptive security appliance flash file system (FFS).
2. Enable application plug-in access on the SSL VPN portal, using optional application plug-in bookmarks.
3. Optionally, deploy access control features on the Cisco ASA adaptive security appliance SSL VPN gateway to control access from application plug-ins to internal resources.



## Configuring Application Plug-Ins

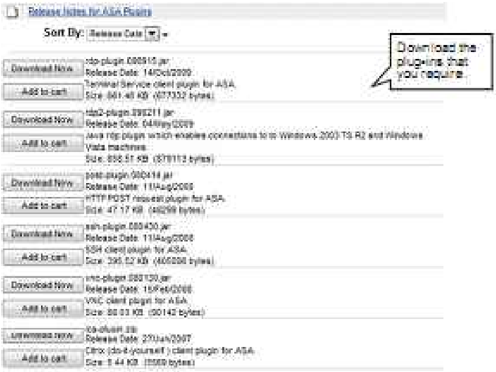
Configuration Scenario

This figure presents the configuration scenario that is used in upcoming configuration tasks. You will import all required application plug-ins on the Cisco ASA adaptive security appliance and configure an RDP2 bookmark, which the client will select after login. The client will then load the RDP2 plug-in, and access a terminal server (10.10.1.1) in the internal network. You will also configure the Cisco ASA adaptive security appliance to limit access to the protected network using a webtype access control list (ACL), which will only allow the specific RDP connection to the internal network.

The configuration scenario assumes that the Cisco ASA adaptive security appliance is already configured with a basic clientless SSL VPN gateway functionality as was discussed in the previous lesson, "Deploying a Basic clientless VPN Solution."

## Configuring Application Plug-Ins

Task 1: Download and Import Application Plug-Ins



Release Notes for ASA Plugins

Sort By: Release Date

rdp-plugin.080915.jar
Release Date: 14/Oct/2009
Terminal Service client plugin for ASA
Size: 661.46 KB (677332 bytes)

rdp2-plugin.090211.jar
Release Date: 04/May/2009
Java rdp plugin which enables connections to to Windows 2003 TS R2 and Windows Vista machines
Size: 856.51 KB (876113 bytes)

post-plugin.080418.jar
Release Date: 11/Aug/2008
HTTP POST request plugin for ASA
Size: 47.17 KB (48298 bytes)

ssh-plugin.080430.jar
Release Date: 11/Aug/2008
SSH client plugin for ASA
Size: 395.52 KB (405008 bytes)

vnc-plugin.080130.jar
Release Date: 15/Feb/2008
VNC client plugin for ASA
Size: 88.03 KB (90142 bytes)

ica-plugin.zip
Release Date: 27/Jun/2007
Citrix (do-it-yourself) client plugin for ASA
Size: 5.44 KB (5569 bytes)

Download the plug-ins that you require.

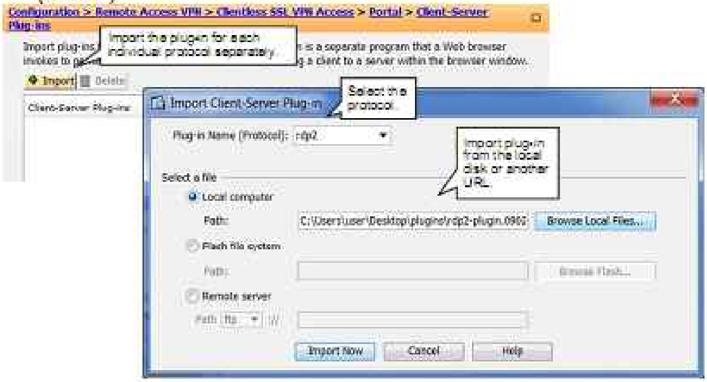
The first configuration step in the application plug-ins configuration sequence is to download the needed application plug-ins from Cisco.com, and install them on the Cisco ASA adaptive security appliance. You can find the application plug-ins in the Cisco.com Cisco ASA adaptive security appliance software download section, or download them as part of the Cisco ASA adaptive security appliance client bundle, which includes the Cisco AnyConnect client, Cisco Secure Desktop, and all application plug-ins.

The Cisco ASA adaptive security appliance client bundle can be found at http://www.cisco.com/cgi-bin/tablebuild.pl/asa-manufacturing.

You can either unpack the client bundle yourself, and install the relevant files manually, or have the Cisco ASA adaptive security appliance automatically install them. The Cisco ASA adaptive security appliance client bundle is a .zip file and if you transfer to the Cisco ASA adaptive security appliance flash, the appliance will automatically decompress it and install all included software upon reboot. The file that is downloaded from Cisco.com must be renamed “client_bundle.zip” for the auto install to work.

## Configuring Application Plug-Ins

Task 1: Download and Import Application Plug-Ins (Cont.)



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins

Import plug-ins ... is a seperate program that a Web browser invokes to p... a client to a server within the browser window.

Plug-in Name (Protocol): rdp2

Select a file

● Local computer

Path: C:\Users\user\Desktop\plugins\rdp2-plugin.090

○ Flash file system

○ Remote server

Path: ftp ://

Import the plugin for each individual protocol separately.
Import
Delete
Client-Server Plug-ins
Import Client-Server Plug-in
Select the protocol.
Import plug-in from the local disk or another URL.
Browse Local Files...
Browse Flash...
Import Now
Cancel
Help

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins

To manually import plug-ins into the security appliance, complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-Ins.**

**Step 2** Click the **Import** button.

**Step 3** Choose the type of plug-in that is to be imported from the Plug-in Name (Protocol) drop-down menu.

**Step 4** Click the **Browse Local Files** button to choose any plug-ins that are downloaded from Cisco.com on your local machine.

**Step 5** After the plug-in has been chosen, click **Import Now** to import the plug-in for use by the security appliance.

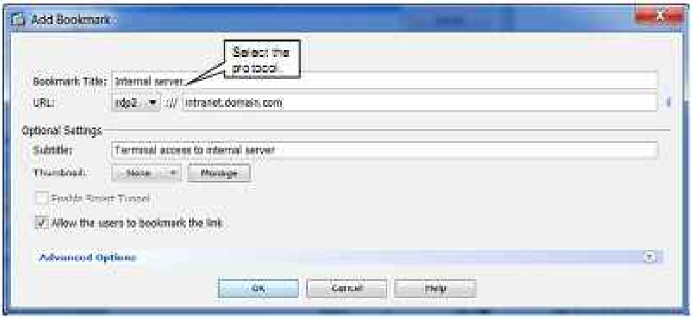
In this figure, the RDP2 plug-in is being imported to the security appliance for use with the SSL VPN. The Cisco ASA adaptive security appliance will unpack the JAR plug-ins file and write the unpacked files to the appropriate Cisco ASA adaptive security appliance file system. After you have imported all the desired plug-ins, they will be listed in the main Client-Server Plug-ins window.

To remove a plug-in that has been imported to the Cisco ASA adaptive security appliance, select the plug-in. and then click the **Delete** button.

## Configuring Application Plug-Ins

### Task 2: Enable Application Plug-In Access

- Create bookmarks with plug-in-related URL protocols.
- Enter plug-in-related URLs with free URL entry.



Add Bookmark

Bookmark Title: Internal server

URL: rdp2 :// intranet.domain.com

Optional Settings

Subtitle: Terminal access to internal server

Thumbnail: None

□ Enable Smart Tunnel

☑ Allow the users to bookmark the link

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks

After the plug-ins have been imported to the Cisco ASA adaptive security appliance, you do not need to authorize their use in group policies. If you are using SSL VPN portal bookmarks, you now have the option of choosing additional protocols—as supported by plug-ins—in the bookmark URL specification. If you allow free URL entry on the SSL VPN portal, users can now enter URLs with protocols that are supported by imported plug-ins. In this second task, you will create bookmarks that use application plug-ins and allow users to start these plug-ins from the SSL VPN portal.

To configure SSL VPN portal bookmarks to use imported plug-ins, complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks** and click **Add** to add a new bookmark list.
Configure the bookmark list name and click **Add** to create individual bookmarks for this list. The Add Bookmark window appears as shown in the figure.

**Step 2** To configure a bookmark title named "Internal server" in this example, choose the desired plug-in protocol, and then configure the target server address. In this example, the RDP2 plug-in using the RDP2 protocol is used, connecting to the intranet.domain.com internal server. An optional subtitle of "Terminal access to internal server" is also defined for this bookmark.

**Step 3** Click **OK** to add the bookmark to the security appliance configuration and then click **Apply** to send the configuration to the security appliance. Save your configuration if necessary.

After the bookmark list with the RDP2 bookmark is configured, apply the bookmark list to the desired group policy as shown in the previous lesson.

## Specifying Applet Settings

Some of the plug-ins allow you to specify additional settings in the URL, which the plug-in will interpret as a set of parameters for the current plug-in session. For example, you can specify the SSH plug-in to use a specific SSH version in the following manner:

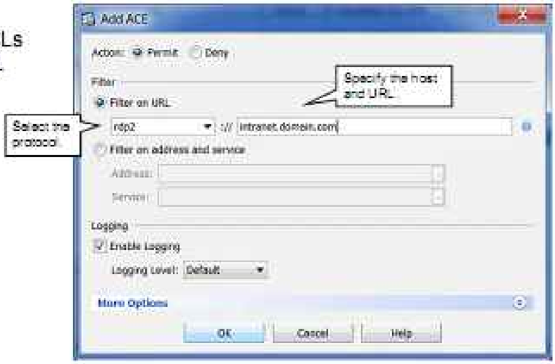
- Specifying the bookmark or free entry URL as ssh://<*target*> will default to SSH version 2 (SSHv2).
- Specifying the bookmark or free entry URL as ssh://<*target*>/?version=1 will use SSH version 1 (SSHv1).

Other plug-ins that are not discussed in this lesson support single sign-on (SSO) to internal resources. They are covered in a later lesson of this module.

### Configuring Application Plug-Ins

Task 3: Control Access to Internal Resources

Webtype ACLs can use URL syntax.



Add ACE

Action: ● Permit ○ Deny

Filter

● Filter on URL

rdp2 :// intranet.domain.com

○ Filter on address and service

Address:

Service:

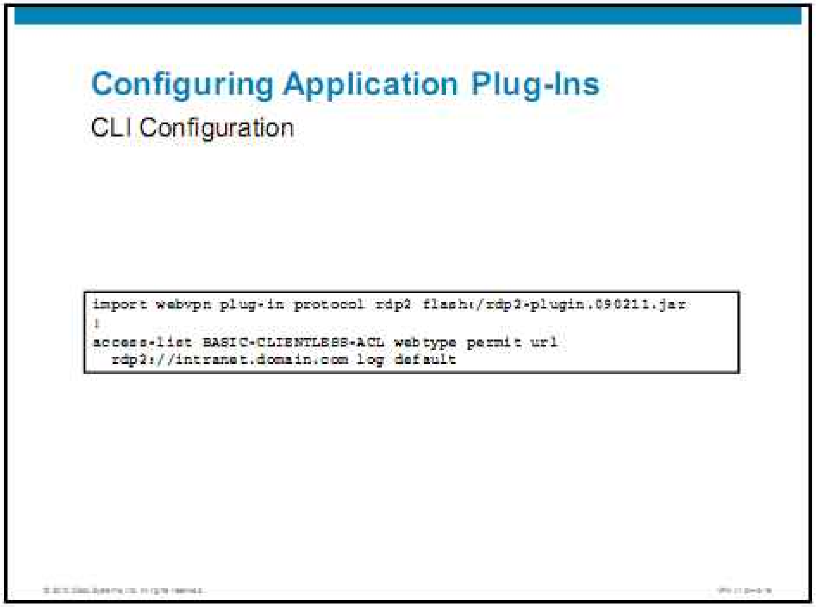
Logging

☑ Enable Logging

Logging Level: Default

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs

In the third task, you can optionally control access to internal resources by creating or modifying your webtype ACLs to permit or deny plug-in-based URLs. To control access, you should create access control entries (ACEs) in your webtype ACLs and apply the webtype ACLs to the desired group policies, as shown in the previous lesson, to allow the appropriate URLs based on the plug-ins protocol. In this example, you will add an ACE to an existing webtype ACL to allow RDP2 access to the intranet.domain.com internal server.



## Configuring Application Plug-Ins

CLI Configuration

```
import webvpn plug-in protocol rdp2 flash:/rdp2-plugin.090211.jar
!
access-list BASIC-CLIENTLESS-ACL webtype permit url
  rdp2://intranet.domain.com log default
```

This output shows the CLI commands that are required to configure application plug-in access.

In the CLI, enter the privileged mode of the Cisco ASA adaptive security appliance and use the **import webvpn plug-in protocol** command to manually import application plug-ins that are located in the flash file system or from a remote URL**.** This configuration will automatically enable all access to URLs that are managed by the plug-in protocol.

Next, optionally create or modify the webtype ACL by creating an ACE that allows access to plug-in-based resources, using the **access-list** *name* **webtype** command.

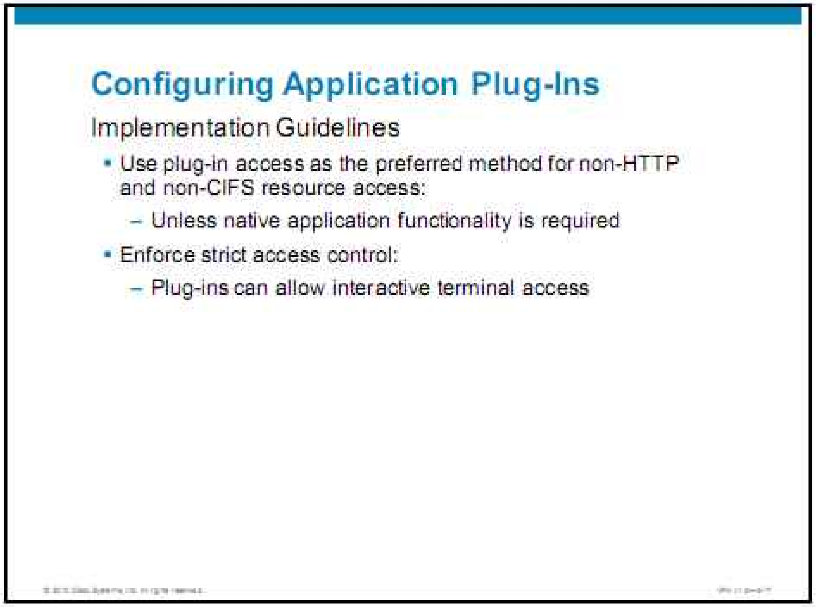
## import webvpn plug-in protocol

To install a plug-in to the adaptive security appliance, enter the **import webvpn plug-in protocol** command in privileged EXEC mode.

**import webvpn plug-in protocol** *protocol URL*

### import webvpn plug-in protocol Parameters

| Parameter | Description |
|---|---|
| *protocol* | ■ **rdp:** The Remote Desktop Protocol (RDP) plug-in lets the remote user connect to a computer running Microsoft Terminal Services. Cisco redistributes this plug-in without any changes. The website containing the original is http://properjavardp.sourceforge.net/.<br>■ **ssh, telnet:** The Secure Shell (SSH) plug-in lets the remote user establish a secure channel to a remote computer or lets the remote user use Telnet to connect to a remote computer. Cisco redistributes this plug-in without any changes. The website containing the original is http://javassh.org/.<br>**Caution** The **import webvpn plug-in protocol ssh,telnet** *URL* command installs *both* the SSH and Telnet plug-ins. Do *not* enter this command once for SSH and once for Telnet. When you type the **ssh,telnet** string, do *not* insert a space. Use the **revert webvpn plug-in protocol** command to remove any **import webvpn plug-in protocol** commands that deviate from these requirements.<br>■ **vnc:** The Virtual Network Computing (VNC) plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on. Cisco redistributes this plug-in without any changes. The website containing the original is http://www.tightvnc.com/. |
| *URL* | Remote path to the source of the plug-in. |



## Configuring Application Plug-Ins

Implementation Guidelines

- Use plug-in access as the preferred method for non-HTTP and non-CIFS resource access:
  - Unless native application functionality is required
- Enforce strict access control:
  - Plug-ins can allow interactive terminal access

When you are implementing application plug-in access in clientless SSL VPNs, consider the following guidelines:

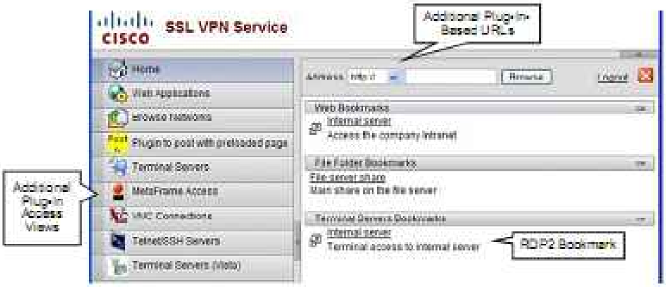
- Use application plug-ins as the preferred method of access to non-HTTP and non-CIFS resources, unless your business process requires the use of features not available in the lightweight clients inside application plug-ins.
- Most plug-ins provide interactive terminal access to resources in the protected network. Because such powerful resource access can lead to serious security incidents, limit the required access to a minimum using webtype ACLs, especially from unmanaged, and less trustworthy, remote clients.

## Verifying Application Plug-Ins

Verify Access

The SSL VPN portal will automatically change:

- Plug-in-related views
- URL entry for plug-in access



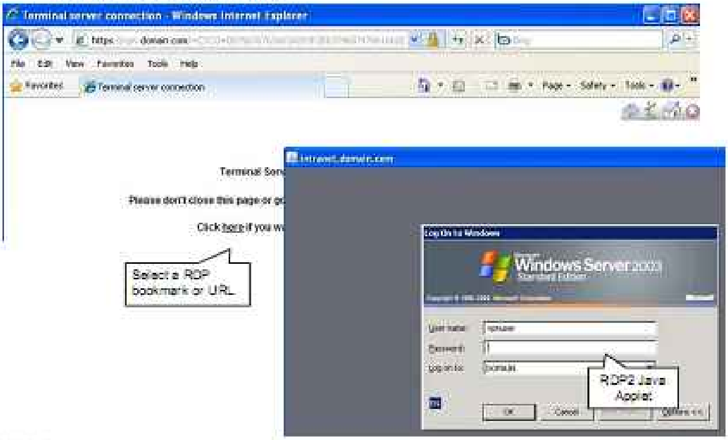
To verify the availability of application plug-ins and their proper operation, log in to the SSL VPN portal. You should see additional plug-in-related views on the left side of the SSL VPN portal home page. These views—if selected—will display all plug-in-related bookmarks on the right side of the portal page. By default, all bookmarks are listed. In this example, the newly created RDP2 bookmark is available in the right pane of the portal window.

Users can also use the URL entry control (if allowed) to select URLs for protocols that are enabled by imported plug-ins.

This example is also showing other imported plug-ins like Telnet/SSH, Citrix MetaFrame, VNC, and so on.

## Verifying Application Plug-Ins

Verify Access (Cont.)



Terminal server connection - Windows Internet Explorer

Terminal Serv

Please don't close this page or go

Click here if you w

intranet.domain.com

Log On to Windows

User name:

Password:

Log on to:

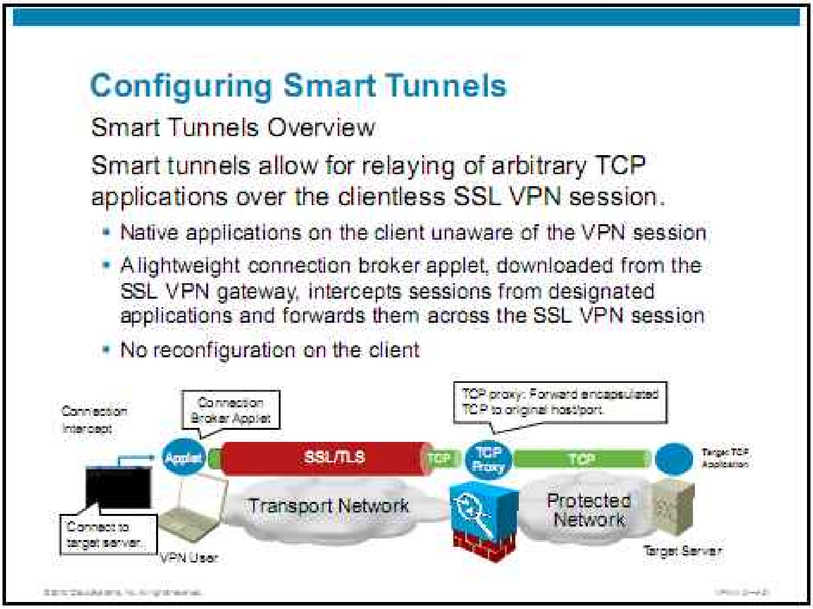
Select a RDP bookmark or URL

RDP2 Java Applet

Click the plug-in bookmark, or enter a plug-in-related URL to start an application plug-in. The portal will start a plug-in in a new window. In this example, selecting the RDP2 plug-in resulted in starting the RDP2 application plug-in, which opened a Java RDP2 client in a new window, showing the login page of an internal server.

# Configuring Smart Tunnels

This topic describes how to configure and verify smart tunnels in clientless SSL VPN.



## Configuring Smart Tunnels

Smart Tunnels Overview

Smart tunnels allow for relaying of arbitrary TCP applications over the clientless SSL VPN session.

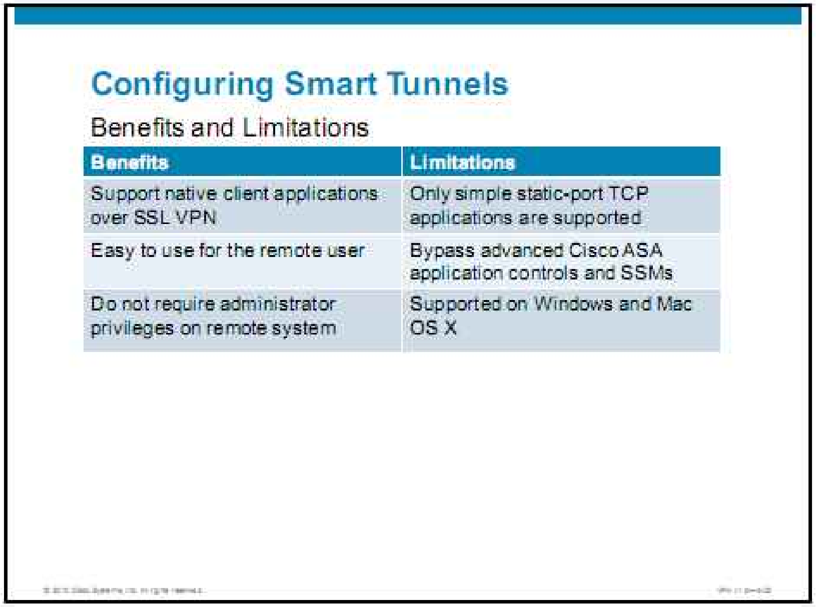
- Native applications on the client unaware of the VPN session
- A lightweight connection broker applet, downloaded from the SSL VPN gateway, intercepts sessions from designated applications and forwards them across the SSL VPN session
- No reconfiguration on the client

Smart tunnels enable users to use native client applications without the need for administrative rights or application reconfiguration. They work by downloading a smart tunnel agent (connection broker) applet to the client system. This applet intercepts all local socket calls (that is, connection requests of the application to the operating system kemel) from Window Sockets 2 (Winsock2) TCP applications, and automatically redirects them into the SSL VPN session.

This figure illustrates smart-tunnel-based application access:

1. A user connects and authenticates to the SSL VPN portal. A smart tunnel configuration is in place for that user and automatically downloads and executes the smart tunnel agent on the client system. For example, the user starts the Lotus Sametime instant messaging client.
2. The smart tunnel applet intercepts the TCP connection of the IBM Lotus Sametime client to the real server and forwards it over the existing SSL VPN session.
3. The SSL VPN gateway extracts the TCP session from the SSL VPN session, establishes a TCP connection with the real target server, and acts as a data relay between the two TCP sessions.

As long as the clientless SSL VPN session of the user is established, specific local applications can access protected resources, with the agent relaying their communications through the session of the browser.



## Configuring Smart Tunnels

Benefits and Limitations

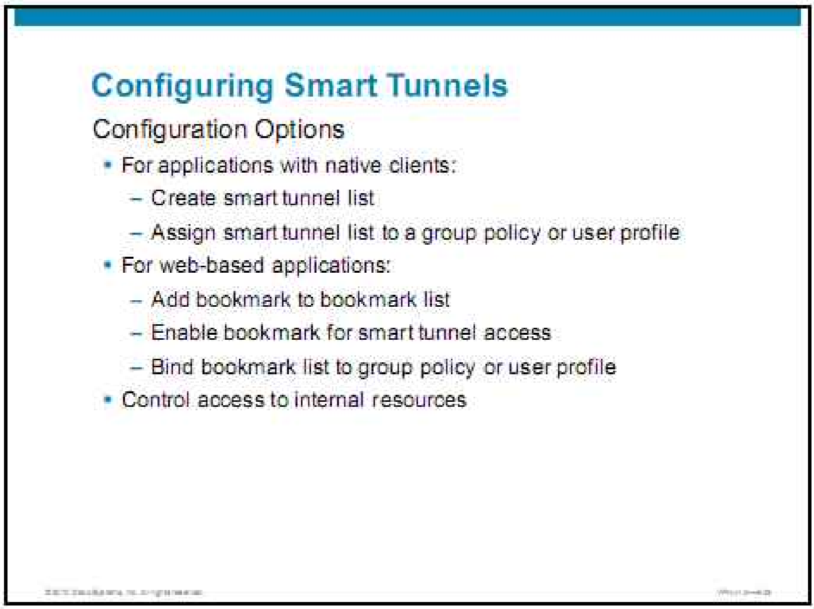
| Benefits | Limitations |
|---|---|
| Support native client applications over SSL VPN | Only simple static-port TCP applications are supported |
| Easy to use for the remote user | Bypass advanced Cisco ASA application controls and SSMs |
| Do not require administrator privileges on remote system | Supported on Windows and Mac OS X |

The benefits of smart tunnels are as follows:

- They support the use of fully featured, native applications that are already installed on the remote system of the user.
- They are easy to use for the remote user because users use their local network applications just as they do in the protected network or any other non-VPN location.
- They do not require administrator privileges on the remote system.

The limitations of smart tunnels are as follows:

- Only Winsock2, TCP-based applications are eligible for smart tunnel access.
- Smart tunnels only support simple, static-port TCP applications. Most client-server applications operate in this manner and are therefore supported by smart tunnels.
- Access to the internal network bypasses the advanced Cisco ASA adaptive security appliance application layer controls and security services modules. However, you can control the resources that are available to smart tunnel users by destination server and application (port).
- Smart tunnels are supported only on the Microsoft Windows and Apple Mac OS X platforms.



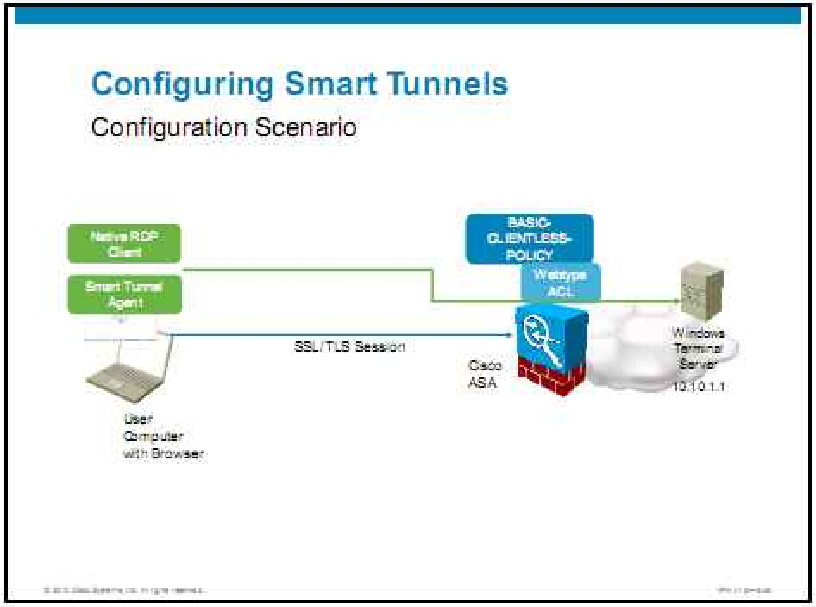
## Configuring Smart Tunnels

Configuration Options

- For applications with native clients:
  - Create smart tunnel list
  - Assign smart tunnel list to a group policy or user profile
- For web-based applications:
  - Add bookmark to bookmark list
  - Enable bookmark for smart tunnel access
  - Bind bookmark list to group policy or user profile
- Control access to internal resources

You have several options when deploying smart tunnel access through a Cisco ASA adaptive security appliance SSL VPN gateway:

- For applications with native clients:
  - Create a smart tunnel list.
  - Assign the smart tunnel list to a group policy or user profile.
- For web-based applications:
  - Add a bookmark to the bookmark list.
  - Enable a bookmark for smart tunnel access.
  - Bind a bookmark list to a group policy or user profile.
- Control access to internal resources.



## Configuring Smart Tunnels

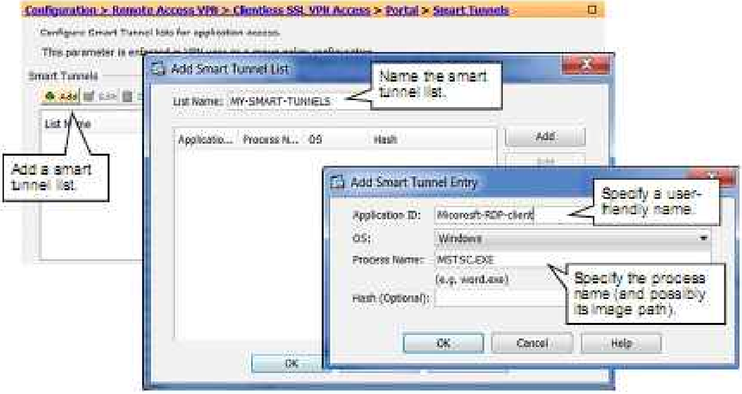
### Configuration Scenario

This figure presents the configuration scenario that is used in upcoming configuration tasks. You will configure the Cisco ASA adaptive security appliance to download and enable the smart tunnel applet to the client, and relay all traffic of the native Microsoft Windows RDP client to the internal network. The remote user will use the native Microsoft Windows RDP client to connect to the internal terminal server at 10.10.1.1. You will also configure the Cisco ASA adaptive security appliance to limit access to the protected network using a webtype ACL, which will only allow the specific RDP connection to the internal network.

As with the previous configuration scenario, this configuration scenario assumes that the Cisco ASA adaptive security appliance is already configured with a basic clientless SSL VPN gateway functionality. It also is assumed that the configuration is using local authentication, authorization, and accounting (AAA) authentication and a verifiable identity certificate and that all local users are assigned the BASIC-CLIENTLESS-POLICY group policy.

## Configuring Smart Tunnels

Create Smart Tunnel List (Native Application Access)



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels
Configure Smart Tunnel lists for application access.
This parameter is enforced in VPN users ...
Smart Tunnels
Add
Edit
List Name
Add Smart Tunnel List
Application...
Process N...
OS
Hash
Add
Edit
OK
Add Smart Tunnel Entry
(e.g. word.exe)
OK
Cancel
Help

List Name: MY-SMART-TUNNELS

Application ID: Microsoft-RDP-client

OS: Windows

Process Name: MSTSC.EXE

Hash (Optional):

Add a smart tunnel list.

Name the smart tunnel list.

Specify a user-friendly name.

Specify the process name (and possibly its image path).

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels

If you want to enable smart tunnel access for applications with a native client, you create a list of applications that are subject to smart tunnels relaying on the remote client.

To configure a smart tunnel list, complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**, and click **Add** to add a new smart tunnel list.

**Step 2** Configure a list name (MY-SMART-TUNNELS in this example), and then click **Add** to add a smart tunnel list entry (that is, application).

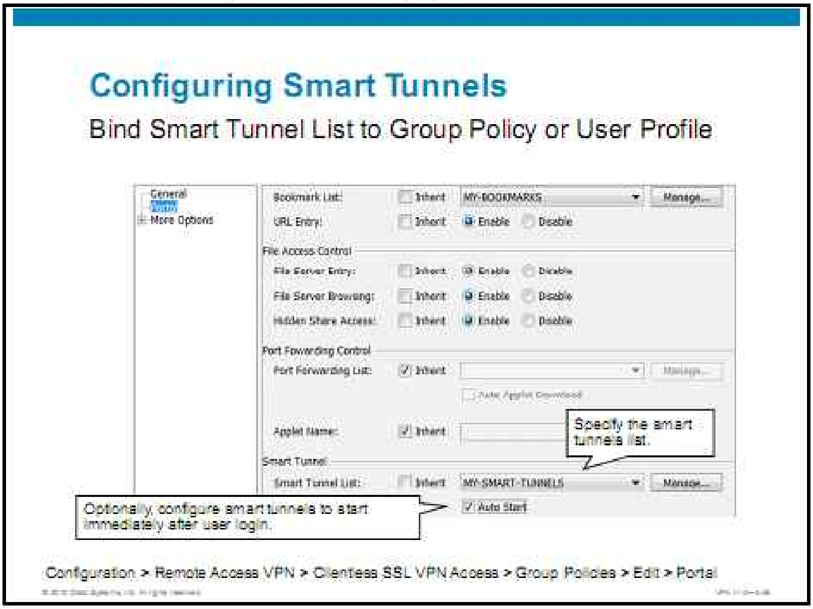
**Step 3** In the Add Smart Tunnel Entry window, specify the properties of the application on the remote system of the user:

- **Application ID:** This is a user-friendly name that will be displayed on the portal, informing users which applications are relayed to the central site.
- **OS:** Specify the operating system on which this entry will be active (Windows or OS X). In this example, Windows is used.
- **Process Name:** Specify the name of the application executable that performs network connections. You can only specify the executable name, or the entire pathname, if you require uniqueness. In this example, the MSTSC.EXE executable name of the Microsoft Windows native RDP client is used.
- **Hash:** Optionally, specify the cryptographic Secure Hash Algorithm 1 (SHA-1) hash of the executable to uniquely identify it. Use this option if there are many executables with the same name, if you want to allow only a specific build or version of the executable to be included in smart tunnels, or to lower the risk of rogue executables being included in smart tunnels. Hashes are only supported on the Windows platform.

**Step 4** Click **OK** twice to accept the new smart tunnel list entry and smart tunnel list.

## Application Image Hashing

To obtain the hash value for an application, enter the checksum of the application (that is, the checksum of the executable file) into a utility that calculates a hash using the SHA-1 algorithm. One example of such a utility is the Microsoft File Checksum Integrity Verifier (FCIV), which is available at http://support.microsoft.com/kb/841290/. After installing FCIV, place a temporary copy of the application to be hashed on a path that contains no spaces (for example, c:\temp\mstsc.exe), then enter **fciv.exe -sha1** *application* at the command line (for example, **fciv.exe -sha1 c:\temp\mstsc.exe**) to display the SHA-1 hash.



### Configuring Smart Tunnels

Bind Smart Tunnel List to Group Policy or User Profile

General
More Options

Bookmark List: ☐ Inherit MY-BOOKMARKS ▾ Manage...
URL Entry: ☐ Inherit ● Enable ○ Disable

File Access Control
File Server Entry: ☐ Inherit ● Enable ○ Disable
File Server Browsing: ☐ Inherit ● Enable ○ Disable
Hidden Share Access: ☐ Inherit ● Enable ○ Disable

Port Fowarding Control
Port Forwarding List: ☑ Inherit ▾ Manage...
☐ Auto Applet Download
Applet Name: ☑ Inherit

Smart Tunnel
Smart Tunnel List: ☐ Inherit MY-SMART-TUNNELS ▾ Manage...
☑ Auto Start

Specify the smart tunnels list.

Optionally configure smart tunnels to start immediately after user login.

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

To enable smart tunnel access for applications with a native client, you will apply a smart tunnel policy to a group policy or user profile.

To modify an existing clientless SSL VPN group policy, complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies** and choose the previously configured clientless SSL VPN group policy (not shown).

**Step 2** Click **Edit** to edit the clientless SSL VPN group policy.

**Step 3** Choose the **Portal** option from the menu in the left pane and uncheck the **Inherit** check box next to the Smart Tunnel List field in the Smart Tunnel area. From the drop-down box, select the configured smart tunnel list—in this example, the MY-SMART-TUNNELS list.

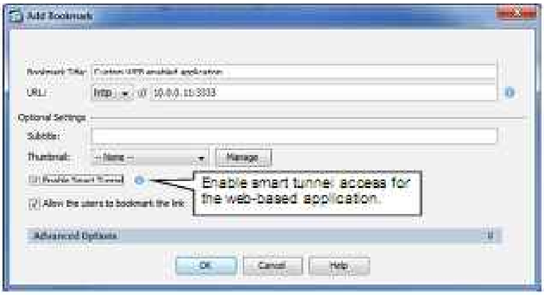
**Step 4** Optionally, check the **Auto Start** check box to configure the smart tunnel to start automatically for this group policy.

**Step 5** Click **OK** and **Apply** to apply the changes to the Cisco ASA adaptive security appliance. Click **Save** to save the configuration, if needed.

## Configuring Smart Tunnels

### Enable Bookmarks for Smart Tunnel Access

- Bookmarked application will display in a separate web browser
- All traffic from that browser will pass over smart tunnel
- Used for web-based application access



Add Bookmark

Bookmark Title: Custom VPN enabled application

URL: http :// 10.0.0.11:3333

Optional Settings

Subtitle:

Thumbnail: -- None --

☑ Enable Smart Tunnel

☑ Allow the users to bookmark the link

Enable smart tunnel access for the web-based application.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks

To deploy smart tunnels for web-based application access, enable a bookmark for smart tunnel by completing these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**, and create a bookmark list or edit an existing one.

**Step 2** Add a bookmark or edit an existing bookmark. In the example, a bookmark for a custom web-based application running on port 3333 is configured.

**Step 3** Check the **Enable Smart Tunnel** check box. Only HTTP and HTTPS bookmarks can be configured for smart tunnel access.

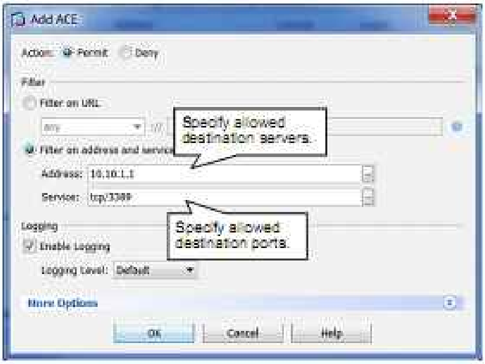
**Step 4** Click **OK** and **Apply** to apply the configuration.

The bookmarked application will appear in a separate web browser, not in the SSL VPN portal. All traffic from that browser will pass over the smart tunnel.

## Configuring Smart Tunnels

### Control Access to Internal Resources

Webtype ACEs support **address and service** syntax.



Add ACE

Action: ● Permit ○ Deny

Filter

○ Filter on URL

any ://

● Filter on address and service

Address: 10.10.1.1

Service: tcp/3389

Logging

☑ Enable Logging

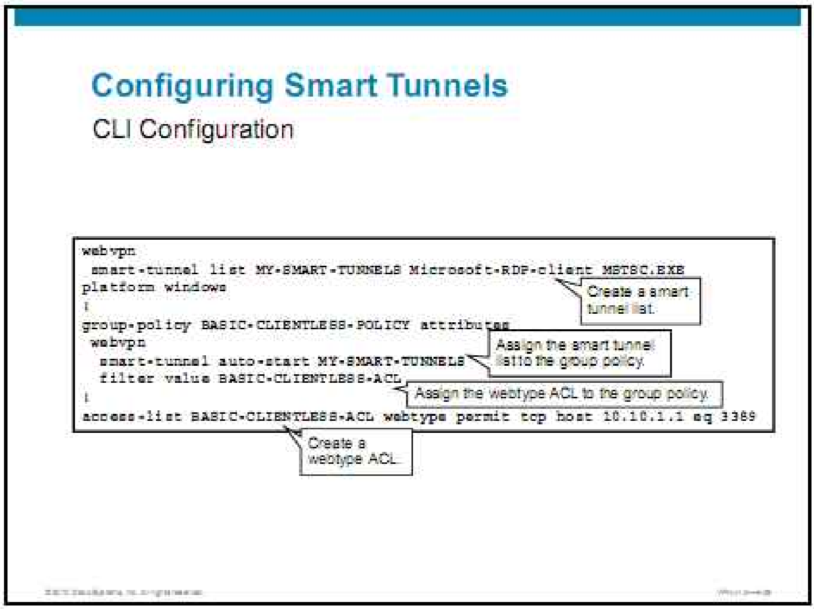
Logging Level: Default

Specify allowed destination servers.

Specify allowed destination ports.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs

You can optionally control access to internal resources by creating or modifying your webtype ACLs to permit or deny smart tunnel access to specific resources. To control access, you should create ACEs in your webtype ACLs that are applied to the desired group policies, and click the **Filter on Address and Service** radio button in the webtype ACE. In this example, the webtype ACE only allows access to the 10.10.1.1 server on TCP port 3389 (RDP).



## Configuring Smart Tunnels

CLI Configuration

```
webvpn
 smart-tunnel list MY-SMART-TUNNELS Microsoft-RDP-client MSTSC.EXE
platform windows
!
group-policy BASIC-CLIENTLESS-POLICY attributes
 webvpn
  smart-tunnel auto-start MY-SMART-TUNNELS
  filter value BASIC-CLIENTLESS-ACL
!
access-list BASIC-CLIENTLESS-ACL webtype permit tcp host 10.10.1.1 eq 3389
```

Create a smart tunnel list.

Assign the smart tunnel list to the group policy.

Assign the webtype ACL to the group policy.

Create a webtype ACL.

This output shows the CLI commands that are required to configure smart tunnel access on the Cisco ASA adaptive security appliance.

In the CLI, enter SSL VPN server configuration submode on the Cisco ASA adaptive security appliance using the **webvpn** command, and configure smart tunnel application lists using the **smart-tunnel list** command. In the example, a smart tunnel list named MY-SMART-TUNNELS, which specifies the RDP Windows applications, is defined.

Next, assign the configured smart tunnel application list to a group policy by entering group-policy attributes mode and then switching to its webvpn submode. Use the **smart-tunnel** command to assign the smart tunnels list. Use the optional **auto-start** argument to automatically download and start the smart tunnel agent. In the example, the MY-SMART-TUNNELS smart tunnel list is applied to the BASIC-CLIENTLESS-POLICY group policy.

Finally, you may create a webtype ACL and ACEs that govern smart tunnel access using the **access-list name webtype** command. In the example, the webtype ACL will only permit access to the 10.10.1.1 server over port 3389 (RDP).

### smart-tunnel list

To populate a list of applications that can use a clientless (browser-based) SSL VPN session to connect to private sites, use the **smart-tunnel list** command in webvpn configuration mode.

To remove an application from a list, use the **no** form of the command, specifying the entry. To remove an entire list of applications from the adaptive security appliance configuration, use the **no** form of the command, specifying only the list.

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]

### smart-tunnel list Parameters

| Parameter | Description |
|---|---|
| *list* | Name of a list of applications or programs. Use quotation marks around the name if it includes a space. The CLI creates the list if it is not present in the configuration. Otherwise, the CLI adds the entry to the list. |
| *application* | Name of the application to be granted smart tunnel access. The string can be up to 64 characters. |
| *path* | For Mac OS, the full path to the application. For Windows, the filename of the application; or a complete or partial path to the application, including its filename. The string can be up to 128 characters. |
| **platform** *OS* | (Optional if the operating system is Microsoft Windows) Enter **windows** or **mac** to specify the host of the application. |
| *hash* | (Optional and applicable only for Windows) Enter the hash of the application. The SHA-1 hash is always 40 hexadecimal characters. |

## smart-tunnel auto-start

To start smart tunnel access automatically upon user login in a clientless (browser-based) SSL VPN session, use the **smart-tunnel auto-start** command in group-policy webvpn configuration mode or username webvpn configuration mode.

To remove the **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group policy, use the **no** form of the command.

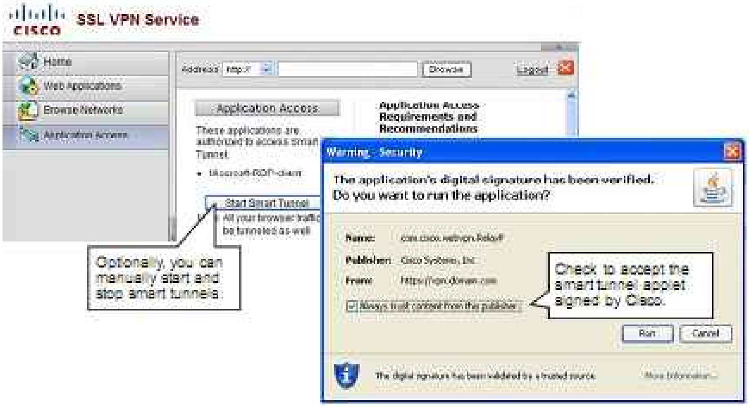
**smart-tunnel auto-start** *list*

### smart-tunnel auto-start Parameters

| Parameter | Description |
|---|---|
| *list* | The name of a smart tunnel list that is already present in the adaptive security appliance webvpn configuration.<br>To view any smart tunnel list entries already present in the SSL VPN configuration, enter the **show running-config webvpn** command in privileged EXEC mode. |

## Verifying Smart Tunnels

### Manual Start (Smart Tunnel List)



These applications are authorized to access Smart Tunnel:

- Microsoft-RDP-client

All your browser traffic will be tunneled as well

Warning - Security

The application's digital signature has been verified.
Do you want to run the application?

Name: com.cisco.webvpn.Relay
Publisher: Cisco Systems, Inc.
From: https://vpn.domain.com

☑ Always trust content from this publisher.

The digital signature has been validated by a trusted source.

Optionally, you can manually start and stop smart tunnels.

Check to accept the smart tunnel applet signed by Cisco.

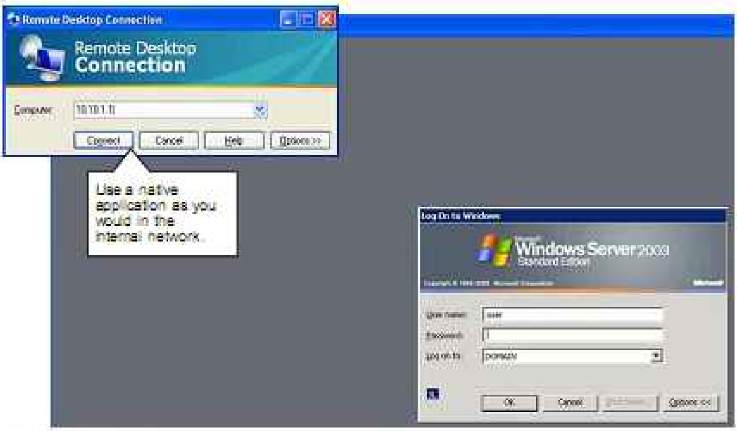
To verify the availability of smart tunnels and their proper operation, log into the SSL VPN portal. You should see an Application Access view on the left side of the SSL VPN portal home page.

If you have configured smart tunnels to start automatically, the browser will automatically download and execute the smart tunnel relay agent. You will be prompted to inspect and accept digitally signed smart tunnel relay applets from the SSL VPN gateway.

If you have not configured smart tunnels to start automatically, select the Application Access view, and click the **Start Smart Tunnel** button. The browser will download and execute the smart tunnel relay agent on demand.

## Verifying Smart Tunnels

### Manual Start with RDP Example (Smart Tunnel List)



Computer: 10.10.1.10

Use a native application as you would in the internal network.

User name: user

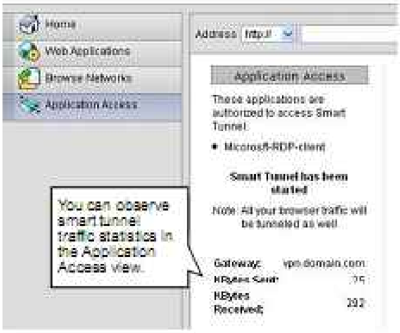
Password:

Log on to: DOMAIN

After the smart tunnel relay agent is running, you can now start the native applications that are present in the smart tunnel list of your group policy and access internal resources directly (from an end-user perspective). In this example, the native Microsoft Windows RDP client is used as it were started in a non-VPN environment (or a full tunneling Cisco AnyConnect session), displaying the login page of an internal server.

## Verifying Smart Tunnels

### Statistics (Smart Tunnel List)



Application Access

These applications are authorized to access Smart Tunnel:

- Micorosft-RDP-client

**Smart Tunnel has been started**

Note: All your browser traffic will be tunneled as well.

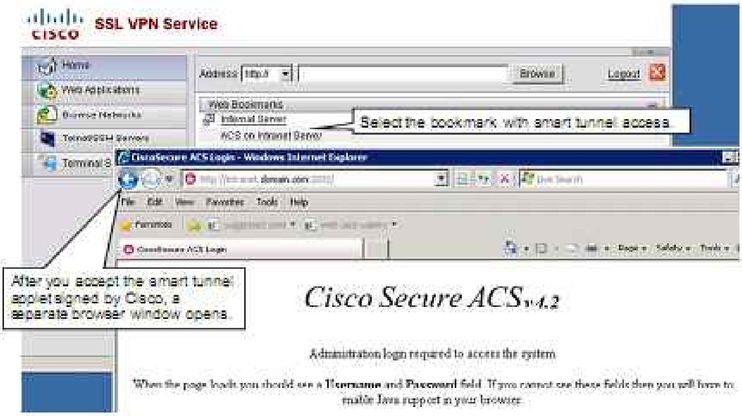
You can observe smart tunnel traffic statistics in the Application Access view.

| | |
|---|---|
| Gateway: | vpn.domain.com |
| KBytes Sent: | 25 |
| KBytes Received: | 292 |

In the Application Access view, you can also observe basic smart tunnel statistics and settings, such as the list of applications that are enabled for smart tunneling and the amount of data that is exchanged through the smart tunnel session since its start.

# Verifying Smart Tunnels

## Bookmark



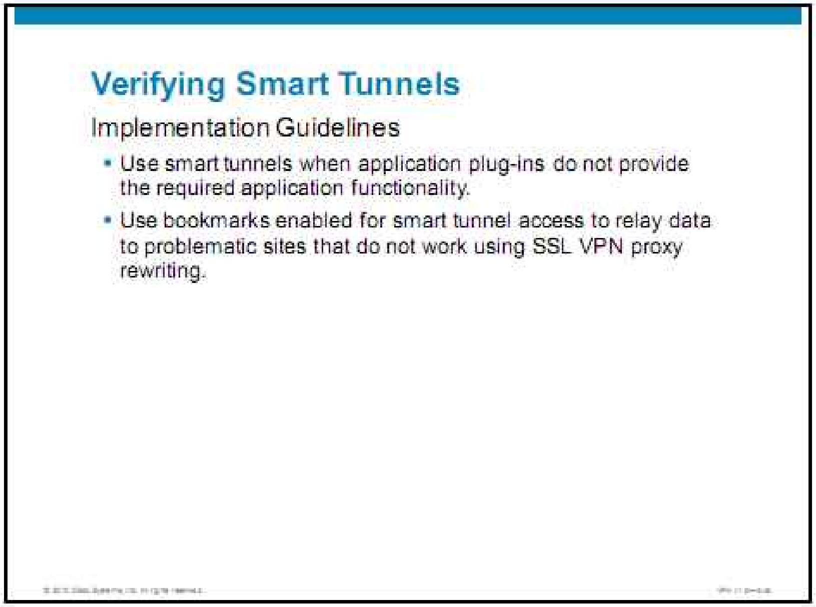
Select the bookmark with smart tunnel access.

After you accept the smart tunnel applet signed by Cisco, a separate browser window opens.

Administration login required to access the system

When the page loads you should see a **Username** and **Password** field. If you cannot see these fields then you will have to enable Java support in your browser.

This figure illustrates smart tunnel access using a bookmark. When you select the bookmark, the application will display in a separate browser window. You must accept the smart tunnel applet that is signed by Cisco before using the application.



## Verifying Smart Tunnels

Implementation Guidelines

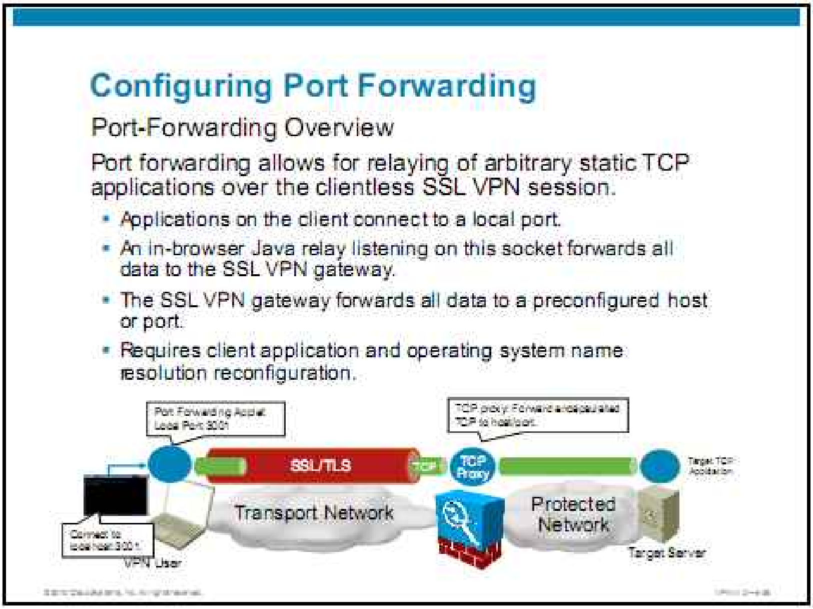
- Use smart tunnels when application plug-ins do not provide the required application functionality.
- Use bookmarks enabled for smart tunnel access to relay data to problematic sites that do not work using SSL VPN proxy rewriting.

When you implement smart tunnel access in clientless SSL VPNs, consider the following guidelines:

- Use smart tunnel access as the preferred method to support native remote user applications, especially when you cannot support a business process with application plug-ins.
- You can also use smart tunnels as a remedy for applications that have issues with the SSL VPN proxy rewriting engine. Use bookmarks enabled for smart tunnel access to relay data to problematic sites.

# Configuring Port Forwarding

This topic describes how to configure and verify port forwarding in clientless SSL VPN.



## Configuring Port Forwarding

Port-Forwarding Overview

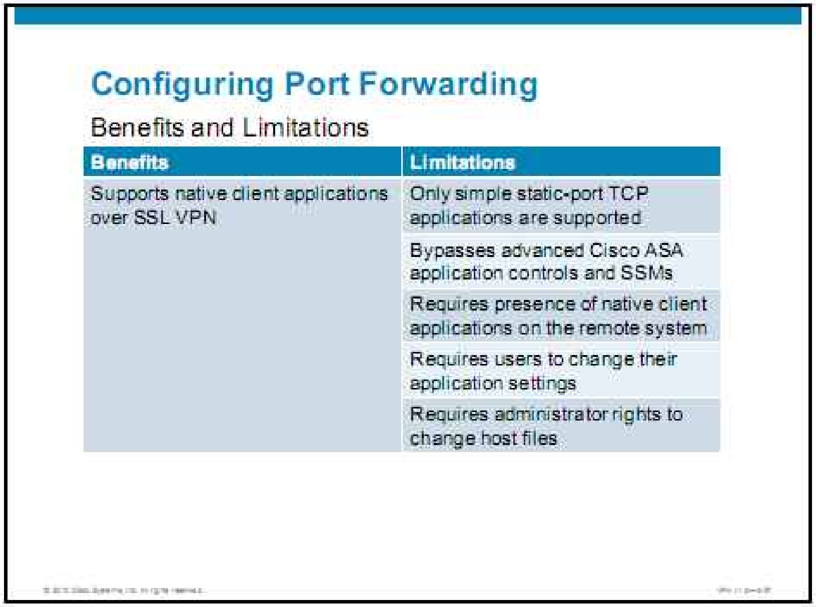
Port forwarding allows for relaying of arbitrary static TCP applications over the clientless SSL VPN session.

- Applications on the client connect to a local port.
- An in-browser Java relay listening on this socket forwards all data to the SSL VPN gateway.
- The SSL VPN gateway forwards all data to a preconfigured host or port.
- Requires client application and operating system name resolution reconfiguration.

Port forwarding is a legacy technology for supporting TCP-based applications over a clientless SSL VPN connection. Port forwarding is an alternative to smart tunnels, and makes use of a local Java helper applet to provide access to certain applications that are not supported by clientless SSL VPN by default. The Java helper application requires local applications to make a connection to the local host to provide port-forwarding functionality, and hence require some modification of application settings or user actions.

This figure illustrates the port forwarding process to access an internal Telnet server:

1. After SSL VPN portal login, a port-forwarding Java applet that was downloaded from the SSL VPN portal is started inside the browser. The applet dynamically modifies the local hosts file, and listens on the loopback address of the remote host at port 3001 to forward any incoming connections over the SSL VPN session.
2. A user opens a Telnet client and attempts to connect to an internal server, on port 3001.
3. The local hosts file, which is dynamically modified by the Java applet, is analyzed. It has an entry for the internal server, which points to 127.0.0.1. The Telnet client connects to the local host on port 3001. The Java applet forwards this connection over the SSL VPN session to the SSL VPN gateway.
4. The VPN gateway extracts the TCP session from the SSL VPN session, establishes a TCP connection with the destination on the standard Telnet port (23), and acts as a data relay between the two TCP sessions.



## Configuring Port Forwarding

Benefits and Limitations

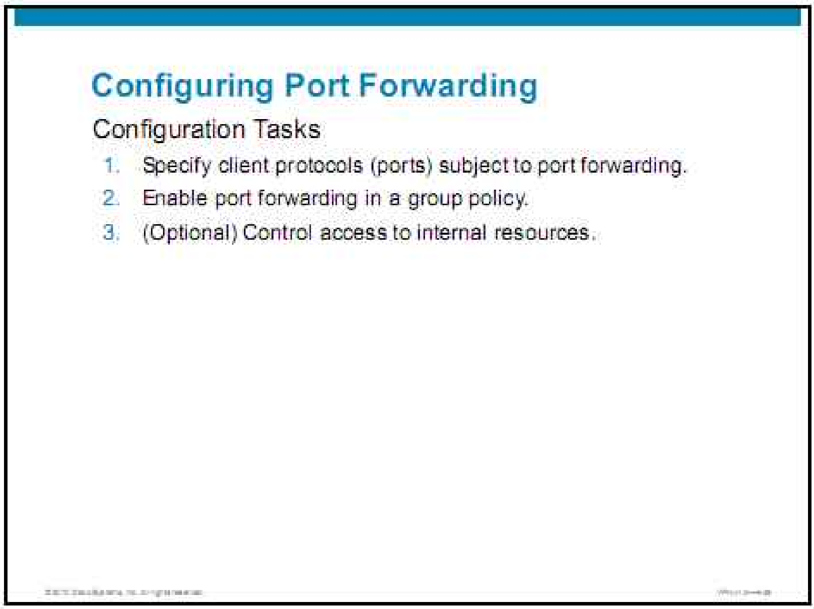
| Benefits | Limitations |
|---|---|
| Supports native client applications over SSL VPN | Only simple static-port TCP applications are supported |
| | Bypasses advanced Cisco ASA application controls and SSMs |
| | Requires presence of native client applications on the remote system |
| | Requires users to change their application settings |
| | Requires administrator rights to change host files |

The benefits of port forwarding are as follows:

- They support the use of fully featured, native applications that are already installed on the system of the remote user.

The limitations of port forwarding are as follows:

- Port forwarding only supports simple, static-port TCP applications.
- Access to the internal network bypasses the advanced Cisco ASA adaptive security appliance application layer controls and security services modules. However, you can control the resources that are available to port forwarding users by destination server and application (port).
- It requires preinstalled native applications on the remote system.
- It requires users to change their application settings (for example, the destination port of the server), and even their application usage (if a different application profile is needed for non-VPN and VPN use).
- Port forwarding requires administrative rights because it changes the local hosts file.



## Configuring Port Forwarding

Configuration Tasks

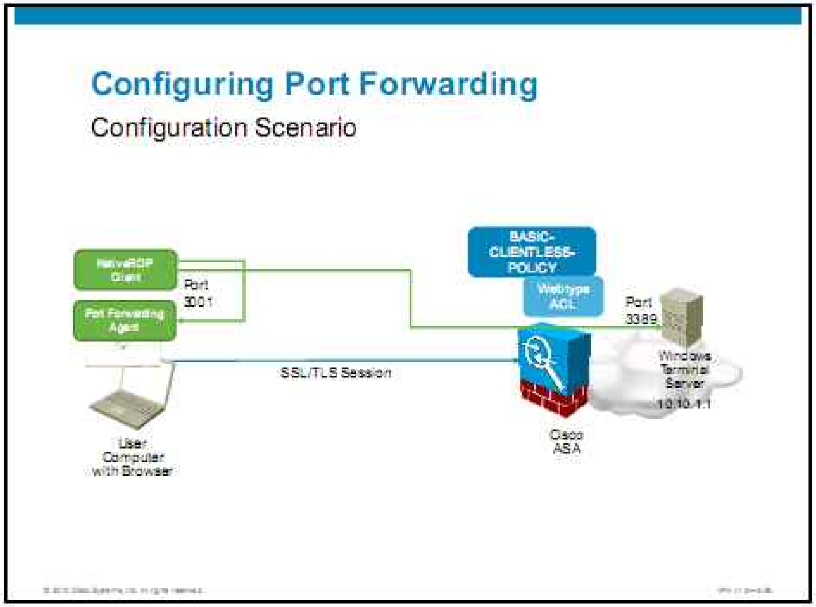
1. Specify client protocols (ports) subject to port forwarding.
2. Enable port forwarding in a group policy.
3. (Optional) Control access to internal resources.

To configure port forwarding access through a Cisco ASA adaptive security appliance SSL VPN gateway, you will perform the following configuration tasks:

1. Specify the client application protocols (ports) that are subject to port forwarding after SSL VPN login.

2. Enable port forwarding in a group policy, and optionally specify that the port-forwarding applet should start automatically after SSL VPN login.

3. Optionally, deploy access control features on the Cisco ASA adaptive security appliance SSL VPN gateway to control access from applications using port forwarding to internal resources.



## Configuring Port Forwarding

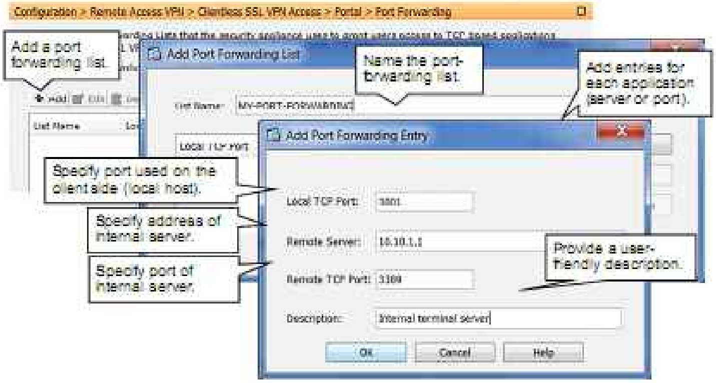
Configuration Scenario

This figure presents the configuration scenario that is used in upcoming configuration tasks. You will configure the Cisco ASA adaptive security appliance to download and enable the Java port-forwarding applet to the client. The Java port-forwarding client listens for incoming TCP connections from the local host, on the local TCP port of 3001, and relays these connections to the internal terminal server at 10.10.1.1. The remote user uses the native Microsoft RDP client to connect to the local port, which relays the RDP session to the internal terminal server. You will also configure the Cisco ASA adaptive security appliance to limit access to the protected network using a webtype ACL, which only allows the specific RDP connection to the internal network.

As with the previous configuration scenario, this configuration scenario assumes that the Cisco ASA adaptive security appliance is already configured with a basic clientless SSL VPN gateway functionality. It is also assumed that the configuration is using local AAA authentication and a verifiable identity certificate, and that all local users are assigned the BASIC-CLIENTLESS-POLICY group policy.

## Configuring Port Forwarding

Task 1: Specify Client Protocols for Port Forwarding


Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding
Add Port Forwarding List
Add Port Forwarding Entry
Add
Edit
List Name
OK
Cancel
Help

Add a port forwarding list.

Name the port-forwarding list.

List Name: MY-PORT-FORWARDING

Add entries for each application (server or port).

Specify port used on the client side (local host).

Local TCP Port: 3001

Specify address of internal server.

Remote Server: 10.10.1.1

Specify port of internal server.

Remote TCP Port: 3389

Provide a user-friendly description.

Description: Internal terminal server

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding

In the first configuration task of this configuration sequence, you will create a list of remote application ports and internal resources that are subject to port forwarding on the remote client. You can specify a single list of ports and internal resources for each group policy, which you can apply to one or more connection profiles.

To configure a port-forwarding list, complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding**, and click **Add** to add a new port-forwarding list.

**Step 2** Configure a list name (MY-PORT-FORWARDING in this example) and then click **Add** to add a port-forwarding entry.

**Step 3** Configure the port-forwarding list entry with the following information:

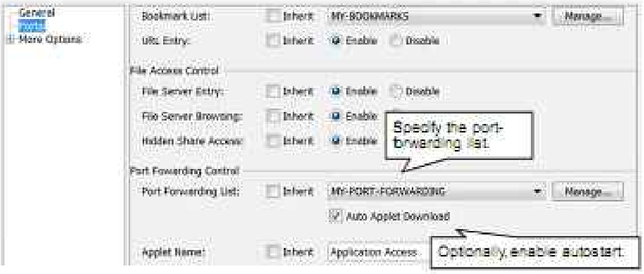
- **Local TCP Port:** The port that the Java applet will listen on for port forwarding of this entry. In this example, TCP port 3001 is used. To avoid conflicts with existing services on the local host, use a port number greater than 1024.
- **Remote Server:** The address of the target server in the protected network. You can also provide the name of a remote server. If you provide the name, the Java applet will modify the local host file. Recall that administrator privileges are needed to change the local host file.
- **Remote TCP Port:** The port that the target server in the protected network will listen on for network connections.
- **Description:** User-friendly description of the port-forwarding entry.

**Step 4** Click **OK** twice to accept the new port-forwarding entry and port-forwarding list.

**Note** Remember that the connection is only cryptographically protected between the remote user and the Cisco ASA adaptive security appliance. If a protocol such as Telnet is used with port forwarding, the traffic leaving the security appliance will not be encrypted.

## Configuring Port Forwarding

### Task 2: Enable Port Forwarding in a Group Policy



Bookmark List: □ Inherit MY-BOOKMARKS ▾ Manage...
URL Entry: □ Inherit ● Enable ○ Disable

File Access Control
File Server Entry: □ Inherit ● Enable ○ Disable
File Server Browsing: □ Inherit ● Enable
Hidden Share Access: □ Inherit ● Enable

Port Fowarding Control
Port Forwarding List: □ Inherit MY-PORT-FORWARDING ▾ Manage...
☑ Auto Applet Download
Applet Name: □ Inherit Application Access

Specify the port-forwarding list.

Optionally, enable autostart.

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

In the second configuration task, you will apply a port-forwarding policy to a group policy, which will in turn enable port forwarding on one or more connection profiles.

To modify the existing Clientless SSL VPN group policy, complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**, and choose the previously configured Clientless SSL VPN group policy.

**Step 2** Click **Edit** to edit the Clientless SSL VPN group policy.

**Step 3** Choose the **Portal** option from the menu in the left pane and uncheck the **Inherit** check box from the Port-Forwarding List and Applet Name fields.

**Step 4** Choose the configured port-forwarding list (MY-PORT-FORWARDING) from the drop-down menu, and check the **Auto Applet Download** check box. The Auto Applet Download option will automatically start the configured port-forwarding configuration after the user logs into the SSL VPN portal.

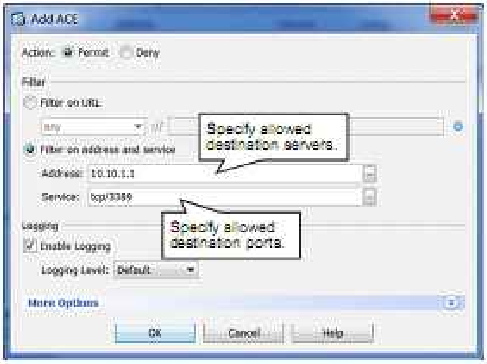
**Step 5** Optionally, configure an applet name for the application to be used with the Port-Forwarding SSL VPN.

**Step 6** Click **OK** and **Apply** to apply the changes to the Cisco ASA adaptive security appliance. Click **Save** to save the configuration, if necessary.

## Configuring Port Forwarding

Task 3: (Optional) Control Access to Internal Resources

Webtype ACEs support **address and service** syntax.



Add ACE

Action: ● Permit ○ Deny

Filter

○ Filter on URL

any ▾ ://

● Filter on address and service

Address: 10.10.1.1

Service: tcp/3389

Logging

☑ Enable Logging

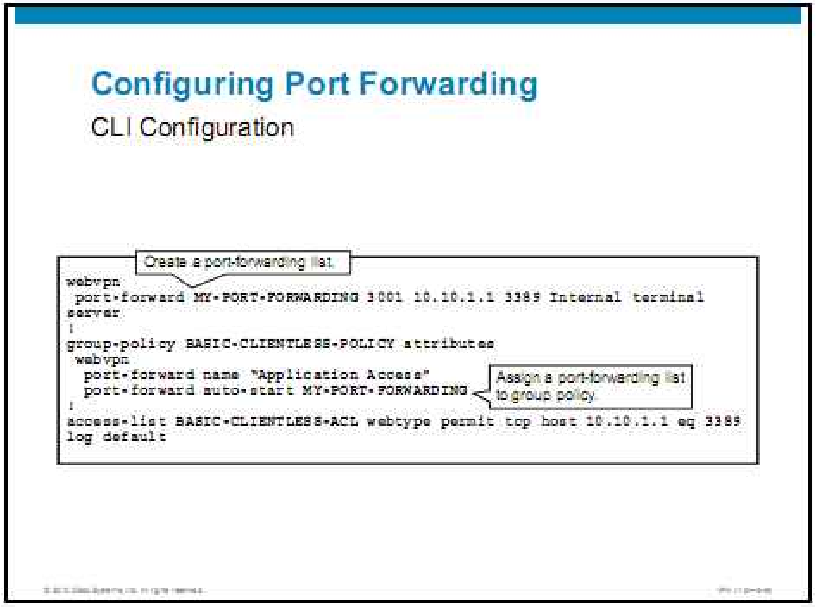
Logging Level: Default ▾

Specify allowed destination servers.

Specify allowed destination ports.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs

In the third task, you can optionally control access to internal resources by creating or modifying your webtype ACLs to permit or deny port-forwarding access to specific resources. The configuration of these rules is the same as with the smart tunnel feature.



## Configuring Port Forwarding

CLI Configuration

Create a port-forwarding list

```
webvpn
 port-forward MY-PORT-FORWARDING 3001 10.10.1.1 3389 Internal terminal
server
!
group-policy BASIC-CLIENTLESS-POLICY attributes
 webvpn
  port-forward name "Application Access"
  port-forward auto-start MY-PORT-FORWARDING
!
access-list BASIC-CLIENTLESS-ACL webtype permit tcp host 10.10.1.1 eq 3389
log default
```

Assign a port-forwarding list to group policy

This output shows the CLI commands that are required to configure port forwarding on the Cisco ASA adaptive security appliance.

In the CLI, enter SSL VPN server configuration submode on the Cisco ASA adaptive security appliance using the **webvpn** command, and create a port-forwarding list and its entries using one or more **port-forward** commands. Next, assign the port-forwarding list to a group policy, in its group-policy attributes mode and webvpn submode, using the **port-forward name** command. Optionally, configure the Cisco ASA adaptive security appliance to automatically start the port-forwarding applet using the **port-forward auto-start** command. Finally, you may create a webtype ACL and ACEs that govern port forwarding access using the **access-list** *name* **webtype** command.

In the example, a port forwarding list named MY-PORT-FORWARDING, which specifies a local port of 3001, with the remote server IP address of 10.10.1.1 and a remote port of 3389 is defined. A description about this port-forwarding list is also configured.

The MY-PORT-FORWARDING port-forwarding list is applied to the BASIC-CLIENTLESS-POLICY group policy. Autostart is enabled and a name that identifies the port forwarding to the users is also configured.

The webtype ACL will only permit access to the 10.10.1.1 server over port 3389 (RDP).

## port-forward

To configure the set of applications that users of a clientless SSL VPN session can access over forwarded TCP ports, use the **port-forward** command in webvpn configuration mode.

**port-forward** {*list_name local_port remote_server remote_port description*}

To configure access to multiple applications, use this command with the same *list_name* multiple times, once for each application.

To remove a configured application from a list, use the **no port-forward** *list_name local_port* command (you do not need to include the *remote_server* and *remote_port* parameters).

**no port-forward** *listname localport*

To remove an entire configured list, use the **no port-forward** *list_name* command.

**no port-forward** *list_name*

### port-forward Parameters

| Parameter | Description |
|---|---|
| *description* | Provides the application name or short description that displays on the end-user Port Forwarding Java applet screen. Maximum 64 characters. |
| *list_name* | Groups the set of applications (forwarded TCP ports) that users of clientless SSL VPN sessions can access. Maximum, 64 characters. |
| *local_port* | Specifies the local port that listens for TCP traffic for an application. You can use a local port number only once for a *list_name*. Enter a port number in the range 1–65,535. To avoid conflicts with existing services, use a port number greater than 1024. |
| *remote_port* | Specifies the port to connect to for this application on the remote server. This is the actual port that the application uses. Enter a port number in the range **1–**65,535 or port name. |
| *remote_server* | Provides the DNS name or IP address of the remote server for an application. If you enter the IP address, you may enter it in either IP version 4 (IPv4) or IP version 6 (IPv6) format. Cisco recommends using a hostname so that you do not have to configure the client applications for a specific IP address. The **dns server-group name-server** command must resolve the hostname to an IP address. |

## port-forward-name

To configure the display name that identifies TCP port forwarding to end users for a particular user or group policy, use the **port-forward-name** command in webvpn mode, which you enter from group-policy or username mode. To delete the display name, including a null value that is created by using the **port-forward-name none** command; use the **no** form of the command. The **no** option restores the default name, Application Access. To prevent a display name, use the **port-forward none** command.

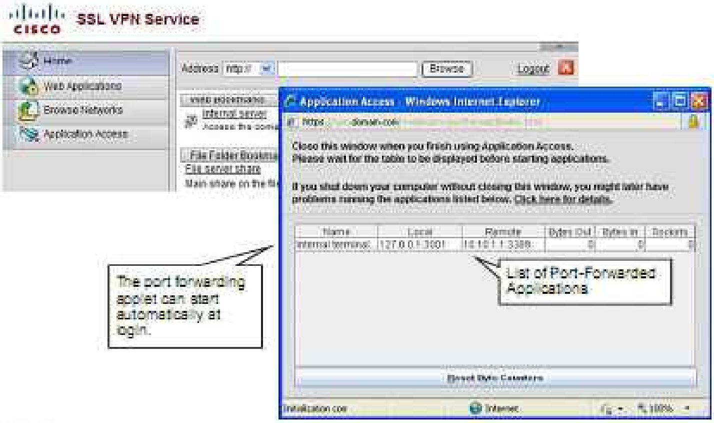
**port-forward-name** {**value** *name* | **none**}

### port-forward-name Parameters

| Parameter | Description |
|---|---|
| **none** | Indicates that there is no display name. Sets a null value, which disallows a display name. Prevents inheriting a value. |
| **value** *name* | Describes port forwarding to end users. Maximum of 255 characters. |

## Verifying Port Forwarding

### Autostart



Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.

If you shut down your computer without closing this window, you might later have problems running the applications listed below. Click here for details.

| Name | Local | Remote | Bytes Out | Bytes In | Sockets |
|---|---|---|---|---|---|
| internal terminal | 127.0.0.1:3001 | 10.10.1.1:3389 | 0 | 0 | 0 |

The port forwarding applet can start automatically at login.

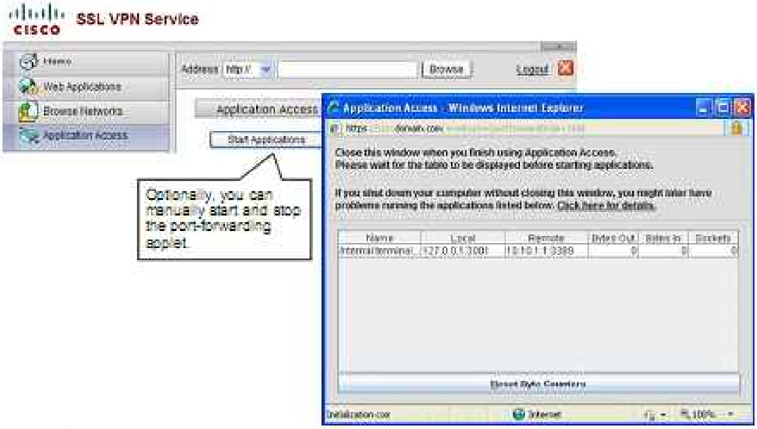
List of Port-Forwarded Applications

To verify the availability of port forwarding and its proper operation, log into the SSL VPN portal. You should see an Application Access view on the left side of the SSL VPN portal home page.

If you have configured the port-forwarding applet to start automatically, the browser will automatically download and execute the Java applet, which will use a separate popup window. In most browsers, you have to authorize this popup window separately.

## Verifying Port Forwarding

Manual Start



Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.

If you shut down your computer without closing this window, you might later have problems running the applications listed below. Click here for details.

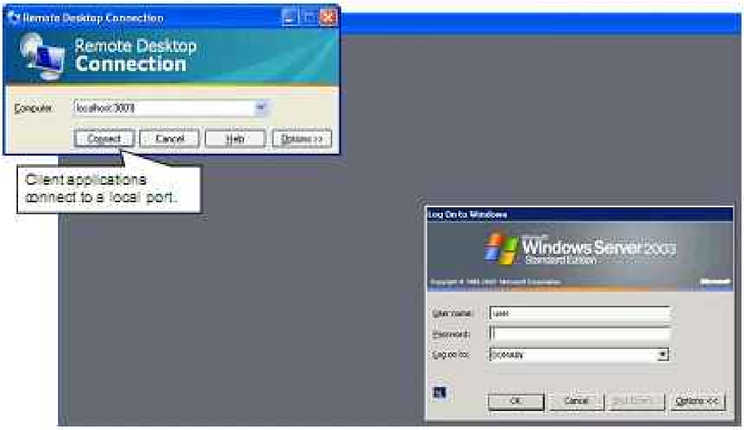
| Name | Local | Remote | Bytes Out | Bytes In | Sockets |
|---|---|---|---|---|---|
| internal terminal | 127.0.0.1:3001 | 10.10.1.1:3389 | 0 | 0 | 0 |

Optionally, you can manually start and stop the port-forwarding applet.

If you have not configured port forwarding to start automatically, select the Application Access view, and click the **Start Applications** button. The browser will download and execute the Java port-forwarding applet on demand.

## Verifying Port Forwarding

RDP Example



Computer: localhost:3001

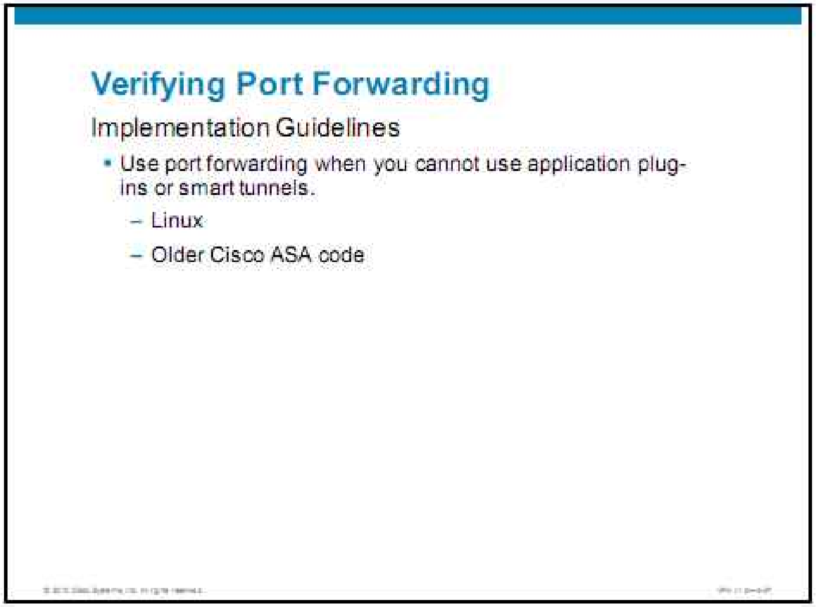
User name: user

Password:

Log on to: DOMAIN

Client applications connect to a local port.

After the port forwarding Java applet is running, you can start a native application and access internal resources by either connecting to a local host port (as shown in this figure) or by connecting to the real hostname of the internal server. You connect over the local port (3001 in this example) of the Java applet because the Java applet will also modify the hosts file. In this example, the native Microsoft Windows RDP client connects to the local host port, where it is forwarded to an internal RDP internal server.



## Verifying Port Forwarding

### Implementation Guidelines

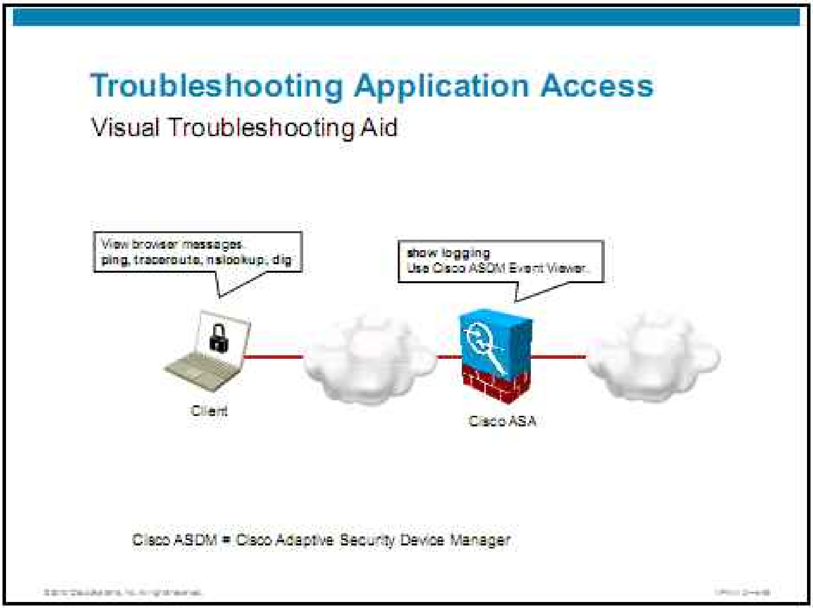
- Use port forwarding when you cannot use application plug-ins or smart tunnels.
  - Linux
  - Older Cisco ASA code

When you implement port forwarding in clientless SSL VPNs, consider the following guideline:

- Use port forwarding to support native remote-user applications when smart tunnels are not available or cannot be deployed. Examples include Linux workstations or deployments of older Cisco ASA adaptive security appliance code.

# Troubleshooting Advanced Application Access

This topic describes how to troubleshoot advanced application access in clientless SSL VPN.



## Troubleshooting Application Access

Visual Troubleshooting Aid

View browser messages.
ping, traceroute, nslookup, dig

show logging
Use Cisco ASDM Event Viewer.

Cisco ASDM = Cisco Adaptive Security Device Manager

When you troubleshoot advanced application access in clientless SSL VPNs, you should perform troubleshooting tasks on both the client and the Cisco ASA adaptive security appliance, if possible. This figure shows some most useful troubleshooting commands and actions that you can use on the involved components.

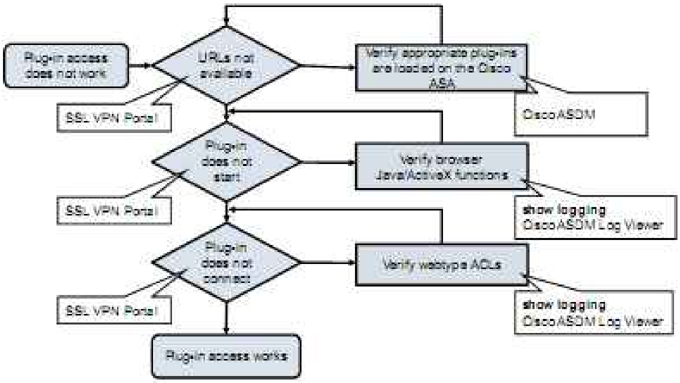
On the client, you can use operating system utilities to determine the reason for connectivity or name resolution issues. Here are some examples of these utilities:

- The **ping** utility to determine Layer 3 reachability of the Cisco ASA adaptive security appliance from the client
- The **traceroute** utility to troubleshoot Layer 3 path problems between the client and the Cisco ASA adaptive security appliance
- The **nslookup** and **dig** utilities to troubleshoot name resolution, if the browser or application cannot resolve the URL for the SSL VPN portal or an internal resource

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

## Troubleshooting Application Access

Application Plug-Ins



If you are encountering access issues with application plug-ins, you may follow these steps to troubleshoot the issue:

**Step 1** First, check that the URL type you are trying to access is available on the Cisco ASA adaptive security appliance (for example, in the free URL entry field). If they are not, you may have forgotten to import a specific application plug-in into the Cisco ASA adaptive security appliance.

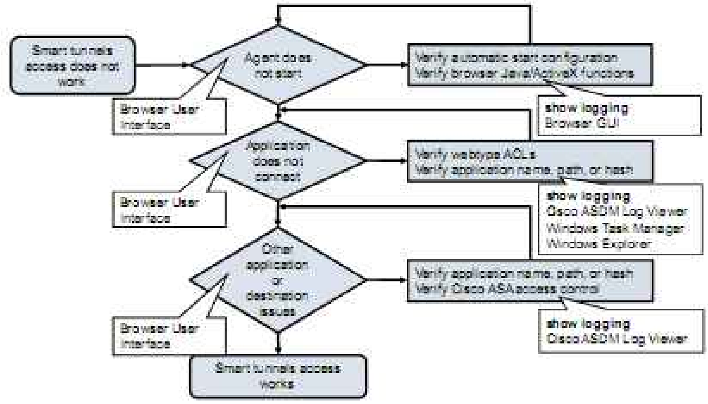
**Step 2** If URLs are available, but the application plug-ins do not start, you may have a client configuration or compatibility issue. Verify that the SSL VPN gateway is added to the list of trusted sites, that the client system has a supported release of the Java Runtime Environment, or that it supports ActiveX control execution.

**Step 3** Finally, if the application plug-ins start but cannot connect to the target server, verify webtype ACLs on the Cisco ASA adaptive security appliance to see if they permit or deny the connection. Additionally, verify that the SSL VPN gateway has a route to the target server, the target server has a route to the SSL VPN gateway, and there is no access control between them that could impair communications.

If these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.

## Troubleshooting Application Access

### Smart Tunnels



Smart tunnels access does not work

Agent does not start

Browser User Interface

Verify automatic start configuration
Verify browser Java/ActiveX functions

**show logging**
Browser GUI

Application does not connect

Browser User Interface

Verify webtype ACLs
Verify application name, path, or hash

**show logging**
Cisco ASDM Log Viewer
Windows Task Manager
Windows Explorer

Other application or destination issues

Browser User Interface

Verify application name, path, or hash
Verify Cisco ASA access control

**show logging**
Cisco ASDM Log Viewer

Smart tunnels access works

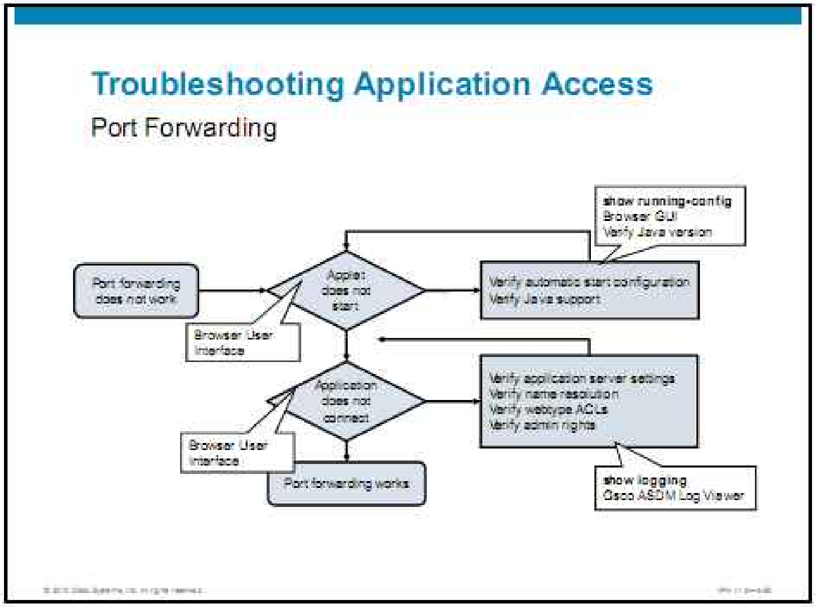
If you are encountering access issues with smart tunnels, you may follow these steps to troubleshoot the issue:

**Step 1** First, check that the smart tunnel agent starts. If it does not, verify that the client system has a supported release of the Java Runtime Environment, or that it supports ActiveX control execution.

**Step 2** If the agent starts, but your application does not connect, verify that you have specified the correct application name (for example, using the Windows Task Manager or Explorer on a remote Windows system) or hash. Also, verify webtype ACLs on the Cisco ASA adaptive security appliance to see if they permit or deny the connection. Additionally, verify that the SSL VPN gateway has a route to the target server, the target server has a route to the SSL VPN gateway, and there is no access control between them that could impair communications.

**Step 3** Finally, if other applications that are not included in the Smart Tunnels policy on your system are experiencing connectivity problems, ensure that you have not specified additional, unwanted applications in the smart tunnel list using wildcarding. Additionally, if you have problems accessing only specific destinations, verify that the Cisco ASA adaptive security appliance is not blocking them, for example, by preventing same-security-level communication.

If these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.



## Troubleshooting Application Access

Port Forwarding

If you are encountering access issues with port forwarding, you may follow these steps to troubleshoot the issue:

**Step 1** First, check that the port-forwarding Java applet starts. If it does not, verify that the client system has a supported release of the Java Runtime Environment.

**Step 2** Verify that the Java applet has correctly configured the client system:

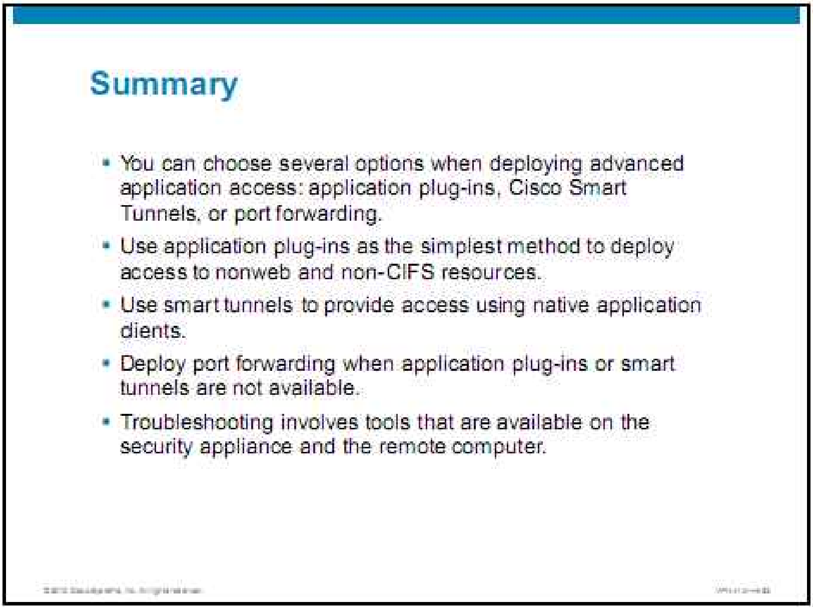
- On the client PC, open a command prompt window and use the **netstat –an** command to verify that local listening ports have been opened by the Port Forwarding applet.
- Verify that the hosts file on the client computer has been updated to support TCP port forwarding. Examine the hosts file in the Windows system32\drivers\etc subfolder to see if entries with a local host address have been added after the applet starts.

**Step 3** If the agent starts, but your application does not connect, verify that you have specified the correct ports in the application, that names are correctly resolved to local host, and that the user has administrative rights. Next, verify webtype ACLs on the Cisco ASA adaptive security appliance to see if they permit or deny the connection. Additionally, verify that the SSL VPN gateway has a route to the target server, the target server has a route to the SSL VPN gateway, and there is no access control between them that could impair communications.

If these steps do not resolve your issue, you may need to deploy troubleshooting tools that are beyond the scope of this course.

# Summary

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



## Summary

- You can choose several options when deploying advanced application access: application plug-ins, Cisco Smart Tunnels, or port forwarding.
- Use application plug-ins as the simplest method to deploy access to nonweb and non-CIFS resources.
- Use smart tunnels to provide access using native application clients.
- Deploy port forwarding when application plug-ins or smart tunnels are not available.
- Troubleshooting involves tools that are available on the security appliance and the remote computer.

## Lesson 3

# Deploying Advanced Authentication and SSO in a Clientless SSL VPN

## Overview

Most enterprises need scalable authentication schemes, in which the network devices offload the authentication process to back-end user databases, such as Lightweight Directory Access Protocol (LDAP), TACACS+, or RADIUS. In clientless SSL VPNs, public key infrastructure (PKI) offers a scalable and secure authentication method. This lesson discusses the various authentication approaches that should be evaluated when designing a clientless SSL VPN solution, including the option of combining multiple authentications in a single process. In the lesson, you will learn how to provide user-friendly authentication strategy, by requiring only a single sign-on (SSO) when accessing various resources.

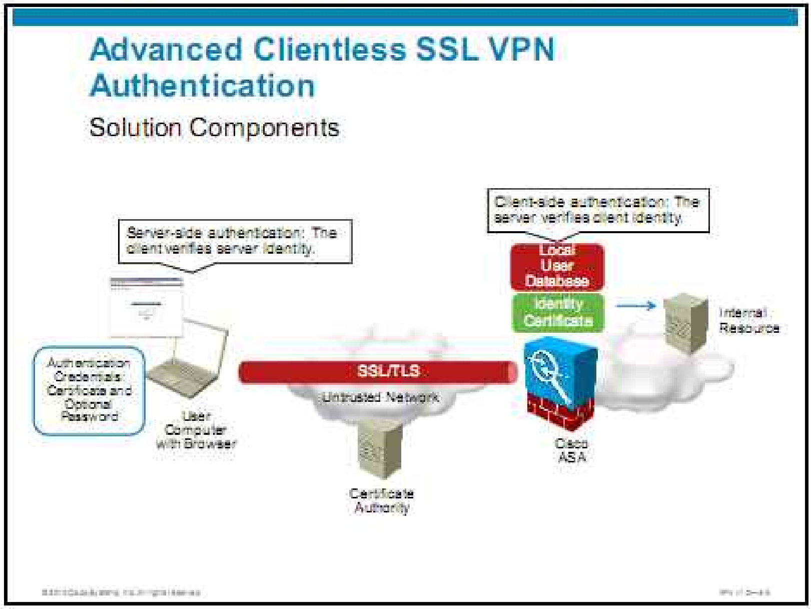
### Objectives

Upon completing this lesson, you will be able to deploy and manage advanced authentication features of a clientless Cisco SSL VPN. This ability includes being able to meet these objectives:

- Plan the deployment of advanced client authentication in clientless SSL VPNs
- Configure and verify the local CA or integrate with an external CA and provision client certificates
- Configure and verify integration with supporting PKI entities and verify external certificate authorization
- Troubleshoot advanced client authentication in clientless SSL VPNs
- Configure and verify clientless VPN SSO methods

# Configuration Choices, Basic Procedures, and Required Input Parameters

This topic describes how to design clientless SSL VPN authentication.



## Advanced Clientless SSL VPN Authentication

Solution Components

Server-side authentication: The client verifies server identity.

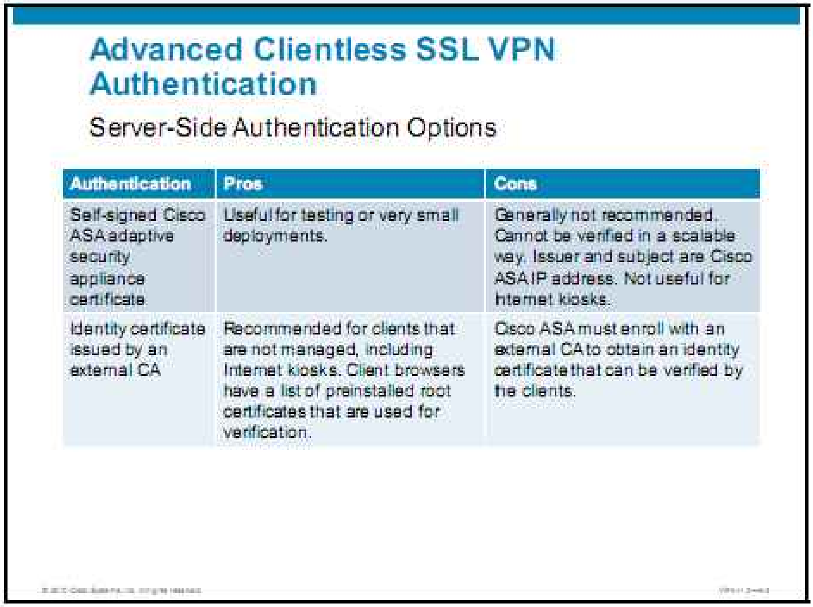
Client-side authentication: The server verifies client identity.

A key aspect of a SSL VPN is secure user authentication. You should consider these features as you design the authentication system:

- **Security:** This aspect is related to the security of the authentication protocol and the trustworthiness of the user credentials. SSL is considered a trusted protocol, but the security depends on the strength of user credentials. In general, static passwords are considered a weaker authentication means than certificates or one-time passwords (OTP). Highest security is obtained by combining various authentication methods together.
- **Scalability:** This design consideration is related to how easy it is to provision new users and maintain the authentication system. Maintenance involves such tasks as credential revocation, high availability, and accountability.
- **Integration:** This design consideration involves integration with existing user databases.

Authentication in an SSL VPN occurs in two stages:

- Server-side authentication, in which the client verifies the authenticity of the server
- Client-side authentication, in which the server verifies the authenticity of the clients



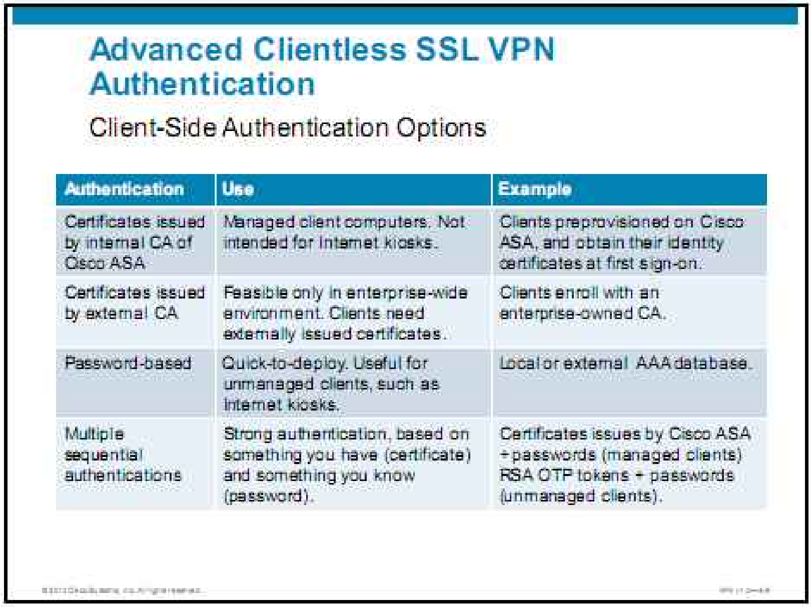
## Advanced Clientless SSL VPN Authentication

### Server-Side Authentication Options

| Authentication | Pros | Cons |
|---|---|---|
| Self-signed Cisco ASA adaptive security appliance certificate | Useful for testing or very small deployments. | Generally not recommended. Cannot be verified in a scalable way. Issuer and subject are Cisco ASA IP address. Not useful for Internet kiosks. |
| Identity certificate issued by an external CA | Recommended for clients that are not managed, including Internet kiosks. Client browsers have a list of preinstalled root certificates that are used for verification. | Cisco ASA must enroll with an external CA to obtain an identity certificate that can be verified by the clients. |

Server-side authentication of a clientless SSL VPN session can be based on these two things:

- **Self-signed Cisco ASA adaptive security appliance certificate:** This certificate is generated automatically by the security appliance and is not verifiable by any external entity. The issuer and subject of the self-signed certificate are set to the IP address of the security appliance. It should be used only in testing or very small deployments. You can install the self-signed certificate into the certificate store of the client computer using the manual import procedure. In this process, the client should compare the fingerprint of the obtained Cisco ASA adaptive security appliance certificate with the original fingerprint received out-of-band (OOB) from the security appliance administrator. The self-signed Cisco ASA security appliance certificates should be avoided in production environments.
- **Identity certificate that is issued by an external CA:** In this scenario, the Cisco ASA adaptive security appliance enrolls with an external certificate authority (CA) to obtain an identity certificate that can be verified by the clients. The clients can verify the server identity certificate, because they have a list of trusted CA root certificates in their browsers. If the security appliance enrolls with a CA from that preinstalled certificate list, the client uses the appropriate root certificate to authenticate the SSL VPN server. This solution is recommended for unmanaged clients, including Internet kiosks.



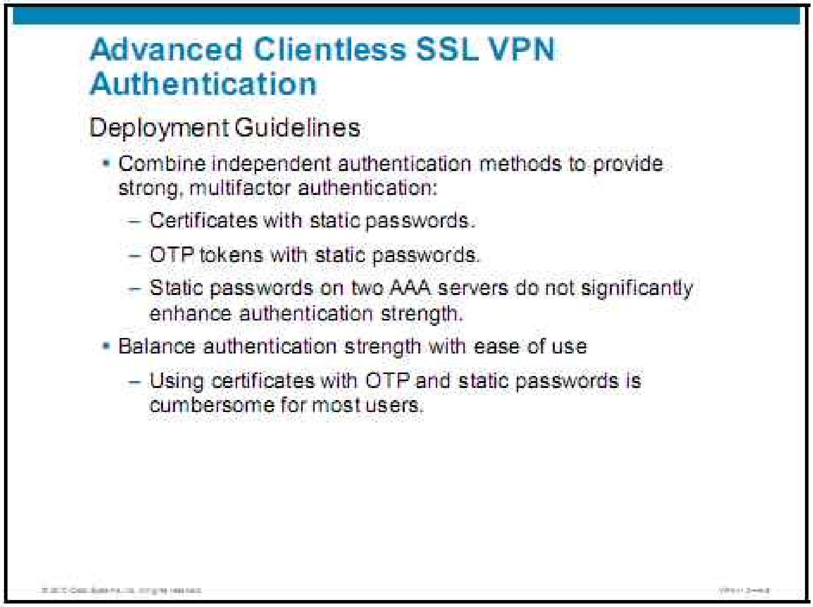
## Advanced Clientless SSL VPN Authentication

Client-Side Authentication Options

| Authentication | Use | Example |
|---|---|---|
| Certificates issued by internal CA of Cisco ASA | Managed client computers. Not intended for Internet kiosks. | Clients preprovisioned on Cisco ASA, and obtain their identity certificates at first sign-on. |
| Certificates issued by external CA | Feasible only in enterprise-wide environment. Clients need externally issued certificates. | Clients enroll with an enterprise-owned CA. |
| Password-based | Quick-to-deploy. Useful for unmanaged clients, such as Internet kiosks. | Local or external AAA database. |
| Multiple sequential authentications | Strong authentication, based on something you have (certificate) and something you know (password). | Certificates issues by Cisco ASA + passwords (managed clients)<br>RSA OTP tokens + passwords (unmanaged clients). |

Client-side authentication of a clientless SSL VPN session can be based on authentication methods:

- **Certificates that are issued by internal CA of Cisco ASA adaptive security appliance:** These certificates are installed on the client computer at the first client connection to the SSL VPN server. This approach is recommended for managed clients only.
- **Certificates that are issued by external CA:** In this deployment mode, the VPN users enroll with the same external CA as the SSL VPN server. The SSL VPN server has an identity certificate that is issued by the same external CA. The SSL VPN server authenticates client certificates using the root certificate. The SSL VPN server must be in possession of the root certificate before its own enrollment. This approach is typically deployed in enterprise-wide environments, where the enterprise maintains its own CA. Otherwise, the cost of user certificates may be an issue.
- **Passwords:** Passwords can be stored either in the local user database or on an external AAA server. They can be static in nature, or dynamic, as in the case of OTPs. Password-based authentication is recommended for users accessing the SSL VPN from unmanaged computers, such as public kiosks. The level of trust that is placed on the password-based authentication can be increased by implementing two-factor authentication, which relies on something you know (password) and something you have (OTP token).
- **Multiple sequential authentications:** In this method, the authentication strength is enhanced by combining two or more independent authentications, which must jointly succeed before a user can access the VPN. The authentications can either be performed against separate databases or be a combination of certificate and authentication, authorization, and accounting (AAA) authentications. Double authentication using different user databases with static passwords is not very common, as it can be argued that static password authentication is not significantly strengthened by another static password.



## Advanced Clientless SSL VPN Authentication

Deployment Guidelines

- Combine independent authentication methods to provide strong, multifactor authentication:
  - Certificates with static passwords.
  - OTP tokens with static passwords.
  - Static passwords on two AAA servers do not significantly enhance authentication strength.
- Balance authentication strength with ease of use
  - Using certificates with OTP and static passwords is cumbersome for most users.

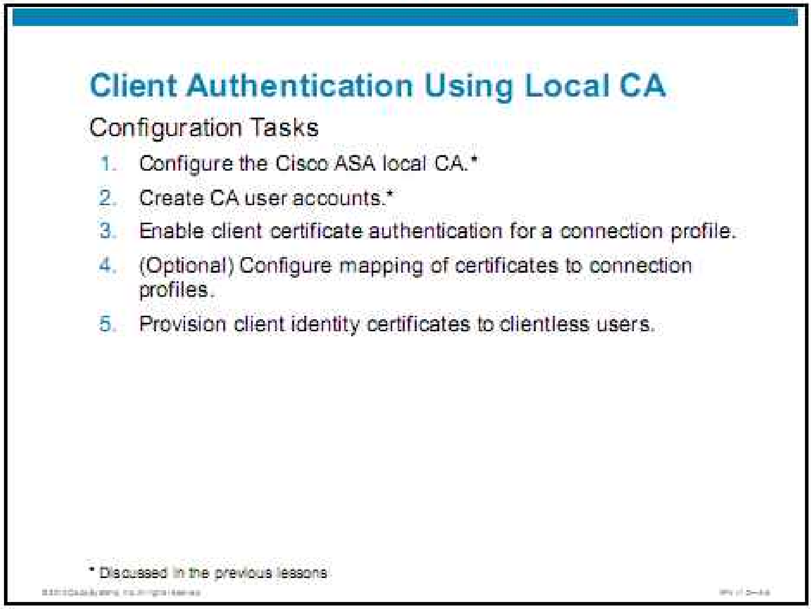
The security appliance offers a wide set of authentication options, but only some combinations of the authentication methods significantly increase the level of trust that is put in the authentication process. These combinations are the most recommended combinations:

- **Certificates with static passwords for managed client computers:** This option is not feasible for Internet kiosks.
- **OTP tokens with static passwords for managed or unmanaged endpoints:** This method can be implemented either as a single authentication using an AAA server that offloads authentication to a back-end OTP server, or as two daisy-chained authentications, one against a static database, and one against an OTP server.

In general, you should make the system as user-friendly as possible, if the security policy is obeyed. Combining too many authentications and requiring the users to enter too many passwords may place a heavy burden on their shoulders.

# Deploying Client Certificate-Based Authentication

This topic describes how to deploy client-side certificate-based authentication.



## Client Authentication Using Local CA

Configuration Tasks

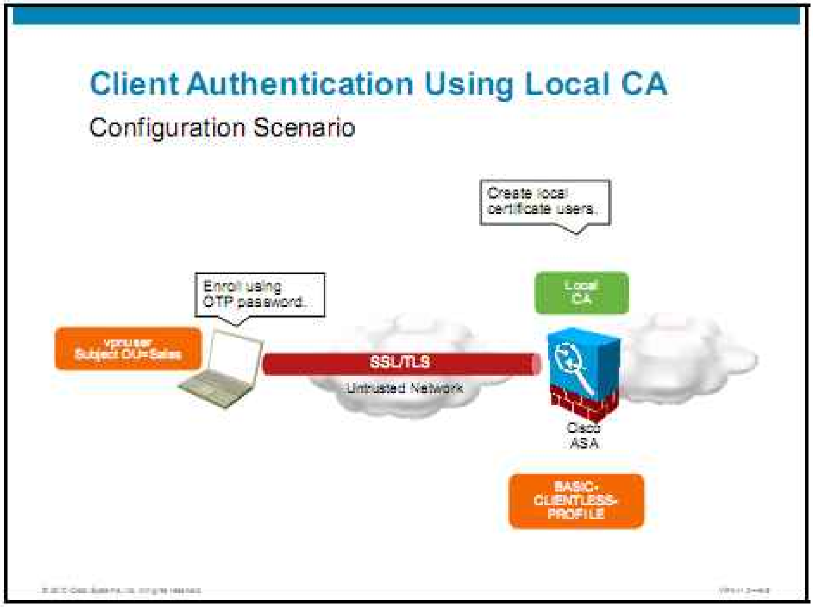
1. Configure the Cisco ASA local CA.*
2. Create CA user accounts.*
3. Enable client certificate authentication for a connection profile.
4. (Optional) Configure mapping of certificates to connection profiles.
5. Provision client identity certificates to clientless users.

* Discussed in the previous lessons

To configure client authentication using the local CA, you will perform the following configuration tasks:

1. Configure the Cisco ASA adaptive security appliance local CA (discussed in previous lessons and not discussed here again).
2. Create CA user accounts (discussed in previous lessons and not discussed here again).
3. Enable client certificate authentication for a connection profile.
4. Optionally, configure mapping of certificates to connection profiles.
5. Provision client identity certificates to clientless users.

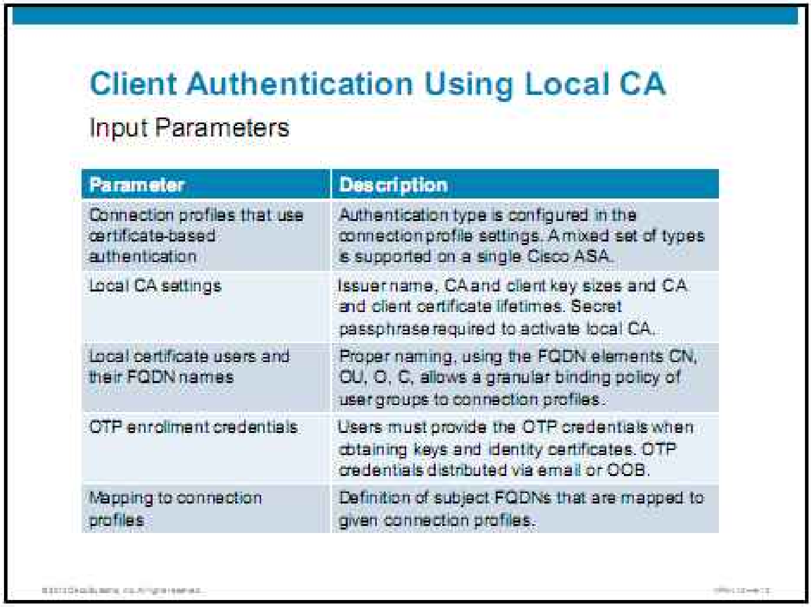
These tasks are described in the next pages.



## Client Authentication Using Local CA

Configuration Scenario

This figure presents the configuration scenario that is used in upcoming configuration tasks. You will enable the local CA function on the security appliance and create CA user accounts. The fully qualified domain names (FQDNs) of the users will include the organizational unit to which they belong. When the users connect to the SSL VPN, the Cisco ASA adaptive security appliance will check the organizational unit information to apply the correct connection profile to the user session, BASIC-CLIENTLESS-PROFILE in the example.



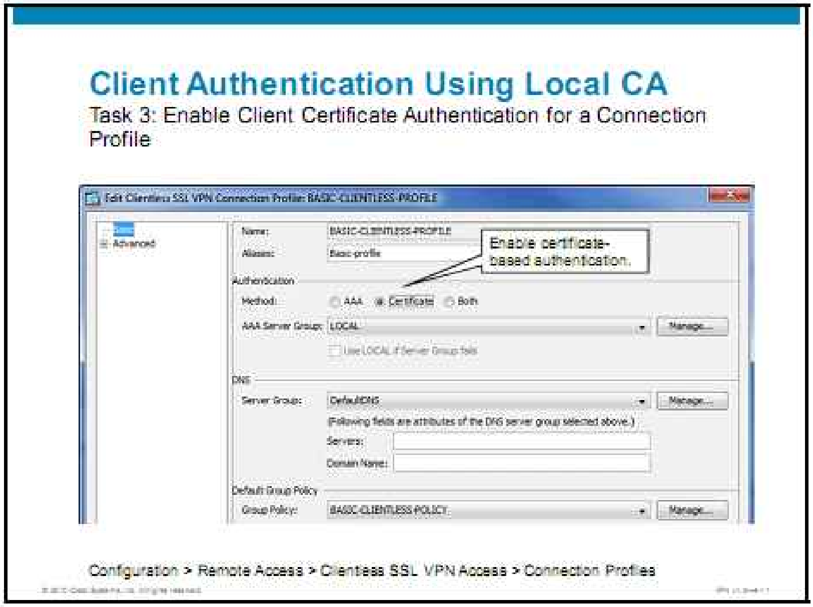
## Client Authentication Using Local CA

Input Parameters

| Parameter | Description |
|---|---|
| Connection profiles that use certificate-based authentication | Authentication type is configured in the connection profile settings. A mixed set of types is supported on a single Cisco ASA. |
| Local CA settings | Issuer name, CA and client key sizes and CA and client certificate lifetimes. Secret passphrase required to activate local CA. |
| Local certificate users and their FQDN names | Proper naming, using the FQDN elements CN, OU, O, C, allows a granular binding policy of user groups to connection profiles. |
| OTP enrollment credentials | Users must provide the OTP credentials when obtaining keys and identity certificates. OTP credentials distributed via email or OOB. |
| Mapping to connection profiles | Definition of subject FQDNs that are mapped to given connection profiles. |

You have to gather these input parameters prior implementing certificate-based client authentication using the local CA:

- **Connection profiles that use certificate-based authentication:** The authentication type is configured in the connection profile settings. To authenticate users using local CA certificates, the appropriate connection profiles must be configured for certificate-based authentication.
- **Local CA settings:** These parameters include the issuer name, key sizes of the CA and the clients, and CA and client certificate lifetimes. The key size of the client defines the length of the private- and public-key pair that the appliance generates for each client. All these parameters have default values that can be used for most environments. Only the secret passphrase must be explicitly entered to activate the local CA feature.
- **Local certificate users and their FQDN names:** The FQDN elements, such as common name (CN), organizational unit (OU), organization name (O), and country (C), allow a granular policy of binding user groups to connection profiles. An example of such a policy could match the country of the SSL VPN user (C attribute) and assign a connection profile that uses a localized customization.
- **OTP enrollment credentials:** OTP enrollment credentials must be generated by the security appliance local CA and distributed to the users before they can connect to the SSL VPN. These credentials must be distributed OOB, for example by emailing them to the users.
- **Mapping to connection profiles:** If you want to assign users to connection profiles based on their FQDN attributes, you must gather the mapping criteria that will define the binding.



## Client Authentication Using Local CA

Task 3: Enable Client Certificate Authentication for a Connection Profile

Edit Clientless SSL VPN Connection Profile: BASIC-CLIENTLESS-PROFILE

Name: BASIC-CLIENTLESS-PROFILE

Aliases: Basic-profile

Authentication

Method: ○ AAA ● Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS

(Following fields are attributes of the DNS server group selected above.)

Servers:

Domain Name:

Default Group Policy

Group Policy: BASIC-CLIENTLESS-POLICY

Enable certificate-based authentication.

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

The configuration procedure starts with the enabling of the local CA and creating CA user accounts, but these tasks are omitted here because they have been explained sufficiently in an earlier lesson. The first two tasks are identical to Cisco AnyConnect client authentication scenarios.

In the third configuration task, you will enable certificate-based authentication in the required connection profiles. To enable certificate-based authentication, complete the following steps:

**Step 1** Choose **Configuration > Remote Access > Clientless SSL VPN Access > Connection Profiles.**

**Step 2** Choose a desired connection profile and click the **Edit** button.

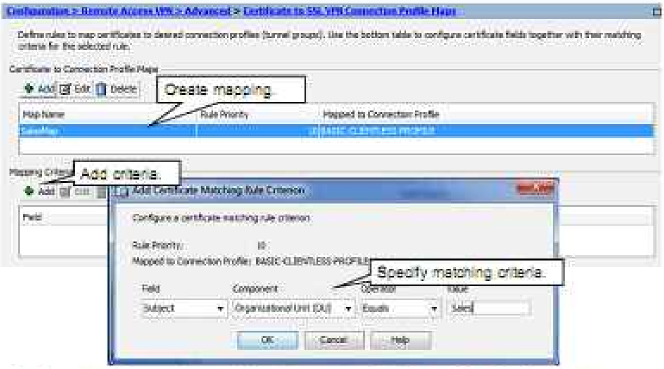
**Step 3** In the Authentication area of the window, click the **Certificate** radio button as the authentication method.

**Step 4** Click **OK**.

**Step 5** Click **Apply** to apply the configuration.

## Client Authentication Using Local CA

Task 4: (Optional) Configure Mapping of Certificates to Connection Profiles



Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps

Define rules to map certificates to desired connection profiles (tunnel groups). Use the bottom table to configure certificate fields together with their matching criteria for the selected rule.

Certificate to Connection Profile Maps

| Map Name | Rule Priority | Mapped to Connection Profile |
|---|---|---|
| SalesMap | 10 | BASIC-CLIENTLESS-PROFILE |

Add Certificate Matching Rule Criterion

Configure a certificate matching rule criterion.

Rule Priority: 10

Mapped to Connection Profile: BASIC-CLIENTLESS-PROFILE

| Field | Component | Operator | Value |
|---|---|---|---|
| Subject | Organizational Unit (OU) | Equals | Sales |

Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps

In the optional fourth task, you can define the mapping of client certificates to the appropriate connection profiles by completing these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps**.

**Step 2** Click **Add** to create a new map. A new window opens (not shown in the figure).

**Step 3** In the Certificate to Connection Profile Map configuration window, enter the map name and the rule priority and select the connection profile that is used for the binding. The rule priority defines the order in which multiple maps are evaluated when searching for a connection profile that will be used for a user session. This step is not shown in the example.

**Step 4** Select a map from the list of entries in the Certificate to Connection Profile Maps area and click **Add** in the Mapping Criteria area. The Add Certificate Matching Rule Criterion window opens.

**Step 5** Define your matching criteria by choosing appropriate parameters from the Field, Component, and Operator drop-down lists and entering the required value in the Value field. If the map consists of multiple matching rules, all conditions must be met to bind the user certificate to the connection profile (the rules are combined using the logical AND operator).

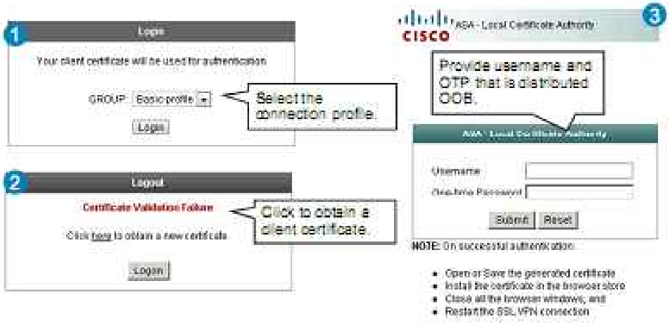
**Step 6** Click **OK**.

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

You may have multiple Certificate to Connection Profile Maps, each containing several matching rules. In this scenario, one map is defined: Salesmap. The salesmap consists of one rule that matches certificates where the organizational unit (OU) attribute in the subject field is set to “Sales” and maps them to connection profile BASIC-CLIENTLESS-PROFILE.

## Client Authentication Using Local CA

Task 5: Provision Client Identity Certificates to Clientless Users



1

Login

Your client certificate will be used for authentication.

GROUP: Basic profile

Login

Select the connection profile.

2

Logout

Certificate Validation Failure

Click here to obtain a new certificate.

Logon

Click to obtain a client certificate.

3

ASA - Local Certificate Authority

Provide username and OTP that is distributed OOB.

ASA - Local Certificate Authority

Username

One-time Password

Submit Reset

NOTE: On successful authentication:

- Open or Save the generated certificate
- Install the certificate in the browser store
- Close all the browser windows, and
- Restart the SSL VPN connection

In the fifth task, the users have to obtain the private- and public-key pair, and their identity certificate from the security appliance. The enrollment occurs in several steps:

1. The Cisco ASA adaptive security appliance points the users to a connection profile or the users select a connection profile that is configured for certificate-based authentication.

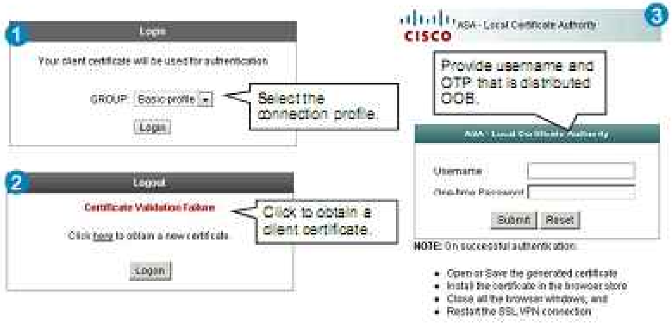
2. The users receive an authentication failure notification and a link for obtaining a new certificate and the keys.

3. After choosing the link, the security appliance prompts users to submit their username and OTP, which they should have already obtained using an OOB method.

4. When the username and OTP combination is correct, the security appliance sends the user a Personal Information Exchange (or Public Key Cryptography Standard #12 [PKCS #12]) file that the user can open or save. The file has the username as its name and extension .p12 and contains the private- and public-key pair and user identity certificate.

## Client Authentication Using Local CA

Task 5: Provision Client Identity Certificates to Clientless Users


1
Login
2
Logout
3
CISCO
ASA - Local Certificate Authority
ASA - Local Certificate Authority
Login
Logon
Submit
Reset

Your client certificate will be used for authentication

GROUP: Basic profile

Select the connection profile.

Certificate Validation Failure

Click here to obtain a new certificate

Click to obtain a client certificate.

Provide username and OTP that is distributed OOB.

Username

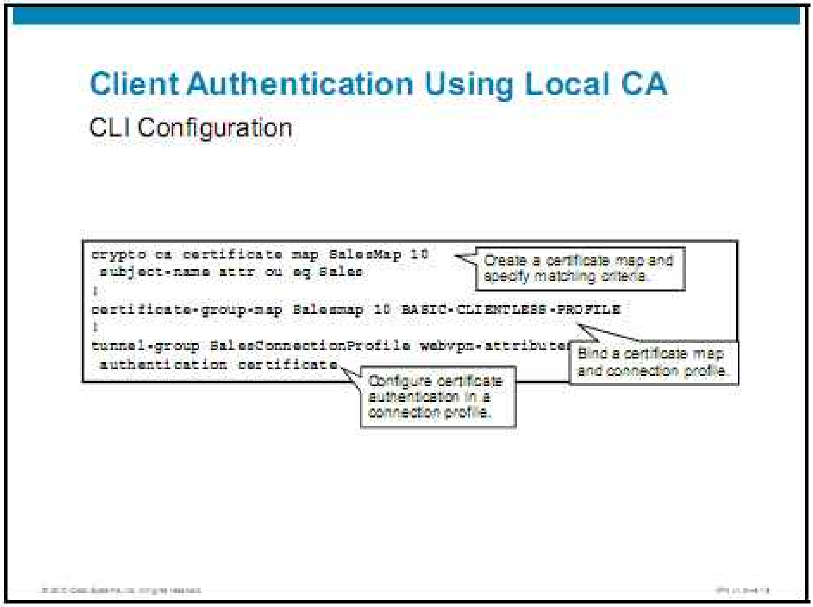
One-time Password

NOTE: On successful authentication:

- Open or Save the generated certificate
- Install the certificate in the browser store
- Close all the browser windows, and
- Restart the SSL VPN connection

In the fifth task, the users have to obtain the private- and public-key pair, and their identity certificate from the security appliance. The enrollment occurs in several steps:

1. The Cisco ASA adaptive security appliance points the users to a connection profile or the users select a connection profile that is configured for certificate-based authentication.
2. The users receive an authentication failure notification and a link for obtaining a new certificate and the keys.
3. After choosing the link, the security appliance prompts users to submit their username and OTP, which they should have already obtained using an OOB method.
4. When the username and OTP combination is correct, the security appliance sends the user a Personal Information Exchange (or Public Key Cryptography Standard #12 [PKCS #12]) file that the user can open or save. The file has the username as its name and extension .p12 and contains the private- and public-key pair and user identity certificate.



## Client Authentication Using Local CA

CLI Configuration

```
crypto ca certificate map SalesMap 10
 subject-name attr ou eq Sales
!
certificate-group-map Salesmap 10 BASIC-CLIENTLESS-PROFILE
!
tunnel-group SalesConnectionProfile webvpn-attribute
 authentication certificate
```

Create a certificate map and specify matching criteria.

Bind a certificate map and connection profile.

Configure certificate authentication in a connection profile.

The figure shows the CLI command that is used to enable client authentication using the local CA. Local CA configuration and local CA user creation are not shown in the figure, because it has been already discussed in the "Deploying Advanced Authentication in AnyConnect Full Tunnel SSL VPNs" lesson.

To create a certificate-to-connection profile mapping using the CLI, use the following commands. First, create a certificate-to-connection profile map using the **crypto ca certificate map** command, followed by a name and rule priority number. Then use the **subject-name atrr** 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. In the example, if the Cisco ASA adaptive security appliance receives a certificate where the organization unit (OU) field of a subject name contains "Sales," the security appliance will use the BASIC-CONNECTION-PROFILE connection profile for that user.

Finally, enable certificates-based authentication for a specific connection profile (tunnel group) using the **authentication certificate** command in tunnel-group configuration mode.

### crypto ca certificate map

To enter CA certificate map mode, use the **crypto ca certificate map** command in global configuration mode. Executing this command places you in CA certificate map mode. Use this group of commands to maintain a prioritized list of certificate mapping rules. The sequence number orders the mapping rules. To remove a crypto CA certificate map rule, use the **no** form of the command.

**crypto ca certificate map** {*sequence-number* | *map-name sequence-number*}

### crypto ca certificate map Parameters

| Parameter | Description |
|---|---|
| *map-name* | Specifies a name for a certificate-to-group map. |
| *sequence-number* | Specifies a number for the certificate map rule you are creating. The range is 1 through 65535. You can use this number when creating a tunnel-group-map, which maps a tunnel group to a certificate map rule. |

## subject-name (crypto ca certificate map)

To indicate that rule entry is applied to the subject distinguished name (DN) of the IPsec peer certificate, use the **subject-name** command in crypto CA certificate map configuration mode. To remove a subject-name, use the **no** form of the command.

**subject-name** [**attr** *tag* **eq** | **ne** | **co** | **nc** *string*]

### subject-name (crypto ca certificate map) Parameters

| Parameter | Description |
|---|---|
| **attr** *tag* | Indicates that only the specified attribute value from the certificate DN will be compared to the rule entry string. The tag values are as follows:<br>■ DNQ = DN qualifier<br>■ GENQ = Generational qualifier<br>■ I = Initials<br>■ GN = Given name<br>■ N = Name<br>■ SN = Surname<br>■ IP = IP address<br>■ SER = Serial number<br>■ UNAME = Unstructured name<br>■ EA = Email address<br>■ T = Title<br>■ O = Organization name<br>■ L = Locality<br>■ SP = State and province<br>■ C = Country<br>■ OU = Organizational unit<br>■ CN = Common name |
| **co** | Specifies that the rule entry string must be a substring in the DN string or indicated attribute. |
| **eq** | Specifies that the DN string or indicated attribute must match the entire rule string. |
| **nc** | Specifies that the rule entry string must not be a substring in the DN string or indicated attribute. |
| **ne** | Specifies that the DN string or indicated attribute must not match the entire rule string. |
| *string* | Specifies the value to be matched. |

## certificate-group-map

To associate a rule entry from a certificate map with a tunnel group, use the **certificate-group-map** command in webvpn configuration mode. To clear current tunnel-group map associations, use the **no** form of this command.

**certificate-group-map** *certificate_map_name index tunnel_group_name*

### certificate-group-map Parameters

| Parameter | Description |
|---|---|
| *`certificate_map_name`* | The name of a certificate map. |
| *`index`* | The numeric identifier for a map entry in the certificate map. The index value can be in a range of 1–65,535. |
| *`tunnel_group_name`* | The name of the tunnel group that is chosen if the map entry matches the certificate. The tunnel-group name must already exist. |

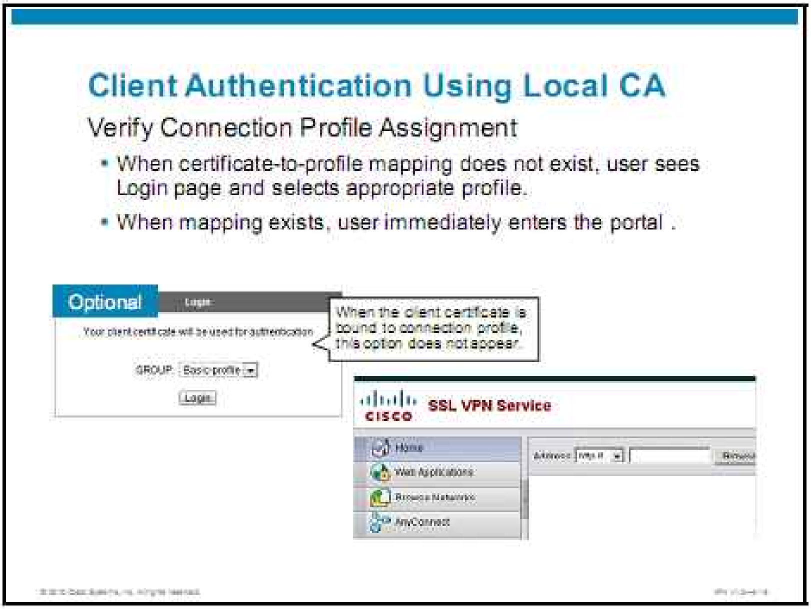
## authentication-certificate

To request a certificate from a WebVPN client that is establishing a connection, use the **authentication-certificate** command in webvpn configuration mode. To cancel the requirement for a client certificate, use the **no** form of this command.

**authentication-certificate** *interface-name*

### authentication-certificate Parameters

| Parameter | Description |
|---|---|
| *`interface-name`* | The name of the interface that is used to establish the connection. Available interfaces names are:<br>■ **inside:** Name of interface GigabitEthernet 0/1<br>■ **outside:** Name of interface GigabitEthernet 0/0 |



Client Authentication Using Local CA

Verify Connection Profile Assignment

- When certificate-to-profile mapping does not exist, user sees Login page and selects appropriate profile.
- When mapping exists, user immediately enters the portal .

Optional

Your client certificate will be used for authentication

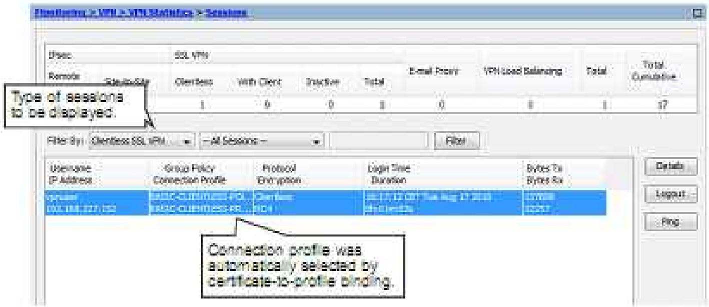
GROUP: Basic profile

When the client certificate is bound to connection profile, this option does not appear.

To verify the certificate-based client authentication, you will connect to the SSL VPN. If the security appliance has a Certificate to Connection Profile Map that binds the user certificate to a connection profile, the specified connection profile will be chosen automatically. If the maps do not match, the users may have the option to select a connection profile, as shown in the left half of the figure. This figure depicts a successful certificate-based authentication in which the user is not prompted for any credentials, as shown in the right half of the figure.

## Client Authentication Using Local CA

Verify Connection Profile Assignment (Cont.)



Monitoring > VPN > VPN Statistics > Sessions

| IPsec |  | SSL VPN |  |  |  | E-mail Proxy | VPN Load Balancing | Total | Total Cumulative |
|---|---|---|---|---|---|---|---|---|---|
| Remote | Site-to-Site | Clientless | With Client | Inactive | Total |  |  |  |  |
|  |  | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 17 |

Filter By: Clientless SSL VPN | -- All Sessions -- | Filter

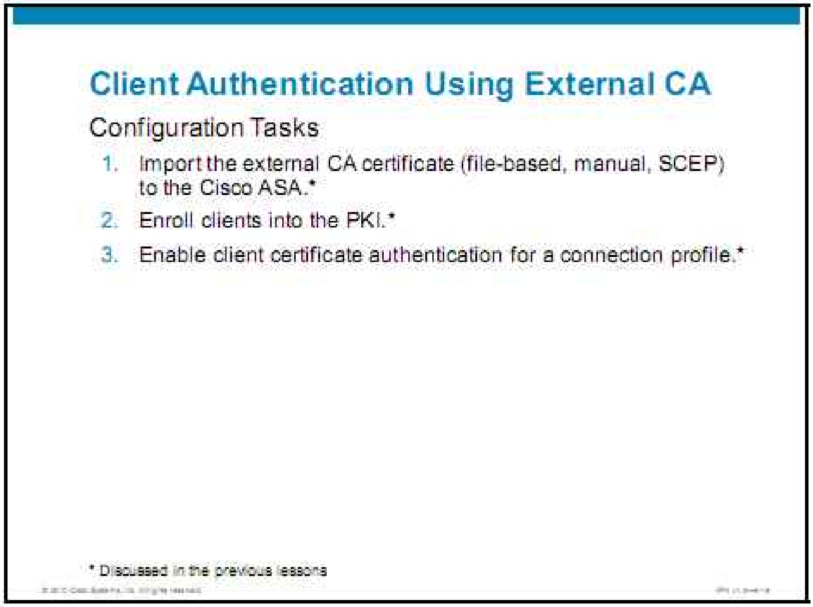
| Username<br>IP Address | Group Policy<br>Connection Profile | Protocol<br>Encryption | Login Time<br>Duration | Bytes Tx<br>Bytes Rx |
|---|---|---|---|---|
| vpnuser<br>192.168.227.132 | BASIC-CLIENTLESS-POL...<br>BASIC-CLIENTLESS-PR... | Clientless<br>RC4 | 18:17:12 CDT Tue Aug 17 2010<br>0h:01m:03s | 107838<br>32257 |

Type of sessions to be displayed.

Connection profile was automatically selected by certificate-to-profile binding.

Monitoring > VPN > VPN Statistics > Sessions

To view the user sessions parameters, including the selected connection profile, you may choose **Monitoring > VPN > VPN Statistics > Sessions**, and select **Clientless SSL VPN** from the Filter By drop-down menu to view the session parameters. This verification will show if the correct profile has been activated by the Certificate to Connection Profile Map.



## Client Authentication Using External CA

Configuration Tasks

1. Import the external CA certificate (file-based, manual, SCEP) to the Cisco ASA.*
2. Enroll clients into the PKI.*
3. Enable client certificate authentication for a connection profile.*

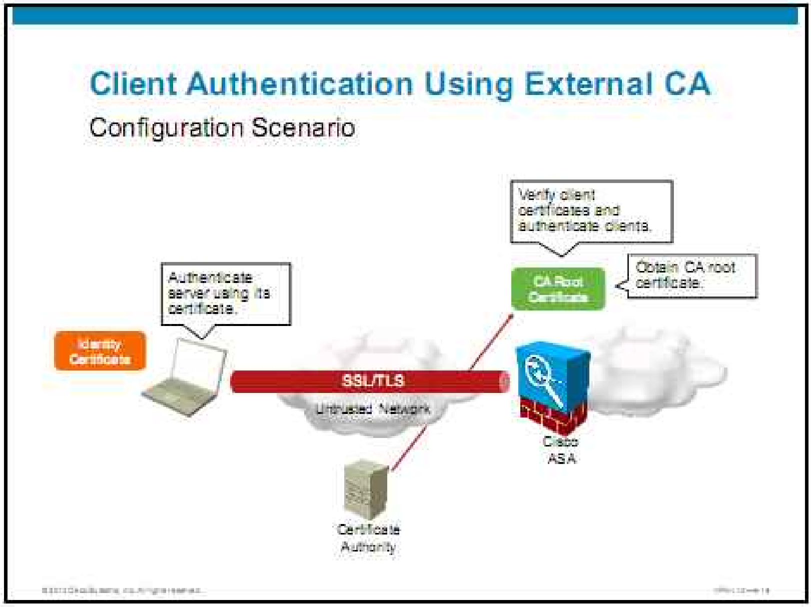
* Discussed in the previous lessons

To configure client authentication using an external CA, you will perform the following tasks:

1. Import the external CA root certificate to the security appliance. The CA root certificate can be installed using file import, manual (cut-and-paste), or Simple Certificate Enrollment Protocol (SCEP).

2. Enroll clients into the PKI.

3. Enable client certificate authentication for a connection profile.



## Client Authentication Using External CA

Configuration Scenario

Verify client certificates and authenticate clients.
Obtain CA root certificate.
CA Root Certificate
Authenticate server using its certificate.
Identity Certificate
SSL/TLS
Untrusted Network
Cisco ASA
Certificate Authority

This figure illustrates the configuration scenario for deploying browser (client) certificates using an external CA.

The security appliance receives the root certificate of the external CA and enrolls with it to obtain its identity certificate.

The users may have the root certificate preinstalled in their browsers, depending on which CA provider is selected in a particular enterprise environment. Alternatively, the enterprise may manage its own CA. In either case, the users must enroll with the CA to obtain their identity certificates.

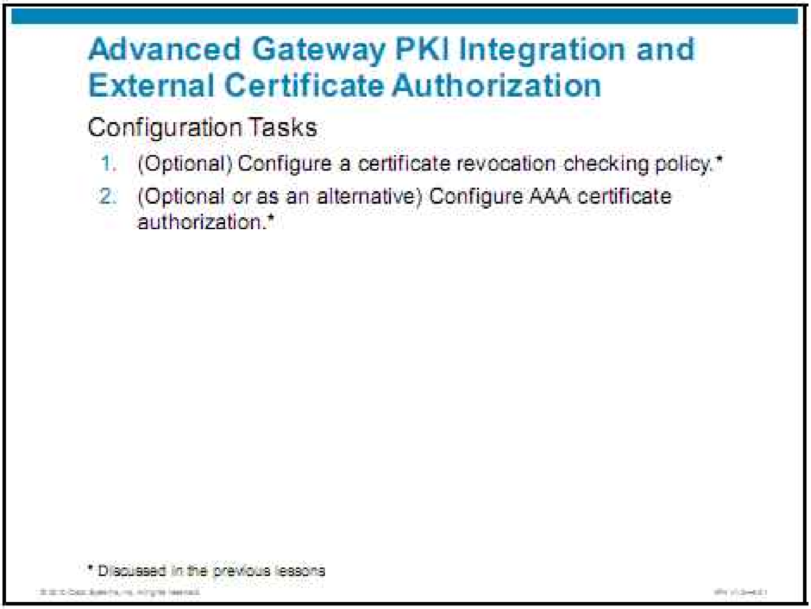
Both server authentication and client authentication are certificate-based. The entities use the self-signed root certificate to verify the authenticity of the peer certificate. Once the peer certificate is validated, the entities extract the embedded public key to verify the peer signature.

You have to gather some input data before deploying browser (client) certificates using an external CA. The parameters belong to three areas:

- **Data for external CA enrollment procedure:** Enrollment procedure varies based on the CA provider. The enterprise may choose to install and manage its own CA. CA root certificate can be imported to the Cisco ASA adaptive security appliance using a file import, a cut-and-paste process, or SCEP.
- **Client authentication policy:** Optionally, you may combine certificate-based client authentication with AAA that uses passwords to authenticate the users.
- **Mapping to connection profiles:** Optionally, use the definition of FQDNs mapped to given connection profiles. This method is required only if client-side authentication is certificate-based and users should be directed to various connection profiles based on their X.500 subject names.

# Deploying Advanced Gateway PKI Integration, External Certificate Authorization, and Double Authentication

This topic describes how to integrate the SSL VPN server in a PKI environment, deploy external certificate authorization, and implement double authentication.



## Advanced Gateway PKI Integration and External Certificate Authorization

Configuration Tasks

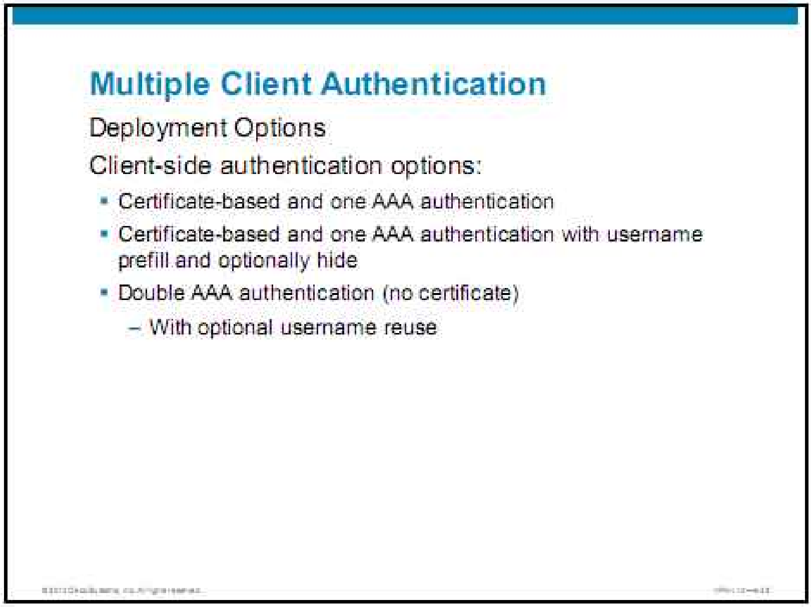
1. (Optional) Configure a certificate revocation checking policy.*
2. (Optional or as an alternative) Configure AAA certificate authorization.*

* Discussed in the previous lessons

To configure client authentication using an external CA, you will perform the following tasks:

1. Optionally, configure a certificate revocation checking policy.
2. Optionally, or as an alternative, configure AAA certificate authorization.

These steps are the same as for full tunneling SSL VPNs and are not repeated here.



## Multiple Client Authentication

Deployment Options

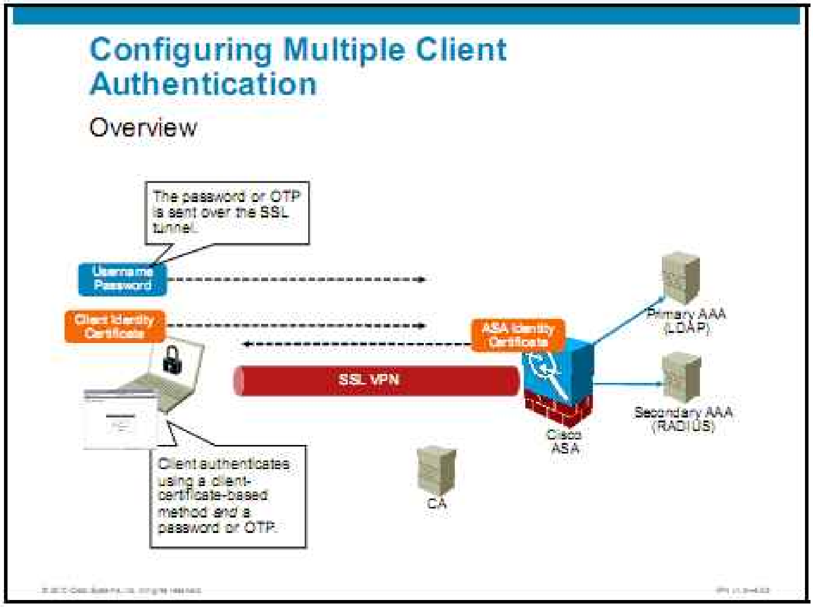
Client-side authentication options:

- Certificate-based and one AAA authentication
- Certificate-based and one AAA authentication with username prefill and optionally hide
- Double AAA authentication (no certificate)
  - With optional username reuse

You can deploy one of several multiple authentication combinations. The multiple client-side authentication options in clientless SSL VPN are identical to the ones in Cisco AnyConnect VPN Clients and include these:

- Certificate-based and one AAA authentication
- Certificate-based and one AAA authentication where username for AAA authentication can be extracted from certificate subject field and hidden from users
- Double AAA authentication (no certificate) with optional username reuse

This topic presents how to configure multiple client authentications for clientless SSL VPN connections.



## Configuring Multiple Client Authentication

Overview

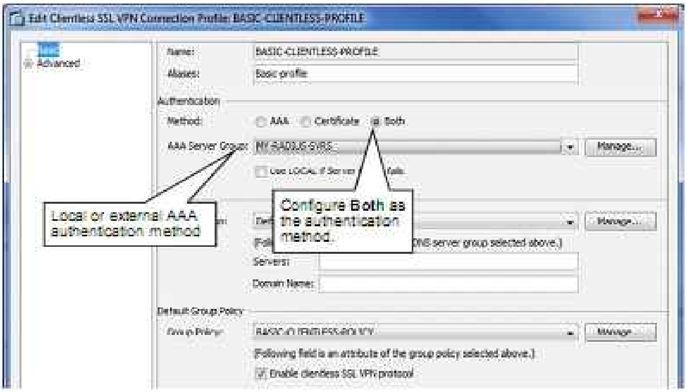
The password or OTP is sent over the SSL tunnel.

Client authenticates using a client-certificate-based method and a password or OTP.

This figure presents the configuration scenario that is used in upcoming configuration tasks. First, you will configure certificate-based authentication with a single AAA password-based authentication using the RADIUS server. Then you will configure double authentication, where primary authentication will be performed on the LDAP server and secondary on the RADIUS server.

## Certificate-Based and AAA Authentication

### Certificate and One AAA Authentication



Edit Clientless SSL VPN Connection Profile: BASIC-CLIENTLESS-PROFILE

- Basic
- Advanced

Name: BASIC-CLIENTLESS-PROFILE

Aliases: Basic profile

Authentication

Method: ○ AAA ○ Certificate ● Both

AAA Server Group: MY-RADIUS-SVRS

☐ Use LOCAL if Server ... fails

(Following field is an attribute of the DNS server group selected above.)

Servers:

Domain Name:

Default Group Policy

Group Policy: BASIC-CLIENTLESS-POLICY

(Following field is an attribute of the group policy selected above.)

☑ Enable clientless SSL VPN protocol

Local or external AAA authentication method

Configure **Both** as the authentication method.

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

You will configure the respective connection profiles for both authentication types. Complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

**Step 2** Select the desired connection profile and click **Edit**.

**Step 3** Click the **Both** radio button in the Authentication section of the window.

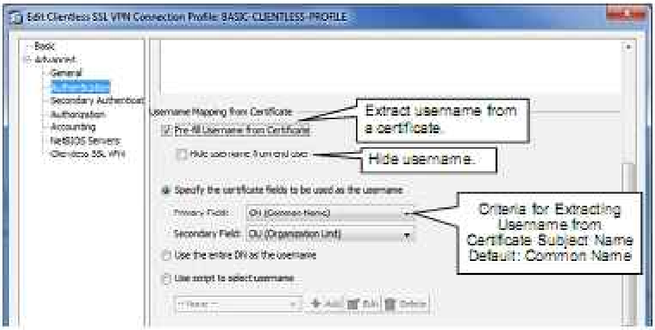
**Step 4** Select the appropriate primary AAA server group from the AAA Server Group drop-down menu. In this example, MY-RADIUS-SVRS server group will be used.

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

**Step 6** Click **Apply** to apply the configuration.

## Certificate-Based and AAA Authentication

Certificate and One AAA Authentication with Prefill



Edit Clientless SSL VPN Connection Profile: BASIC-CLIENTLESS-PROFILE

Username Mapping from Certificate

☑ Pre-fill Username from Certificate

□ Hide username from end user

● Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

○ Use the entire DN as the username

○ Use script to select username

-- None --

Extract username from a certificate.

Hide username.

Criteria for Extracting Username from Certificate Subject Name Default: Common Name

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

Next, you may configure the username prefill feature. Complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

**Step 2** Select the desired connection profile and click **Edit**.

**Step 3** Expand the **Advanced** option in the menu and choose **Authentication** in the submenu.

**Step 4** Check the **Pre-fill Username from Certificate** check box.

**Step 5** Optionally, you may hide the username from the end user by checking the Hide the Username from End User check box. This feature increases the security by not showing the username to users logging into SSL VPN.

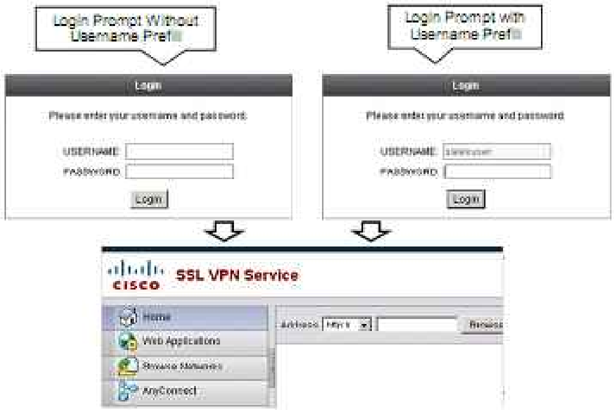
**Step 6** Optionally, modify the default method of extracting the username from the certificate. You may define the primary and secondary fields, choose to use the entire distinguished name (DN) embedded in the certificate, or define a custom script for selecting the username.

**Step 7** Click **OK**.

**Step 8** Click **Apply** to apply the configuration.

# Certificate-Based and AAA Authentication

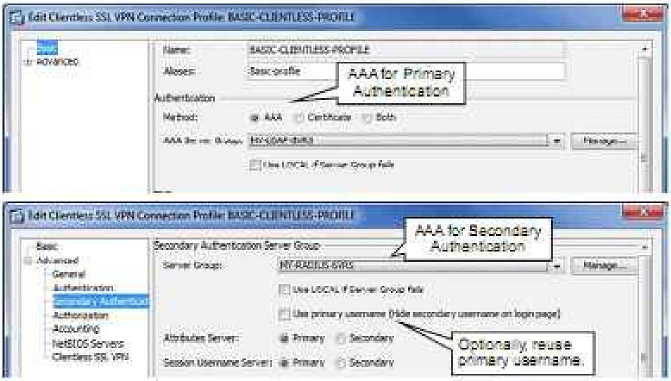
## Verification


Login Prompt Without Username Prefill
Login Prompt with Username Prefill
Login
Please enter your username and password.
USERNAME
PASSWORD
Login
Login
Please enter your username and password.
USERNAME
PASSWORD
Login
cisco
SSL VPN Service
Home
Web Applications
Browse Networks
AnyConnect
Address
Browse

To verify double authentication that uses certificates and a primary AAA method, you use a browser to connect to the SSL VPN. If you have a correct certificate installed in the certificate store, the browser submits it for certificate-based authentication. In the second step, the SSL VPN server requests user credentials. If the username prefill feature is enabled, the username field is filled in and grayed out. If the field is grayed out, the client cannot alter the username. After the user submits the correct static password, access to the SSL VPN portal is granted.

## Double AAA Authentication

Double AAA Authentication



Edit Clientless SSL VPN Connection Profile: BASIC-CLIENTLESS-PROFILE

Name: BASIC-CLIENTLESS-PROFILE

Aliases: Basic-profile

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: MY-LDAP-SVRS

□ Use LOCAL if Server Group fails

Edit Clientless SSL VPN Connection Profile: BASIC-CLIENTLESS-PROFILE

Secondary Authentication Server Group

Server Group: MY-RADIUS-SVRS

□ Use LOCAL if Server Group fails

□ Use primary username (Hide secondary username on login page)

Attributes Server: ● Primary ○ Secondary

Session Username Server: ● Primary ○ Secondary

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

To implement the double AAA scenario, you configure the respective connection profile for AAA authentication and configure the primary AAA server group. Complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

**Step 2** Select the desired connection profile and Click **Edit**.

**Step 3** To configure primary authentication, click the **AAA** radio button in the Authentication area of the window.

**Step 4** Select the appropriate primary server group from the AAA Server Group drop-down menu. In this example, the primary authentication will be offloaded to an external LDAP database.

**Step 5** To configure secondary authentication, expand the **Advanced** option from the menu on the left and choose the **Secondary Authentication** submenu.

**Step 6** Choose the appropriate secondary AAA group from the Server Group drop-down menu. In the example, the MY-RADIUS-SVRS server group is selected.

**Step 7** Optionally, enable fallback to local database by checking the **Use LOCAL if Server Group Fails** check box.

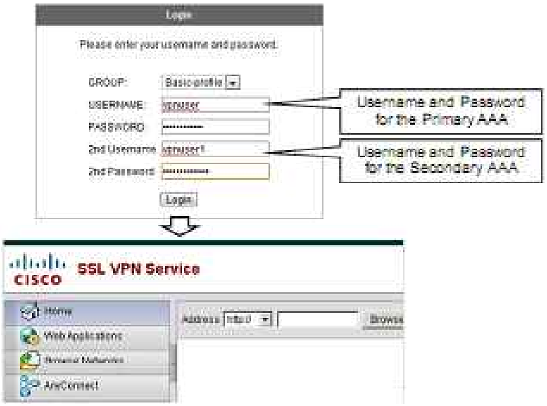
**Step 8** Optionally, reuse the username from the primary authentication by checking the **Use Primary Username (Hide Secondary Username on Logon Page)** check box.

**Step 9** Click **OK**.

**Step 10** Click **Apply** to apply the configuration.

## Double AAA Authentication

### Verification



Login

Please enter your username and password.

GROUP: Basic profile

USERNAME: vpnuser

PASSWORD: ••••••••••

2nd Username: vpnuser1

2nd Password: ••••••••••

Username and Password for the Primary AAA

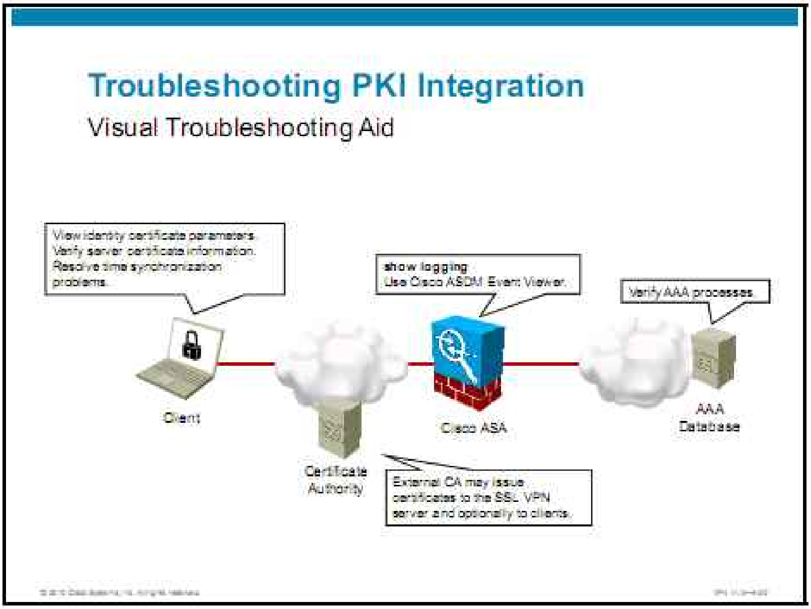
Username and Password for the Secondary AAA

To verify double AAA authentication, you use a browser to connect to the SSL VPN. Depending on the username reuse option for the secondary authentication, the login prompt that is associated with the appropriate connection profile may contain one or two username fields.

If you have a correct certificate installed in the certificate store, the browser will submit it for certificate-based authentication. In the second step, the SSL VPN server requests user credentials. If the username prefill feature is enabled, the username field will be filled in and grayed out. If the field is grayed out, the client cannot alter the username. After the user submits the correct static password, access to the portal is granted.

# Troubleshooting PKI Integration

This topic describes how to troubleshoot the integration of a clientless SSL VPN with PKI.



## Troubleshooting PKI Integration

Visual Troubleshooting Aid

View identity certificate parameters.
Verify server certificate information.
Resolve time synchronization problems.

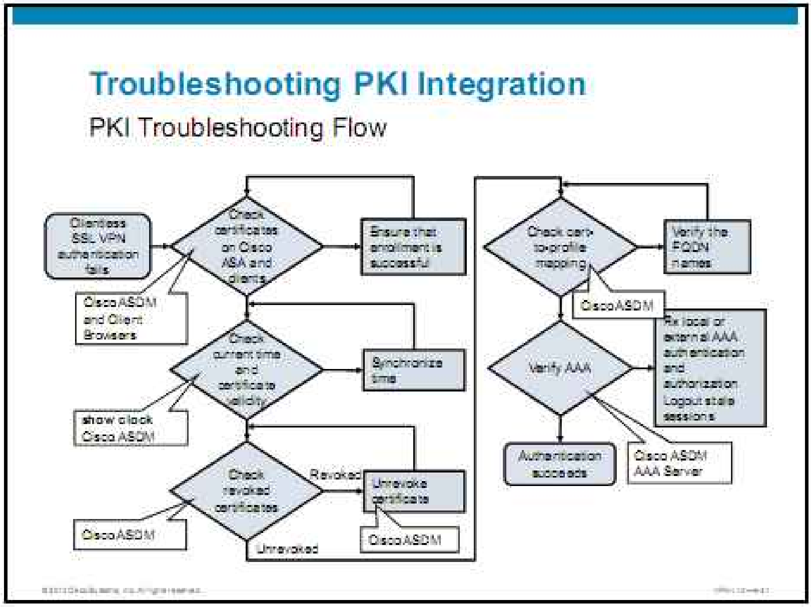
**show logging**
Use Cisco ASDM Event Viewer.

Verify AAA processes.

External CA may issue certificates to the SSL VPN server and optionally to clients.

PKI offers strong authentication capabilities but requires that you understand the principles of certificate operations. To integrate the SSL VPN system successfully with the PKI, you should know how to identify and resolve potential problems.

This figure presents a typical SSL VPN integration with PKI. The CA may issue certificates to the VPN server and optionally to users. The users obtain their identity certificates either from the local CA that is based on the Cisco ASA adaptive security appliance or from the external CA server. A number of verification and troubleshooting tools exist on the user computer, on the security appliance, and on the external servers (AAA, CA). This section focuses on the troubleshooting methods that are available on the security appliance.



## Troubleshooting PKI Integration

PKI Troubleshooting Flow

Clientless SSL VPN authentication fails
Check certificates on Cisco ASA and clients
Ensure that enrollment is successful
Cisco ASDM and Client Browsers
Check current time and certificate validity
Synchronize time
show clock
Cisco ASDM
Check revoked certificates
Revoked
Unrevoke certificate
Cisco ASDM
Cisco ASDM
Unrevoked
Check cert-to-profile mapping
Verify the FQDN names
Cisco ASDM
Verify AAA
Fix local or external AAA authentication and authorization. Logout stale sessions.
Authentication succeeds
Cisco ASDM
AAA Server

If the certificate-based clientless SSL VPN authentication fails, perform these troubleshooting steps:

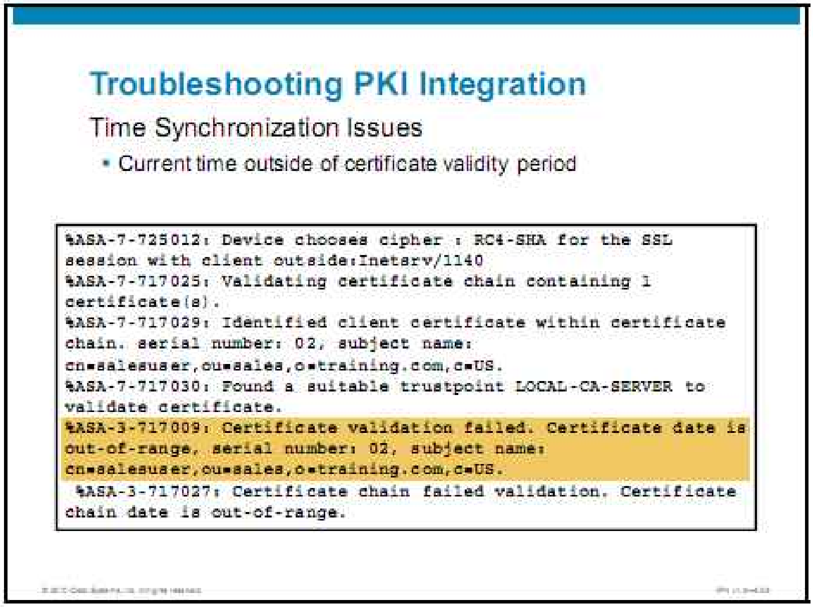
**Step 1** First, check the certificates that are installed on the client and on the security appliance. If the certificates are missing, ensure that the enrollment is completed.

**Step 2** Check the current time on the user computers and the security appliance. Although the time does not need to be synchronized, it must fall within the certificate validity range of the peer certificate. For example, if Cisco ASA adaptive security appliance identity certificate validity range is January 1, 2011 to January 1, 2012, and the current date on user computer is in 2010, the client will consider the Cisco ASA adaptive security appliance certificate invalid. The security appliance performs the same validity check for user certificates.

**Step 3** Check if certificates have been revoked. Revocation is supported for certificates that are issued by the Cisco ASA adaptive security appliance internal CA and external CA. The revoked Cisco ASA adaptive security appliance internal certificates can be viewed and unrevoked in the menu **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Certificates**.

**Step 4** Check certificate-to-profile mapping in the menu **Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps**. If the match criteria are missing or configured incorrectly, the binding feature will either fail or point to a wrong connection profile.

**Step 5** Verify AAA operations. This step should be performed if AAA-based authentication is attached to the certificate-based authentication or is configured as the stand-alone client authentication mechanism. Basic AAA connectivity should be verified on the security appliance. For advanced examination of activity logs, you should use appropriate tools on the AAA server.



## Troubleshooting PKI Integration

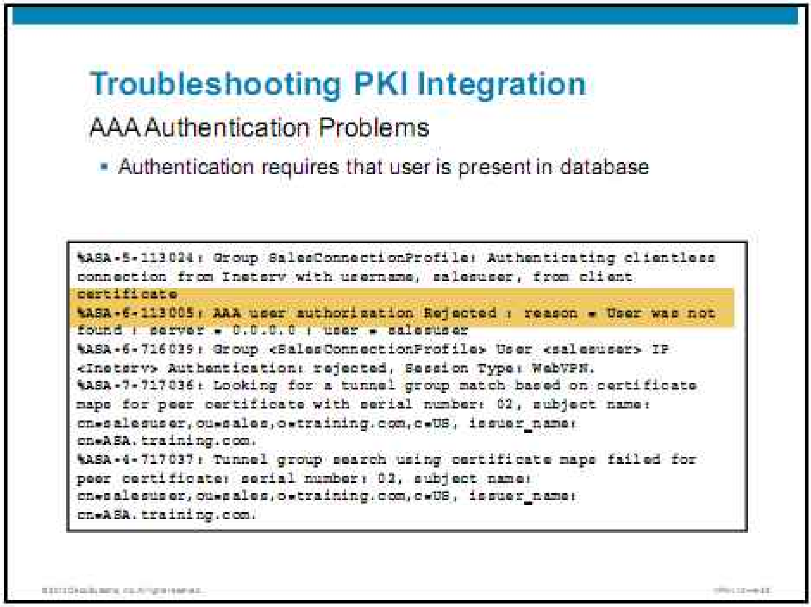
Time Synchronization Issues

- Current time outside of certificate validity period

```
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL
session with client outside:Inetsrv/1140
%ASA-7-717025: Validating certificate chain containing 1
certificate(s).
%ASA-7-717029: Identified client certificate within certificate
chain. serial number: 02, subject name:
cn=salesuser,ou=sales,o=training.com,c=US.
%ASA-7-717030: Found a suitable trustpoint LOCAL-CA-SERVER to
validate certificate.
%ASA-3-717009: Certificate validation failed. Certificate date is
out-of-range, serial number: 02, subject name:
cn=salesuser,ou=sales,o=training.com,c=US.
 %ASA-3-717027: Certificate chain failed validation. Certificate
chain date is out-of-range.
```

This figure illustrates the security appliance console output when the current time on the security appliance lies outside of the user certificate validity range. You must enable logging on the security appliance to view these messages. Instead of monitoring the operations via the console, you may use the real-time log viewer that is available in the Cisco Adaptive Security Device Manager (Cisco ASDM) menu **Monitoring > Logging > Real-Time Log Viewer**.

The relevant message in this output reports that the certificate validation failed due to an out-of-range condition.



## Troubleshooting PKI Integration

AAA Authentication Problems

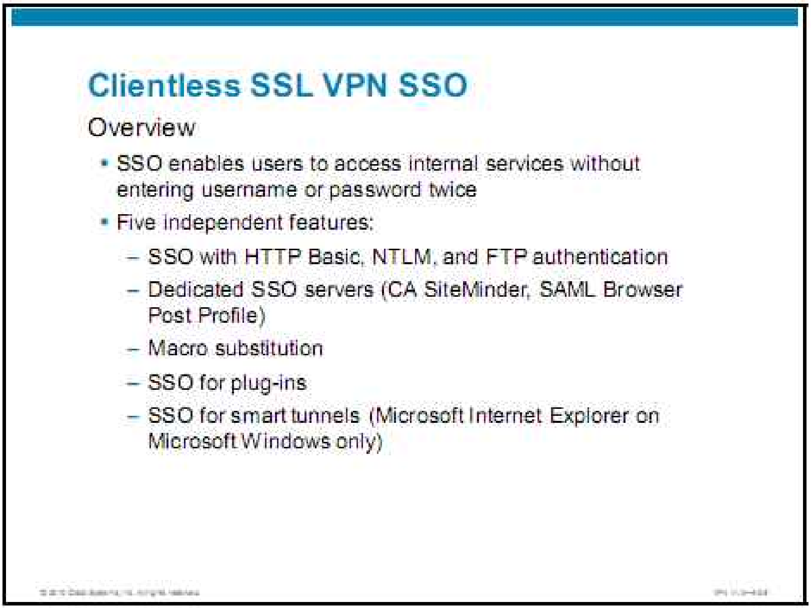
- Authentication requires that user is present in database

```
%ASA-5-113024: Group SalesConnectionProfile: Authenticating clientless
connection from Ineterv with username, salesuser, from client
certificate
%ASA-6-113005: AAA user authorization Rejected : reason = User was not
found : server = 0.0.0.0 : user = salesuser
%ASA-6-716039: Group <SalesConnectionProfile> User <salesuser> IP
<Ineterv> Authentication: rejected, Session Type: WebVPN.
%ASA-7-717036: Looking for a tunnel group match based on certificate
maps for peer certificate with serial number: 02, subject name:
cn=salesuser,ou=sales,o=training.com,c=US, issuer_name:
cn=ASA.training.com.
%ASA-4-717037: Tunnel group search using certificate maps failed for
peer certificate: serial number: 02, subject name:
cn=salesuser,ou=sales,o=training.com,c=US, issuer_name:
cn=ASA.training.com.
```

This figure illustrates the logging output that is generated as a result of an authorization failure. In this example, the security appliance is configured for a very rudimentary authorization—to authorize users who exist in the AAA database. The user authenticates using certificates. Even if the users exist in the local CA user database (**Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database**), they do not need to exist in the AAA user database. If they are not configured as AAA users, the authorization setting "Users must exist in the authorization database to connect" will cause the session to fail. You will see the message "AAA user authorization Rejected : reason = User was not found" as seen in the figure.

# Deploying Clientless SSL VPN SSO

This topic describes the single sign-on (SSO) feature of clientless SSL VPNs.



## Clientless SSL VPN SSO

Overview

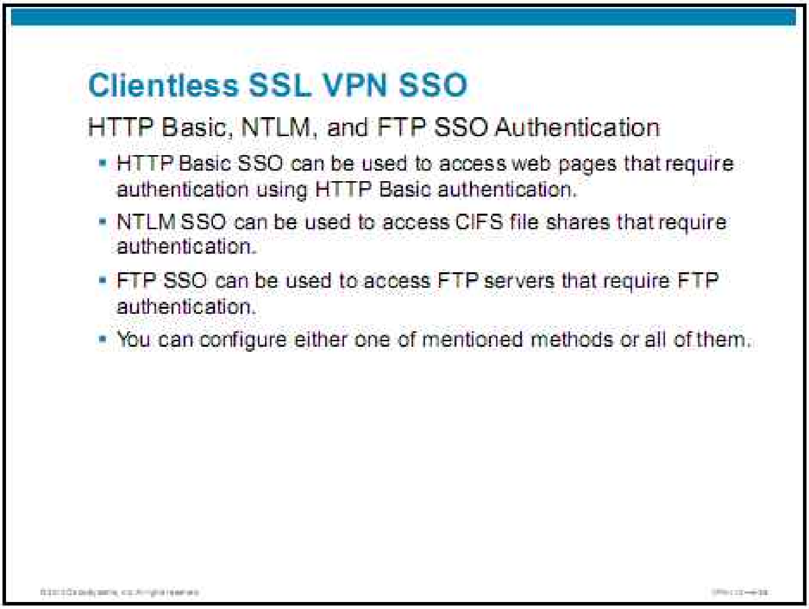
- SSO enables users to access internal services without entering username or password twice
- Five independent features:
  - SSO with HTTP Basic, NTLM, and FTP authentication
  - Dedicated SSO servers (CA SiteMinder, SAML Browser Post Profile)
  - Macro substitution
  - SSO for plug-ins
  - SSO for smart tunnels (Microsoft Internet Explorer on Microsoft Windows only)

SSO is a clientless SSL VPN feature that enables users to access different services on internal servers without entering a username and password more than once. The SSO functionality can be implemented using four independent features:

- **SSO with HTTP Basic, NTLM, and FTP authentication:** This feature configures the adaptive security appliance to automatically pass clientless SSL VPN user login credentials (username and password) on to internal servers that are using HTTP Basic, NT LAN Manager (NTLM), and FTP authentication.
- **Dedicated SSO servers:** In this method, one of two dedicated SSO servers is deployed in the internal network:
  - Computer Associates SiteMinder SSO server
  - Security Assertion Markup Language (SAML), Version 1.1, Browser Post Profile SSO server
- **Macro substitution:** This feature can be used for web-based applications in combination with bookmarks and allows dynamic parameters, such as username and password, to be inserted into an HTTP request.
- **SSO for application plug-ins:** This method enables SSO for users who use application plug-ins to access internal resources.
- **SSO for smart tunnels:** This is a simplified SSO method that you can use for web-based applications that use smart tunnels. This feature is supported only on Microsoft Internet Explorer running on Microsoft Windows operating systems.

This topic briefly describes all five SSO methods.

**Note** Another SSO feature available on the Cisco ASA adaptive security appliance is SSO authentication using HTTP Form, but it is not described in the course.



## Clientless SSL VPN SSO

### HTTP Basic, NTLM, and FTP SSO Authentication

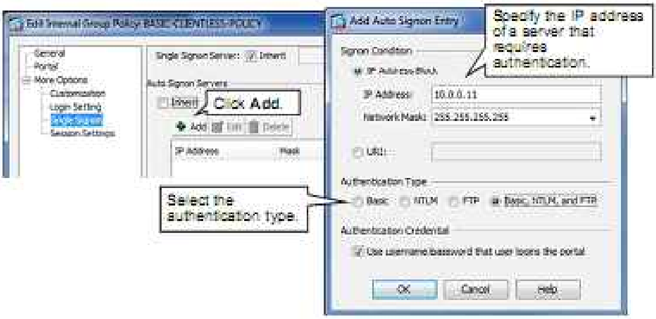
- HTTP Basic SSO can be used to access web pages that require authentication using HTTP Basic authentication.
- NTLM SSO can be used to access CIFS file shares that require authentication.
- FTP SSO can be used to access FTP servers that require FTP authentication.
- You can configure either one of mentioned methods or all of them.

You can use the HTTP Basic authentication feature to access web pages that require authentication using the HTTP Basic authentication method. NTLM SSO can be used to access web pages and Common Internet File System (CIFS) file shares that require NTLM authentication. FTP authentication can be used to access FTP servers, which require authentication. When configuring SSO, you can enable either one of the mentioned methods or all of them.

## Clientless SSL VPN SSO

Configure HTTP Basic, NTLM, and FTP SSO Authentication

- Configure SSO in group policy or in user profile



● IP Address/Mask
IP Address: 10.0.0.11
Network Mask: 255.255.255.255
○ URI:

○ Basic ○ NTLM ○ FTP ● Basic, NTLM, and FTP

☑ Use username/password that user logins the portal

Specify the IP address of a server that requires authentication.

Click Add.

Select the authentication type.

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

To enable SSO using HTTP Basic, NTLM, and FTP authentication using Cisco ASDM, complete the following steps:

**Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies** (not shown in the figure). The Group Policies pane appears.

**Step 2** Select a group policy for which you would like to enable SSO and click **Edit**. The Edit Internal Group Policy window appears.

**Step 3** Expand the **More Options** menu and select the **Single Signon** submenu.

**Step 4** Click **Add** in the Auto Signon Servers area of the window. The Add Auto Signon Entry window appears.

**Step 5** Enter the IP address of the server that requires authentication into the IP Address field. In the example, the server at 10.0.0.11 is specified.

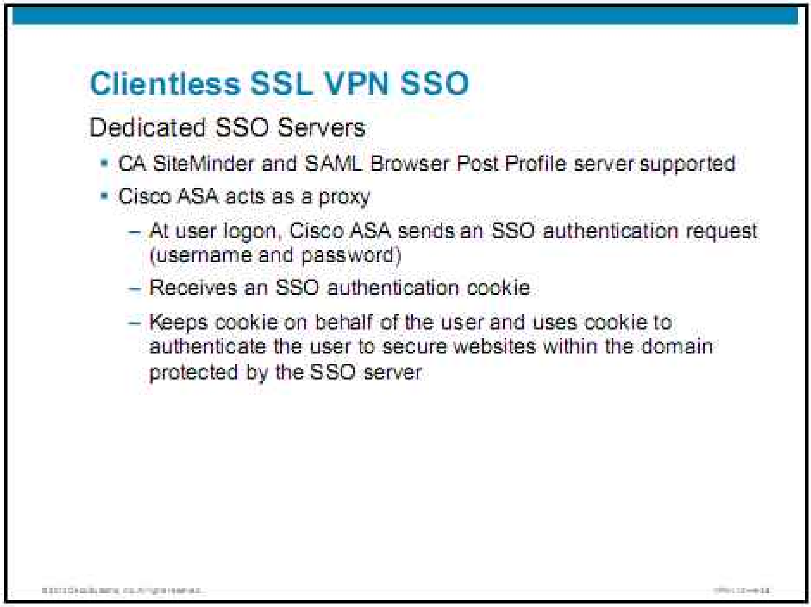
**Step 6** Alternatively, click the URI radio button and enter the server that requires authentication in the URI form.

**Step 7** Select the authentication type by checking appropriate check box. In the example, HTTP Basic, NTLM, and FTP authentication is selected.

**Step 8** Make sure that the Use Username/Password that User Logins the Portal check box is checked.

**Step 9** Click **OK** twice.

**Step 10** Click **Apply** to apply the configuration.



## Clientless SSL VPN SSO

### Dedicated SSO Servers

- CA SiteMinder and SAML Browser Post Profile server supported
- Cisco ASA acts as a proxy
  - At user logon, Cisco ASA sends an SSO authentication request (username and password)
  - Receives an SSO authentication cookie
  - Keeps cookie on behalf of the user and uses cookie to authenticate the user to secure websites within the domain protected by the SSO server

The security appliance supports two dedicated SSO platforms:

- Computer Associates Trust SiteMinder (formerly Netegrity SiteMinder)
- SAML, Version 1.1 Browser Post Profile.

The SSO mechanism invokes after successful user authentication to either an AAA server (SiteMinder) or a SAML Browser Post Profile server. In these cases, the clientless SSL VPN server running on the adaptive security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the clientless SSL VPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS.

If the authenticating server approves the authentication request, it returns an SSO authentication cookie to the clientless SSL VPN server. This cookie is kept on the adaptive security appliance on behalf of the user and used to authenticate the user to secure websites within the domain that is protected by the SSO server.

The SSO process occurs in these steps:

**Step 1** User logs into the clientless SSL VPN portal.

**Step 2** Security appliance authenticates the user on the external AAA database.

**Step 3** After successful authentication, the security appliance submits user profile to the SiteMinder server.

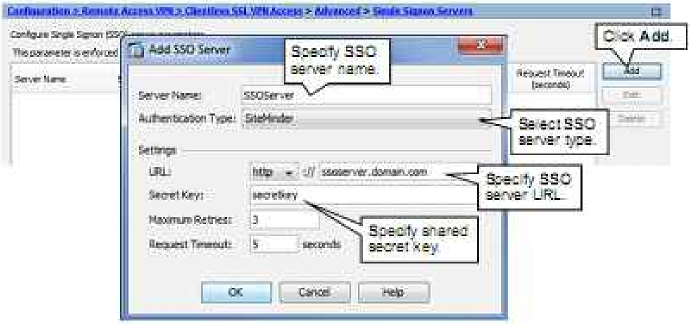
**Step 4** SSO server returns an authentication cookie. The appliance associates the cookie with the client sessions and stores it for the duration of the session.

**Step 5** When the user requests access to an internal server that would normally require repeated authentication, the security appliance delivers the authentication cookie on behalf of the user.

## Clientless SSL VPN SSO

### Dedicated SSO Servers Configuration

- You have to assign configured SSO server to group policy or user profile.



Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Signon Servers

Add SSO Server

Server Name: SSOServer

Authentication Type: SiteMinder

Settings

URL: http ://ssoserver.domain.com

Secret Key: secretkey

Maximum Retries: 3

Request Timeout: 5 seconds

Click Add.

Specify SSO server name.

Select SSO server type.

Specify SSO server URL.

Specify shared secret key.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Signon Servers

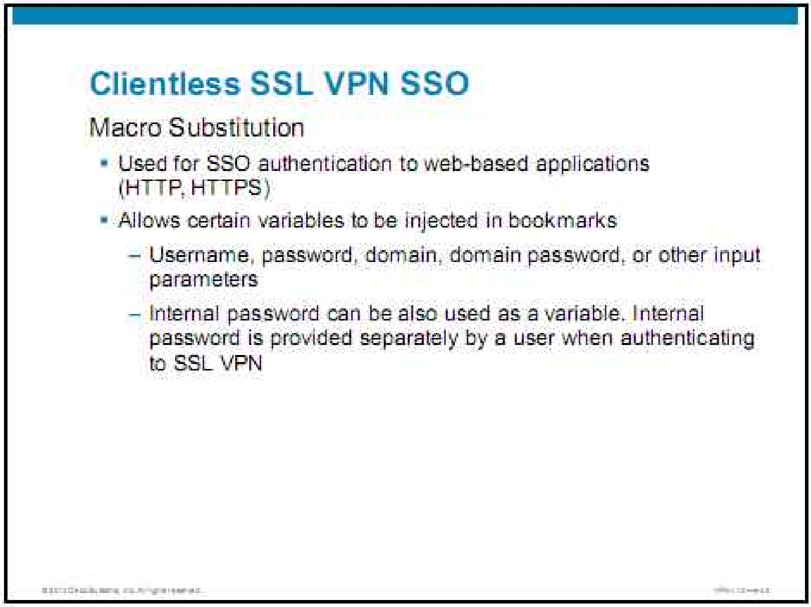
To set up SiteMinder SSO for a user or group, you must first configure an AAA server (RADIUS, LDAP, or others). After the AAA server authenticates the user, the clientless SSL VPN server uses HTTPS to send an authentication request to the SiteMinder SSO server.

To add an SSO server, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Signon Servers**, choose **Add,** and enter these parameters for a SiteMinder server:

- **Server Name:** If adding a server, enter the name of the new SSO server. If editing a server, this field is display only; it displays the name of the selected SSO server.
- **Authentication Type:** Displays the type of SSO server. The types that are currently supported by the Cisco ASA adaptive security appliance are SiteMinder and SAML Browser Post Profile.
- **URL:** Enter the SSO server URL to which the adaptive security appliance makes SSO authentication requests.
- **Secret Key:** Enter the secret key that is used to encrypt authentication requests to the SSO server. It is configured on the security appliance, the SSO server, and the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.
- **Maximum Retries:** The number of times the security appliance retries a failed SSO authentication attempt before the authentication times-out. The range is from 1 to 5 retries inclusive, and the default is three retries.
- **Request Timeout:** The number of seconds before a failed SSO authentication attempt times out. The range is from 1 to 30 seconds, the default is 5 seconds.

In addition to configuring the Cisco ASA adaptive security appliance, the SiteMinder Policy Server must be configured for Cisco authentication scheme. This configuration is not covered in this lesson.

The SAML Browser Post Profile server requires a different set of parameters, which is not shown in the figure.



## Clientless SSL VPN SSO

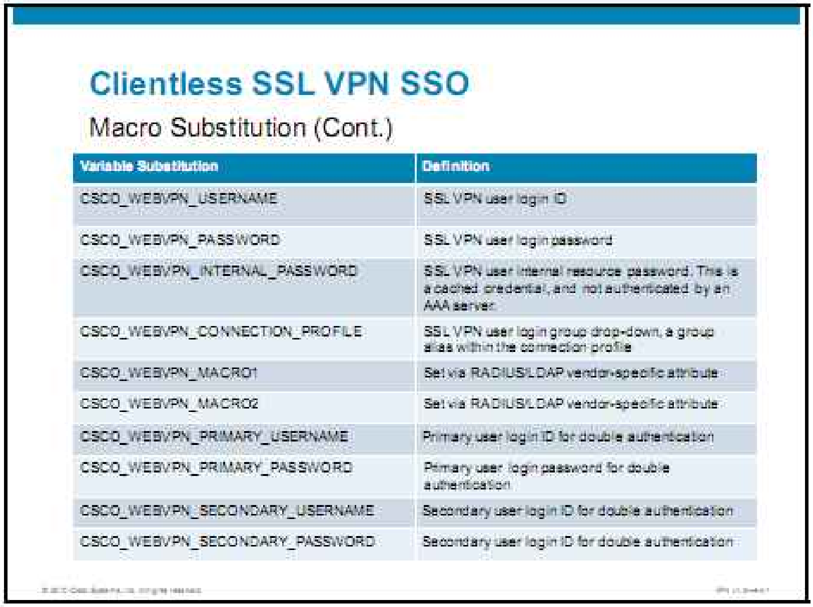
Macro Substitution

- Used for SSO authentication to web-based applications (HTTP, HTTPS)
- Allows certain variables to be injected in bookmarks
  - Username, password, domain, domain password, or other input parameters
  - Internal password can be also used as a variable. Internal password is provided separately by a user when authenticating to SSL VPN

Macro substitution allows for certain variables to be injected in bookmarks for substituting dynamic values, such as the username, password, domain, domain password, or other input parameters.

This functionality provides SSO functionality when you access web-based services through the web interface (such as Microsoft Web Access).

One of the most frequently used variables for SSO is the internal password. The internal password is entered by the VPN user separately from the user password or passwords. The security appliance caches the internal password and uses it for authenticating the user to the internal services. The internal password enables SSO in situations when the VPN users are authenticated based on certificates or OTP credentials. In these situations, there is no user password (certificates), or the password keeps changing (OTP). The internal password is used for SSO and not AAA. The primary and optionally secondary password is used for AAA and not for SSO.



## Clientless SSL VPN SSO

### Macro Substitution (Cont.)

| Variable Substitution | Definition |
|---|---|
| CSCO_WEBVPN_USERNAME | SSL VPN user login ID |
| CSCO_WEBVPN_PASSWORD | SSL VPN user login password |
| CSCO_WEBVPN_INTERNAL_PASSWORD | SSL VPN user internal resource password. This is a cached credential, and not authenticated by an AAA server. |
| CSCO_WEBVPN_CONNECTION_PROFILE | SSL VPN user login group drop-down, a group alias within the connection profile |
| CSCO_WEBVPN_MACRO1 | Set via RADIUS/LDAP vendor-specific attribute |
| CSCO_WEBVPN_MACRO2 | Set via RADIUS/LDAP vendor-specific attribute |
| CSCO_WEBVPN_PRIMARY_USERNAME | Primary user login ID for double authentication |
| CSCO_WEBVPN_PRIMARY_PASSWORD | Primary user login password for double authentication |
| CSCO_WEBVPN_SECONDARY_USERNAME | Secondary user login ID for double authentication |
| CSCO_WEBVPN_SECONDARY_PASSWORD | Secondary user login ID for double authentication |

Variable and macro substitution is configured in the bookmark settings.

The following variables can be used for substitution:

- **CSCO_WEBVPN_USERNAME:** Username from login page
- **CSCO_WEBVPN_PASSWORD:** Password from login page
- **CSCO_WEBVPN_INTERNAL_PASSWORD:** Internal password from login page
- **CSCO_WEBVPN_CONNECTION_PROFILE:** Connection profile from login page

The following macros can be used for substitution in http, https, and cifs URL types:

- **CSCO_WEBVPN_MACRO1:** Radius and LDAP attribute
- **CSCO_WEBVPN_MACRO2:** Radius and LDAP attribute

The following variables can be used for substitution when double AAA authentication is used:

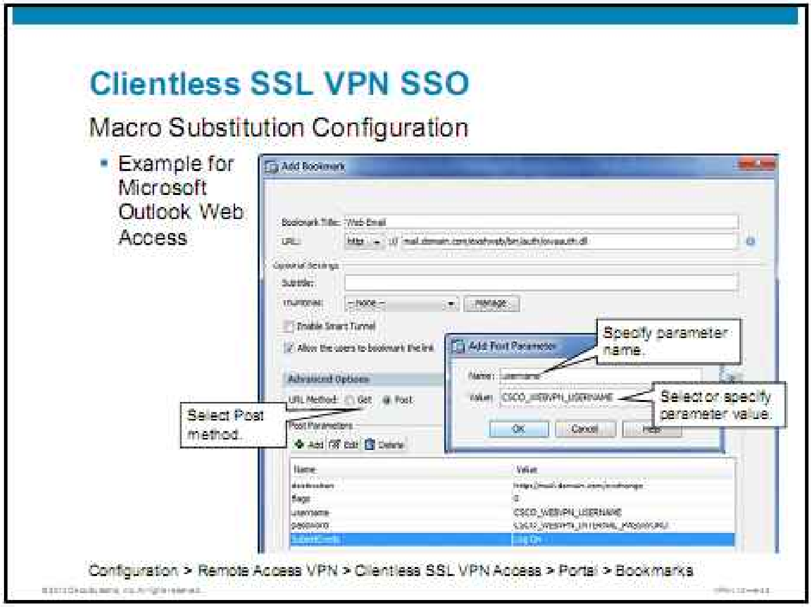
- **CSCO_WEBVPN_PRIMARY_USERNAME:** Primary username from login page
- **CSCO_WEBVPN_SECONDARY_PASSWORD:** Secondary password from login page
- **CSCO_WEBVPN_PRIMARY_PASSWORD:** Primary password from login page
- **CSCO_WEBVPN_SECONDARY_PASSWORD:** Secondary password from login page

You need to enable the VPN users to enter the internal password. The internal password field is disabled by default. To enable the internal password field, perform these steps:

**Step 1** Navigate to the **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles** menu (not shown in the figure).

**Step 2** Check the **Allow User to Enter Internal Password on the Login Page** check box (not shown in the figure).

**Step 3** Click **Apply** to apply the configuration.



## Clientless SSL VPN SSO

### Macro Substitution Configuration

- Example for Microsoft Outlook Web Access

Add Bookmark

Bookmark Title: Web Email

URL: http :// mail.domain.com/exchweb/bin/auth/owaauth.dll

Optional Settings

Subtitle:

Thumbnail: -- None --

□ Enable Smart Tunnel

☑ Allow the users to bookmark the link

Advanced Options

URL Method: ○ Get ● Post

Post Parameters

Add Post Parameter

Name: username

Value: CSCO_WEBVPN_USERNAME

| Name | Value |
|---|---|
| destination | https://mail.domain.com/exchange |
| flags | 0 |
| username | CSCO_WEBVPN_USERNAME |
| password | CSCO_WEBVPN_INTERNAL_PASSWORD |
| SubmitCreds | Log On |

Specify parameter name.

Select or specify parameter value.

Select Post method.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks

This figure shows an example of a bookmark that was created to provide SSO functionality for Outlook Web Access based on username and internal password. Complete the following steps to configure macro substitution for a bookmark:

**Step 1** Inside Cisco ASDM, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks** (not shown in the figure).

**Step 2** Select a bookmark list where you would like to create a macro-substitution-enabled bookmark and click **Edit**. The Edit Bookmark List window appears (not shown in the figure).

**Step 3** Click **Add** to add new bookmark. The Add Bookmark window opens.

**Step 4** Enter the bookmark title into the Bookmark Title window.

**Step 5** Enter the bookmark URL into the URL input field.

**Step 6** Expand the **Advanced Options**.

**Step 7** Click the **Post** radio button to specify that the HTTP POST method will be used to send parameters to a web server.

**Step 8** Click **Add**. The Add Post Parameter window appears.

**Step 9** Enter a parameter name into the Name input field.

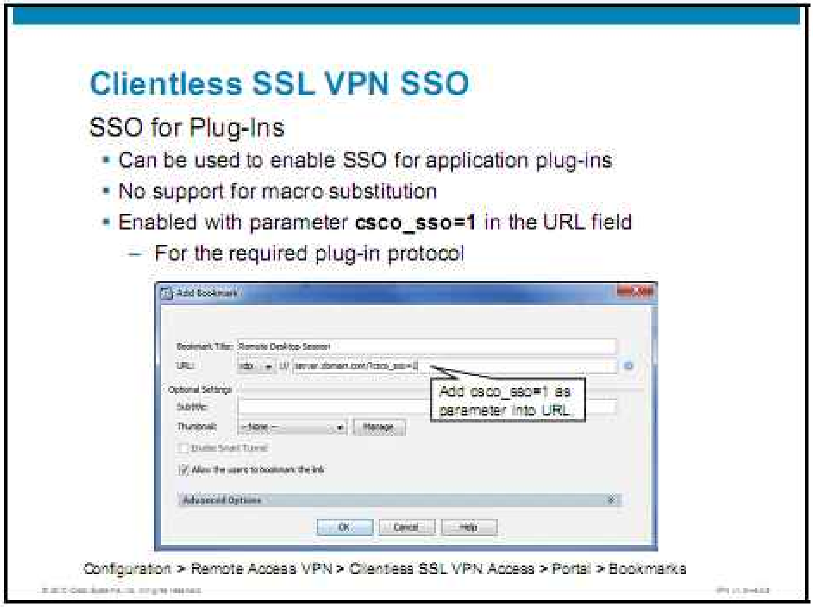
**Step 10** Select a variable or macro from the Value drop-down menu. You can also manually enter an arbitrary parameter value.

**Step 11** Click **OK**.

**Step 12** Repeat the previous four steps to add all parameters.

**Step 13** Click **OK** two times.

**Step 14** Click **Apply** to apply the configuration.



## Clientless SSL VPN SSO

### SSO for Plug-Ins

- Can be used to enable SSO for application plug-ins
- No support for macro substitution
- Enabled with parameter **csco_sso=1** in the URL field
  - For the required plug-in protocol

Bookmark Title: Remote Desktop Session

URL: rdp :// server.domain.com/?csco_sso=1

Optional Settings

Subtitle:

Thumbnail: -- None --

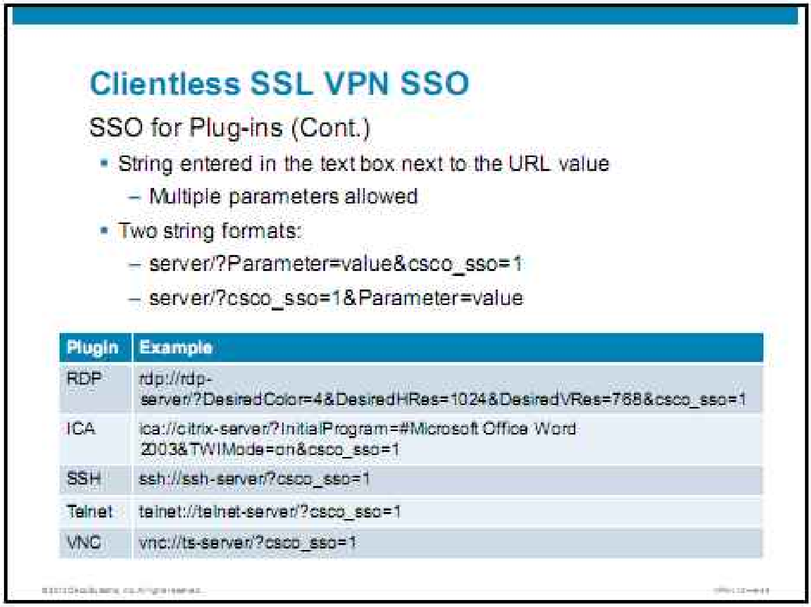
□ Enable Smart Tunnel

☑ Allow the users to bookmark the link

Add csco_sso=1 as parameter into URL

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks

When you access internal applications using client-server plug-ins, you can deploy SSO functionality by configuring bookmarks using the appropriate URL type. The application plug-ins are Java applets that do not support the variable and macro. The SSO functionality is enabled by embedding the **csco_sso=1** parameter in the URl field next to the URL protocol.



## Clientless SSL VPN SSO

### SSO for Plug-ins (Cont.)

- String entered in the text box next to the URL value
  - Multiple parameters allowed
- Two string formats:
  - server/?Parameter=value&csco_sso=1
  - server/?csco_sso=1&Parameter=value

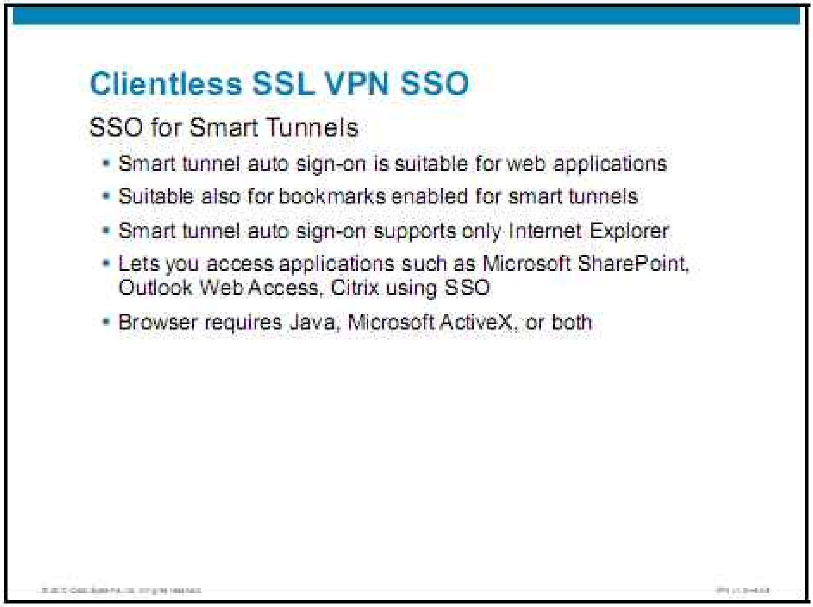
| Plugin | Example |
|---|---|
| RDP | rdp://rdp-server/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768&csco_sso=1 |
| ICA | ica://citrix-server/?InitialProgram=#Microsoft Office Word 2003&TWIMode=on&csco_sso=1 |
| SSH | ssh://ssh-server/?csco_sso=1 |
| Telnet | telnet://telnet-server/?csco_sso=1 |
| VNC | vnc://ts-server/?csco_sso=1 |

The string that is entered in the URI field can include, in addition to the server IP address or FQDN, an &-delimited list of multiple parameters. Together with the SSO setting csco_sso=1, two notations are possible:

- server/?Parameter=value&Parameter=value&csco_sso=1
- server/?csco_sso=1&Parameter=value&Parameter=value

Examples for various plug-in protocols are shown here:

- rdp://rdp-server/?DesiredColor=4&DesiredHRes=1024&DesiredVRes=768&csco_sso=1
- ica://citrix-server/?InitialProgram=#Microsoft Office Word 2003&TWIMode=on&csco_sso=1
- ssh://ssh-server/?csco_sso=1
- telnet://telnet-server/?csco_sso=1
- vnc://ts-server/?csco_sso=1



## Clientless SSL VPN SSO

SSO for Smart Tunnels

- Smart tunnel auto sign-on is suitable for web applications
- Suitable also for bookmarks enabled for smart tunnels
- Smart tunnel auto sign-on supports only Internet Explorer
- Lets you access applications such as Microsoft SharePoint, Outlook Web Access, Citrix using SSO
- Browser requires Java, Microsoft ActiveX, or both

Smart tunnel auto sign-on is a straightforward method that is used to configure SSO for particular internal servers. You should use it if you do not have dedicated SSO servers in your network. With auto sign-on configured for particular internal servers, the adaptive security appliance passes the login credentials that the user of clientless SSL VPN entered to log into the adaptive security appliance (username and password) to those particular internal servers. Auto sign-on is supported only for smart tunnel application access from Internet Explorer.

In auto sign-on, you specify a list of internal servers requiring authentication, to which the appliance should automatically provide user credentials. More specifically, the Cisco ASA adaptive security appliance content rewriter automatically provides credentials to internal HTTP resources that match preconfigured URIs.

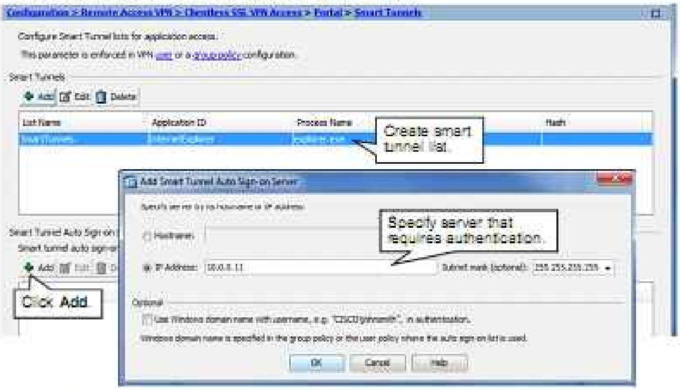
The auto sign-on feature lets you enable the replacement of login credentials for Windows Internet (WinINet) connections. Most Microsoft applications use WinINet, including Internet Explorer. Mozilla browsers (such as Firefox and Flock) do not, so they are not supported by this feature. Auto sign-on supports HTTP-based authentication types: basic and NTLM. Form-based authentication does not work with this feature.

Credentials are statically associated to destination hosts, not services, so if initial credentials are wrong, they cannot be dynamically corrected during runtime. In addition, because of the association with destinations hosts, providing support for an auto-sign-on-enabled host may not be desirable if you want to deny access to some of the services on that host.

You should not enable auto sign-on for servers that do not require authentication or that use credentials different from the adaptive security appliance. When auto sign-on is enabled, the adaptive security appliance passes on the login credentials that the user entered to log into the SSL VPN.

## Clientless SSL VPN SSO

### Configure SSO for Smart Tunnels



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels

Configure Smart Tunnel lists for application access.

This parameter is enforced in VPN user or a group policy configuration.

Smart Tunnels

| List Name | Application ID | Process Name | Hash |
|---|---|---|---|
| SmartTunnels | InternetExplorer | iexplore.exe | |

Smart Tunnel Auto Sign-on Server List

Add Smart Tunnel Auto Sign-on Server

Specify server by its hostname or IP address.

○ Hostname:

● IP Address: 10.0.0.11   Subnet mask (optional): 255.255.255.255

Optional

☐ Use Windows domain name with username, e.g. "CISCO\jsmith", in authentication.

Windows domain name is specified in the group policy or the user policy where the auto sign-on list is used.

Create smart tunnel list.

Specify server that requires authentication.

Click **Add**.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels

You will complete the following steps to configure a list of smart tunnel auto sign-on servers:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels** (not shown in the example).

**Step 2** Click **Add** in the Smart Tunnel Auto Sign-on Server List area. The Add Smart Tunnel Auto Sign-on Server List appears (not shown in the example).

**Step 3** Enter the auto sign-on list name into the List Name field (not shown in the example).

**Step 4** Click **Add**. The Add Smart Tunnel Auto-Sign-on Server window appears.

**Step 5** Click the **IP Address** radio button and enter the IP address of the server requiring authentication.

**Step 6** Optionally, select a subnet mask from the Subnet Mask (Optional) drop-down menu.

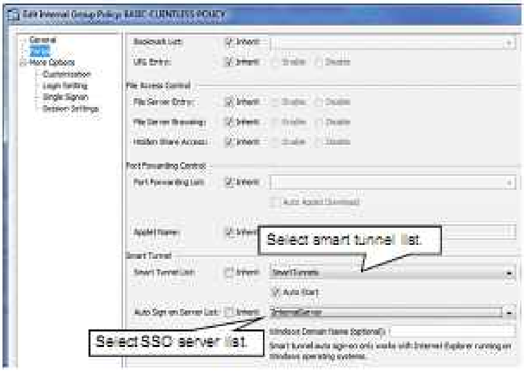
**Step 7** Click **OK** twice.

**Step 8** Click **Apply** to apply the configuration.

## Auto Sign-On with Smart Tunnels for Internet Explorer

### Apply Feature to Users or Policy Groups

- You have to assign smart tunnel list and SSO list to a group policy or user profile.



Edit Internal Group Policy: BASIC-CLIENTLESS-POLICY

Bookmark List: ☑ Inherit
URL Entry: ☑ Inherit ○ Enable ○ Disable
File Access Control
File Server Entry: ☑ Inherit ○ Enable ○ Disable
File Server Browsing: ☑ Inherit ○ Enable ○ Disable
Hidden Share Access: ☑ Inherit ○ Enable ○ Disable
Port Forwarding Control
Port Forwarding List: ☑ Inherit
□ Auto Applet Download
Applet Name: ☑ Inherit
Smart Tunnel
Smart Tunnel List: □ Inherit SmartTunnels
☑ Auto Start
Auto Sign-on Server List: □ Inherit InternalServer
Windows Domain Name (optional):
Smart tunnel auto sign-on only works with Internet Explorer running on Windows operating systems.

Select smart tunnel list.

Select SSO server list.

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

You have to apply the auto sign-on server list to a user profile or group policy. Configuring the feature on the group policy level is recommended because it offers a more scalable approach.

To apply the auto sign-on server list to the group policy, complete these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**.

**Step 2** Choose **Portal** and locate the Smart Tunnel section.

**Step 3** Apply the appropriate Smart Tunnel Server List by either selecting it from the drop-down menu in the Auto Sign-on Server section or have it inherited from a higher-level policy.

**Step 4** Make sure that a smart tunnel application for Microsoft Internet Explorer is also activated for the specific user or user group because the auto-sign feature works only in combination with smart tunnels for Internet Explorer.

In the example, the smart tunnel application list that is named SmartTunnelList, which enables the Internet Explorer smart tunnel, is selected, and the Auto Sign-on Server List that is named InternalServer is selected for the policy-group.

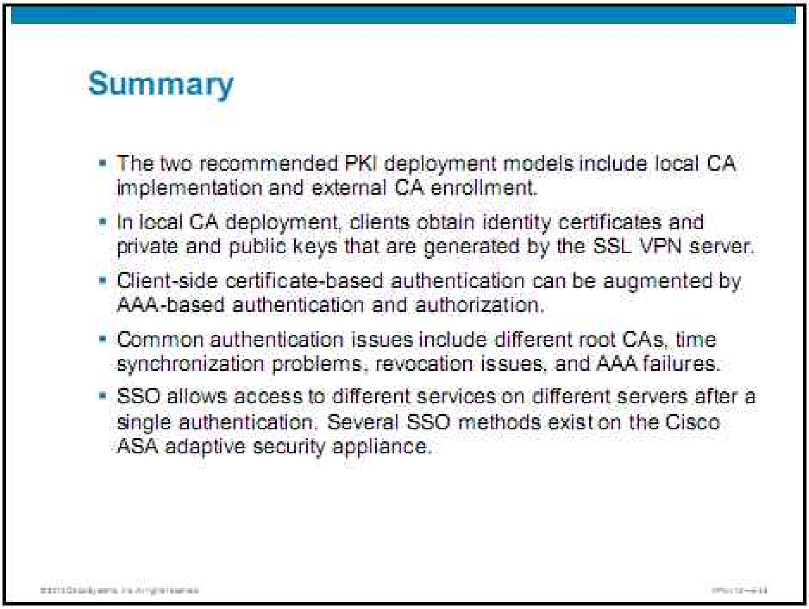
### Feature Support

This table shows the availability of the auto sign-on feature on Cisco ASA adaptive security appliances, as well as the software release that introduced this feature.

| Feature | Platform | Software Release |
|---|---|---|
| Auto sign-on with smart tunnels for IE | All Cisco ASA adaptive security appliance platforms | Version 8.1.2 |
| Variable and macro substitution | All Cisco ASA adaptive security appliance platforms | Version 8.2.1 |

# Summary

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



## Summary

- The two recommended PKI deployment models include local CA implementation and external CA enrollment.
- In local CA deployment, clients obtain identity certificates and private and public keys that are generated by the SSL VPN server.
- Client-side certificate-based authentication can be augmented by AAA-based authentication and authorization.
- Common authentication issues include different root CAs, time synchronization problems, revocation issues, and AAA failures.
- SSO allows access to different services on different servers after a single authentication. Several SSO methods exist on the Cisco ASA adaptive security appliance.

VPN v1.0—4-14

## Lesson 4

# Customizing the Clientless SSL VPN User Interface and Portal

## Overview

Many enterprises wish to customize the user interface that is presented to clientless Secure Sockets Layer (SSL) virtual private network (VPN) clients. Typical needs include language localization that ensures that users navigate through pages that are written in their own language. This lesson discusses basic and advanced customization of portal navigation pages, help pages, and application integration. It explains how to implement language localization and describes the integration options with the Cisco AnyConnect client.

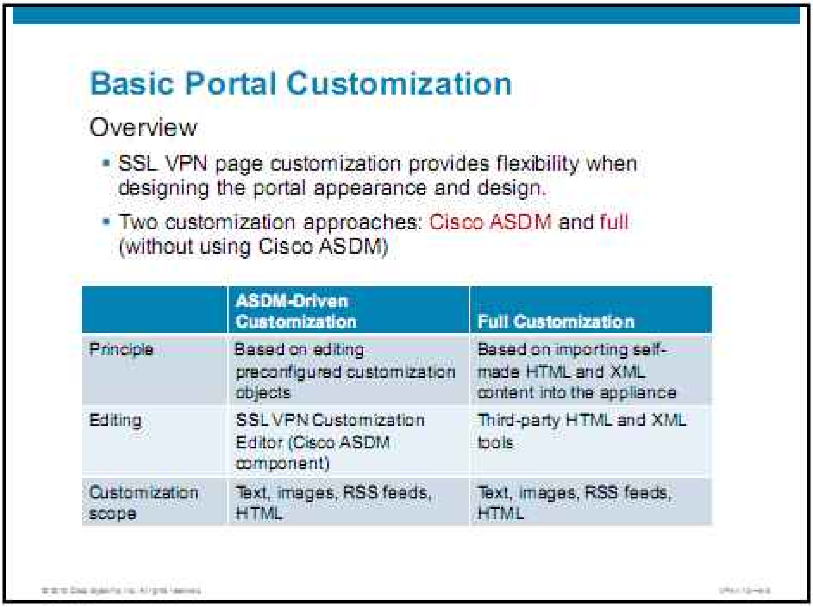
### Objectives

Upon completing this lesson, you will be able to deploy and manage advanced clientless VPN application access features of a Cisco clientless SSL VPN. This ability includes being able to meet these objectives:

- Configure and verify basic customization of the VPN portal navigation pages
- Configure and verify full portal HTML customization
- Configure and verify portal localization
- Configure and verify portal help customization
- Configure and verify integration of the Cisco AnyConnect client with the clientless portal

# Deploying Basic Navigation Customization

This topic describes how to configure and verify the basic customization of the VPN portal navigation panes.



## Basic Portal Customization

Overview

- SSL VPN page customization provides flexibility when designing the portal appearance and design.
- Two customization approaches: Cisco ASDM and full (without using Cisco ASDM)

| | ASDM-Driven Customization | Full Customization |
|---|---|---|
| Principle | Based on editing preconfigured customization objects | Based on importing self-made HTML and XML content into the appliance |
| Editing | SSL VPN Customization Editor (Cisco ASDM component) | Third-party HTML and XML tools |
| Customization scope | Text, images, RSS feeds, HTML | Text, images, RSS feeds, HTML |

The web portal that is accessed by users who connect via clientless SSL VPN can be customized to reflect the requirements that are defined by the enterprise policy or by the local language. The Cisco ASA adaptive security appliance uses customization objects to define the appearance of user screens. The clientless SSL VPN end-user interface consists of a series of HTML panels. A user logs in to the clientless SSL VPN by entering the IP address or Domain Name System (DNS) name of the Cisco ASA adaptive security appliance. The first panel that displays is the login window. The user then navigates through the remaining panels. Both the login window and the subsequent panels can be customized.

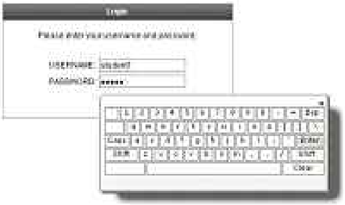
There are two general approaches to portal customization:

- **ASDM-driven customization:** In this basic approach, the administrator uses Cisco Adaptive Security Device Manager (Cisco ASDM) to edit customization objects that correspond to the elements that are visible in the portal. Cisco ASDM automatically launches the SSL VPN Customization Editor, which includes the necessary graphical features to complete the task. Basic customization is simple to configure and allows the customization of most portal elements, such as text, images, RSS feeds, and HTML content.
- **Full customization:** This method allows administrators to create their own HTML or XML content and import it into the appliance. This approach is useful for enterprises that want to use advanced third-party tools to create complex portal content.

## Basic Portal Customization

### On-Screen Keyboard

- Provides protection against key loggers
- Requires that users enter password using Java keyboard
- Can appear for VPN login or any time that authentication is required
- Available for Cisco ASDM and full customization



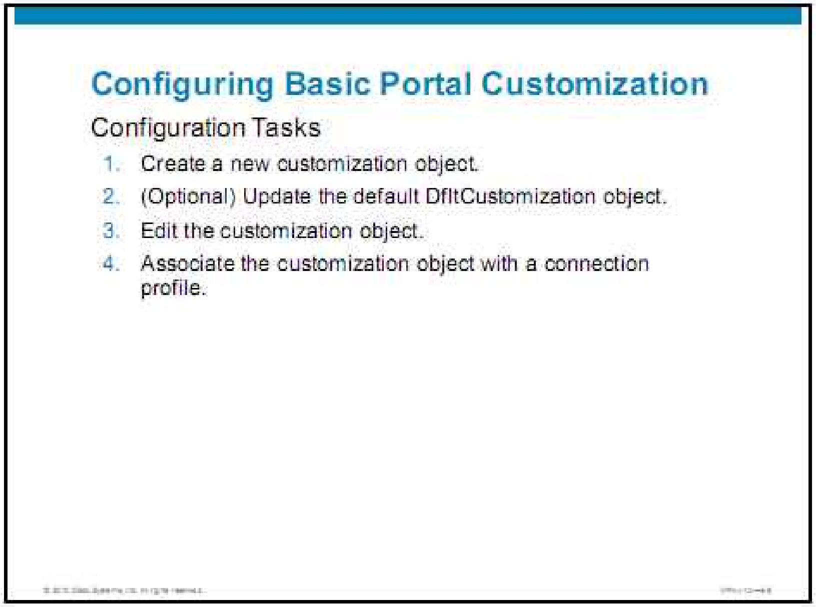
Login

Please enter your username and password

USERNAME: student

PASSWORD: *****

The Cisco ASA security appliance supports the use of a Java-based on-screen keyboard to provide an additional layer of security and helps protect users from security threats such as key loggers. The on-screen keyboard is enabled on the Object Customization page. It can be configured to show only when someone is logging in to the SSL VPN system, or anytime that network authentication is required. The on-screen keyboard feature is available for both basic and full portal customization.



## Configuring Basic Portal Customization

Configuration Tasks

1. Create a new customization object.
2. (Optional) Update the default DfltCustomization object.
3. Edit the customization object.
4. Associate the customization object with a connection profile.

The adaptive security appliance uses customization objects to define the appearance of user screens. A customization object is compiled from an XML file, which contains XML tags for all the customizable screen items that are displayed to remote users.

To perform basic portal customization, you will perform the following configuration tasks:

1. Create a new customization object. The administrator may decide to create a new customization object without manipulating the preconfigured DfltCustomization object. The new customization object is created with the settings of a default template, which is identical to the default configuration of the DfltCustomization object.

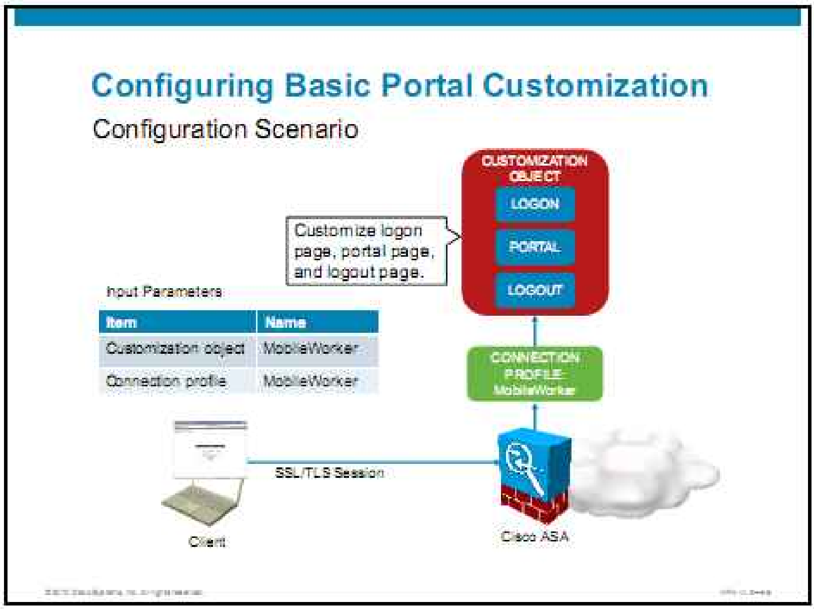
2. Optionally, update the default DfltCustomization object. This is the alternative approach, in which the administrator updates the default customization object.

3. Edit customization object. Editing the object launches the SSL VPN Customization Editor.

4. Associate customization object with connection profile.

VPN users view the customized pages after they access their connection profile. The clients may connect to a connection profile using one of two methods:

- By selecting the appropriate connection profile from the drop-down list that is visible in the logon page
- By connecting to a URL that is associated with the specific connection profile



## Configuring Basic Portal Customization

Configuration Scenario

Input Parameters

| Item | Name |
|---|---|
| Customization object | MobileWorker |
| Connection profile | MobileWorker |

CUSTOMIZATION OBJECT
LOGON
PORTAL
LOGOUT
Customize logon page, portal page, and logout page.
CONNECTION PROFILE: MobileWorker
SSL/TLS Session
Client
Cisco ASA

This figure presents the configuration scenario that is used in upcoming configuration tasks.

The table lists the input parameters that are required to achieve this goal. Before you perform basic portal customization, you will need to gather the required portal parameters. Those parameters include the following:

- Name of the customization object. In this example, the name is MobileWorker.
- Name of the connection profile that must be associated with the customization object. In this scenario, its name is identical to the customization object.

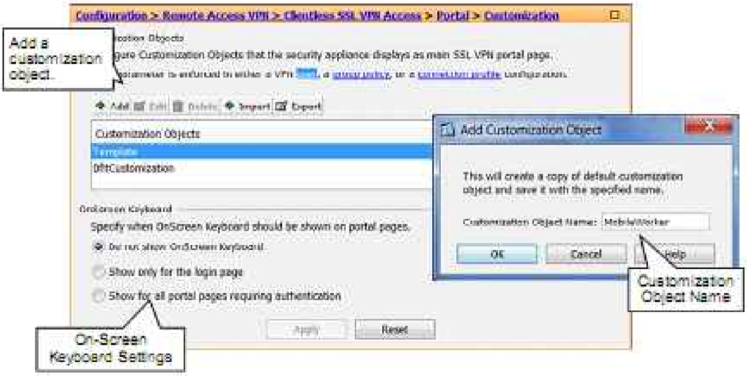
The customization object includes three components: logon page, portal, and logout page. All three elements will be customized in this scenario.

Initially, when a user first connects, the default customization object (named DfltCustomization) that is identified in the connection profile (tunnel group) determines how the logon page appears. If the connection profile list is enabled, and the user selects a different profile that has its own customization, the screen changes to reflect the customization object for that new profile.

After the remote user is authenticated, the screen appearance is determined by the customization object that has been assigned to the connection profile.

## Configuring Basic Portal Customization

### Task 1: Create a New Customization Object



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

…ization Objects

…gure Customization Objects that the security appliance displays as main SSL VPN portal page.

…parameter is enforced in either a VPN tunnel, a group policy, or a connection profile configuration.

Customization Objects

Template

DfltCustomization

OnScreen Keyboard

Specify when OnScreen Keyboard should be shown on portal pages.

● Do not show OnScreen Keyboard

○ Show only for the login page

○ Show for all portal pages requiring authentication

Add Customization Object

This will create a copy of default customization object and save it with the specified name.

Customization Object Name: MobileWorker

Add a customization object.
Add
Edit
Delete
Import
Export
Apply
Reset
OK
Cancel
Help
Customization Object Name
On-Screen Keyboard Settings

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

The first configuration task in the basic customization sequence is to create a new customization object. It is optional, because you may alternatively edit the existing DfltCustomization object that is preinstalled within the image bundle. To create a customization object and configure the on-screen keyboard, complete the following steps:

**Step 1** Choose **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Configuration** and click the **Add** button.

**Step 2** Enter the object name and click **OK**.

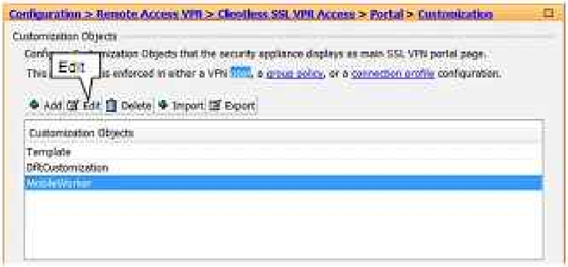
**Step 3** Configure the on-screen keyboard settings by clicking the appropriate radio button at the bottom of the main customization pane. The on-screen keyboard configuration applies to all customization objects, independently of the connection profile that the user connects to. The available choices are as follows:

- Do Not Show Onscreen Keyboard (default setting)
- Show Only for the Login Page
- Show for All Portal Pages Requiring Authentication

**Step 4** Click **Apply** to apply the configuration. The new customization object cannot be edited until it has not been committed to the appliance.

## Configuring Basic Portal Customization

### Task 3: Edit the Customization Object



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

Customization Objects

Configure Customization Objects that the security appliance displays as main SSL VPN portal page.
This is enforced in either a VPN user, a group policy, or a connection profile configuration.

| Customization Objects |
|---|
| Template |
| DfltCustomization |
| MobileWorker |

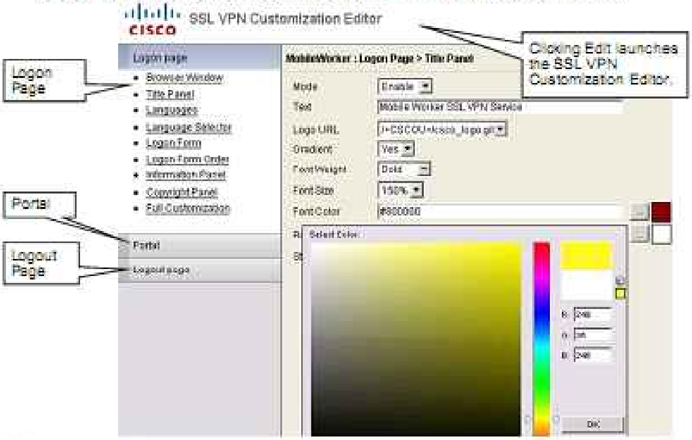
Note: Saving of configuration is required for access to newly created customization object.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

Next, make sure that the appropriate object is highlighted and click **Edit**. This step launches the SSL VPN Customization Editor in a secondary web-browser window.

## Configuring Basic Portal Customization

### Task 3: Edit the Customization Object (Logon Page)



MobileWorker : Logon Page > Title Panel

Mode: Enable
Text: Mobile Worker SSL VPN Service
Logo URL: /+CSCOU+/cisco_logo.gif
Gradient: Yes
Font Weight: Bold
Font Size: 150%
Font Color: #800000

Logon Page

Portal

Logout Page

Clicking Edit launches the SSL VPN Customization Editor.

After you have chosen the newly created customization object and clicked Edit, the main user interface customization window for the SSL VPN Customization Editor will appear. The SSL VPN Customization Editor is split into three distinct areas for user interface configuration:

- Logon page
- Portal page
- Logout page

This figure displays the configuration options that are available in the logon page. Those options include the displayed text, logo URL, and graphic parameters.

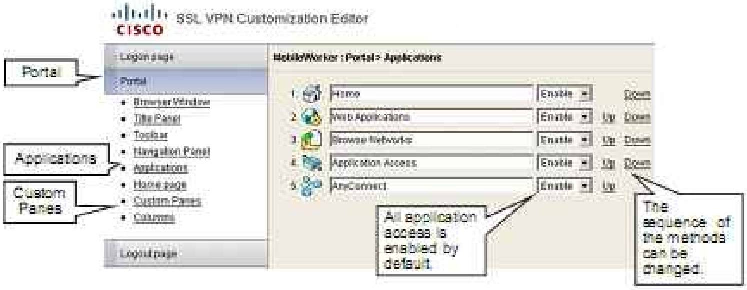
**Note** If you want to use custom elements (such as images) on the portal, you have to upload them first to the Cisco ASA adaptive security appliance. You can upload them using Cisco ASDM by navigating to Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Web Contents and clicking the Import button.

When you make changes to the template pages using the SSL VPN Customization Editor, click the **Save** button to save the changes to the appropriate page.

## Configuring Basic Portal Customization

### Task 3: Edit the Customization Object (Portal)

- Page text, graphics, and colors can be modified for each page.
- Title panels can also be modified by using style sheets (CSS).



MobileWorker : Portal > Applications

1. Home — Enable — Down
2. Web Applications — Enable — Up Down
3. Browse Networks — Enable — Up Down
4. Application Access — Enable — Up Down
5. AnyConnect — Enable — Up

All application access is enabled by default.

The sequence of the methods can be changed.

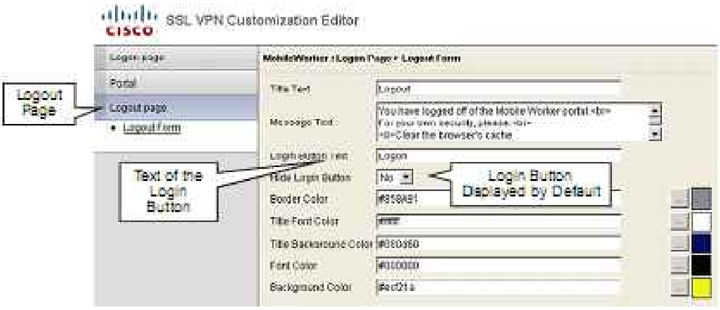
When one of the customization submenus is chosen on the left side of the editor window, the corresponding configuration menu for that selection is displayed on the right side. From these configuration menus, the user can change page text, graphics, and colors. You can modify colors by using a color selector that is available wherever colors can be modified. Title panels also have the option of being configured using cascading style sheets (CSSs).

This figure presents the configuration options that are available in the Portal section. Those options include browser window, title panel, toolbar, navigation panel, applications, home page, custom panes, and columns. Choosing the Applications link displays the available types of applications.

You can reorder the application types or disable any of them. All types are enabled by default.

## Configuring Basic Portal Customization

Task 3: Edit the Customization Object (Logout Page)



MobileWorker › Logon Page › Logout Form

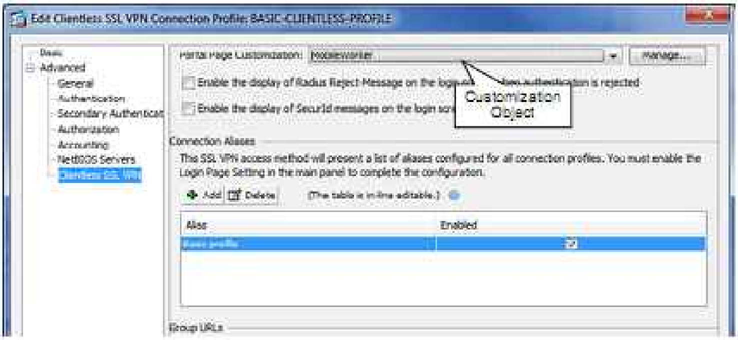
| | |
|---|---|
| Title Text | Logout |
| Message Text | You have logged off of the Mobile Worker portal <br><br>For your own security, please: <br><br><li>Clear the browser's cache |
| Login Button Text | Logon |
| Hide Login Button | No |
| Border Color | #858A91 |
| Title Font Color | #ffffff |
| Title Background Color | #000d60 |
| Font Color | #000000 |
| Background Color | #ecf21a |

The customization of the logout page involves a single element. The logout form defines the text and colors that are to be displayed in the logout page.

**Note** Remember to save the changes to the customized user interface so that it will reflect the desired modifications.

## Configuring Basic Portal Customization

Task 4: Assign Customization Object to Connection Profile



Edit Clientless SSL VPN Connection Profile: BASIC-CLIENTLESS-PROFILE

Portal Page Customization: MobileWorker

☐ Enable the display of Radius Reject-Message on the login s... when authentication is rejected

☐ Enable the display of SecurId messages on the login scr...

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

(The table is in-line editable.)

| Alias | Enabled |
|---|---|
| basic-profile | ☑ |

Group URLs

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

In the fourth task, you must assign the customization object to the respective connection profile. Perform the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

**Step 2** Choose the desired connection profile and click the **Edit** button. A new window opens.

**Step 3** Choose **Advanced > Clientless SSL VPN** and select the customization object from the Portal Page Customization drop-down list.

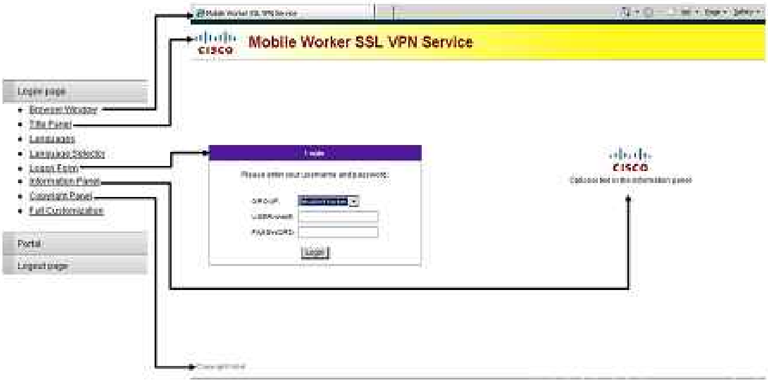
**Step 4** Click **OK**.

**Step 5** Click **Apply** to apply the configuration.

In this figure, the newly defined customization object MobileWorker is being assigned to the connection profile MobileWorker.

## Verifying Basic Portal Customization

Logon Page Verification



© 2010 Cisco Systems, Inc. All rights reserved.

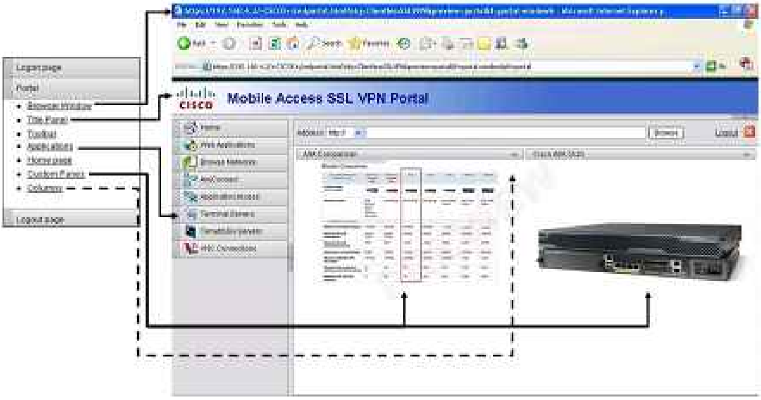
This figure shows a customized portal logon page. The figure illustrates which configuration elements can be found in the logon page.

Specifically, the logon page includes these elements:

- **Browser Window:** Changes the text that is shown in the main browser title bar.
- **Title Panel:** Changes the title that is shown on the main page of the SSL VPN logon page as well as available colors.
- **Languages:** Selects the default language that is used for the logon page.
- **Language Selector:** Provides a drop-down selector for other available languages to the logon page.
- **Logon Form:** Changes the text and colors that are displayed in the Logon box.
- **Information Panel:** The information panel is an optional panel that can be enabled and placed to either side of the logon form. The information panel can include required text and graphics as needed for the logon page.
- **Copyright Panel:** Adds copyright information to the logon page.
- **Full Customization:** Configures the security appliance to use a fully customized web page that you can choose from previously uploaded media that is found in the Web Contents submenu.

## Verifying Basic Portal Customization

### Portal Page Verification



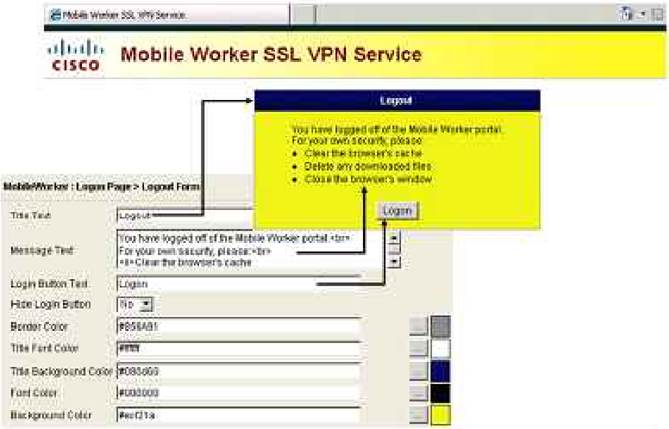
This figure shows a sample customized web portal page. In addition to customized headers, a custom column has been added to provide room for additional information on the web portal.

The following items can be modified when configuring a portal page:

- **Browser Window:** Changes the text that is shown in the main browser title bar.
- **Title Panel:** Changes the title that is shown on the main page of the SSL VPN portal page as well as available colors.
- **Toolbar:** Configures the text that is shown for the address bar and the floating toolbar that is shown when you navigate pages.
- **Applications:** Configures the order and name of available application buttons. Application buttons can also be disabled from this menu.
- **Home Page:** Configures the use of a custom page for the web portal.
- **Custom Panes:** Allows the creation of custom panes to provide additional functionality to the web portal. The following panes are available:
  - — Text
  - — HTML
  - — Image
  - — RSS Feed
- **Columns:** Configures the number of columns to be displayed on the web portal.

# Verifying Basic Portal Customization

## Logout Page Verification



You have logged off of the Mobile Worker portal.
For your own security, please:

- Clear the browser's cache
- Delete any downloaded files
- Close the browser's window

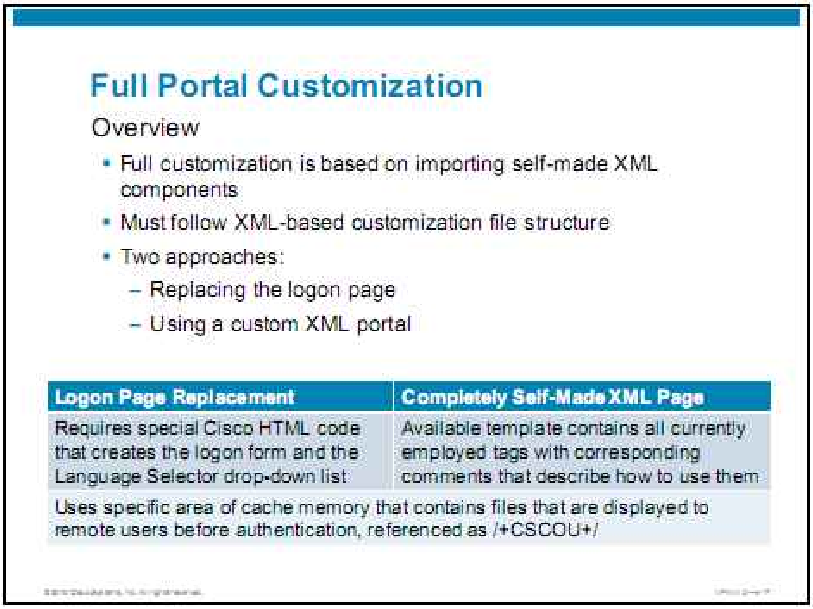
**MobileWorker : Logon Page > Logout Form**

| | |
|---|---|
| Title Text | Logout |
| Message Text | You have logged off of the Mobile Worker portal.<br><br>For your own security, please:<br><br><li>Clear the browser's cache |
| Login Button Text | Logon |
| Hide Login Button | No |
| Border Color | #858A81 |
| Title Font Color | #ffffff |
| Title Background Color | #083d60 |
| Font Color | #000000 |
| Background Color | #ecf21a |

This figure shows a customized logout page. The figure illustrates the correspondence between the configuration options and the logout page elements.

# Deploying Full Portal Customization

This topic describes how to configure and verify full portal HTML customization.



## Full Portal Customization

Overview

- Full customization is based on importing self-made XML components
- Must follow XML-based customization file structure
- Two approaches:
  - Replacing the logon page
  - Using a custom XML portal

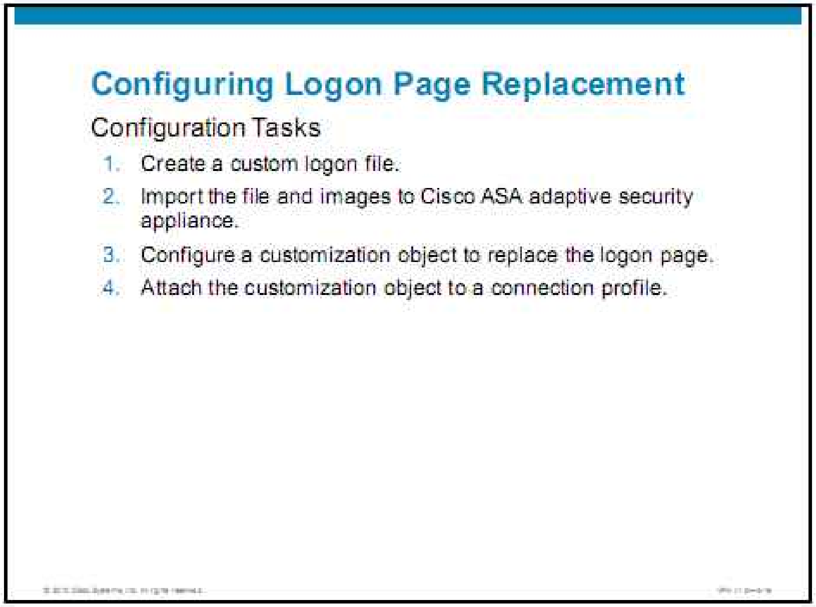
| Logon Page Replacement | Completely Self-Made XML Page |
|---|---|
| Requires special Cisco HTML code that creates the logon form and the Language Selector drop-down list | Available template contains all currently employed tags with corresponding comments that describe how to use them |
| Uses specific area of cache memory that contains files that are displayed to remote users before authentication, referenced as /+CSCOU+/ | |

Full portal customization allows you to create the HTML and XML pages using external tools instead of the SSL VPN Customization Editor, and then import them as portal pages. The self-made content must follow the XML-based customization file structure that is used by Cisco. Optionally, you may choose one of two methods to simplify the full portal customization:

- You can export an XML file to a local computer or server, make changes to the XML tags, and reimport the file to the Cisco ASA adaptive security appliance. The security appliance includes a template that contains all currently employed tags with corresponding comments that describe how to use them.
- You can replace only the logon page and leave the remaining panels unchanged. The self-made logon page must include special Cisco HTML code that creates the logon form and the Language Selector drop-down list.

If you do not simplify the customization process using any of these methods, you can create your own page and import it to the adaptive security appliance for full customization. Either method creates a customization object that you apply to a connection profile or group policy.

In all methods, files that are displayed to remote users before authentication must reside in a specific area of the adaptive security appliance cache memory, which is represented by the path /+CSCOU+/. Therefore, the source for each image in the file must include this path.



## Configuring Logon Page Replacement

### Configuration Tasks

1. Create a custom logon file.
2. Import the file and images to Cisco ASA adaptive security appliance.
3. Configure a customization object to replace the logon page.
4. Attach the customization object to a connection profile.

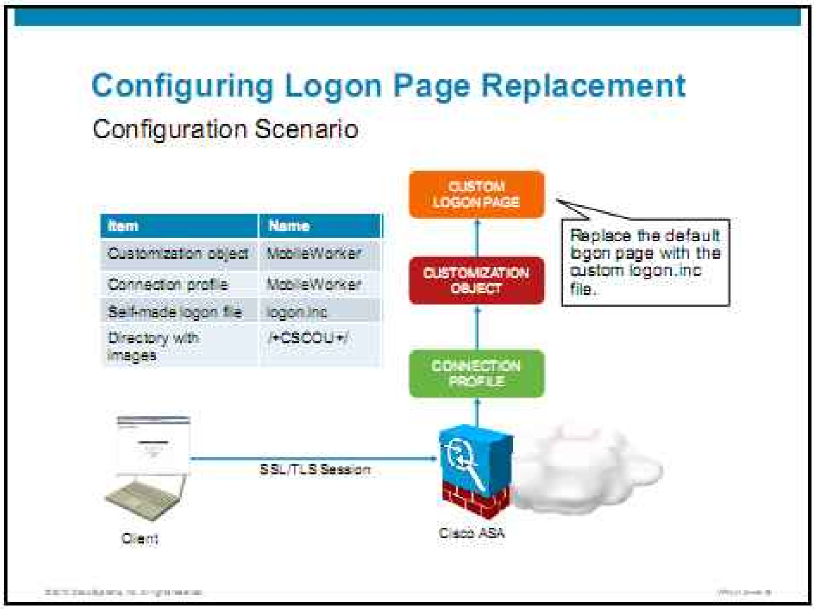
To replace the logon page, perform the following configuration tasks:

1. Create a custom logon page file and name it logon.inc (path to images must be /+CSCOU+/). The file must include the function csco_ShowLoginForm('lform', which injects the Logon form. It may optionally include the function csco_ShowLanguageSelector('selector') that injects the Language Selector, if language customization is desired.

2. Import the file and images to the Cisco ASA adaptive security appliance as Web Content. The Web Content corresponds to the space in the appliance flash memory that stores the files that are related to the SSL VPN portal.

3. Configure the customization object to replace the login page.

4. Associate the customization object with connection profile.



## Configuring Logon Page Replacement

Configuration Scenario

| Item | Name |
|---|---|
| Customization object | MobileWorker |
| Connection profile | MobileWorker |
| Self-made logon file | logon.inc |
| Directory with images | /+CSCOU+/ |

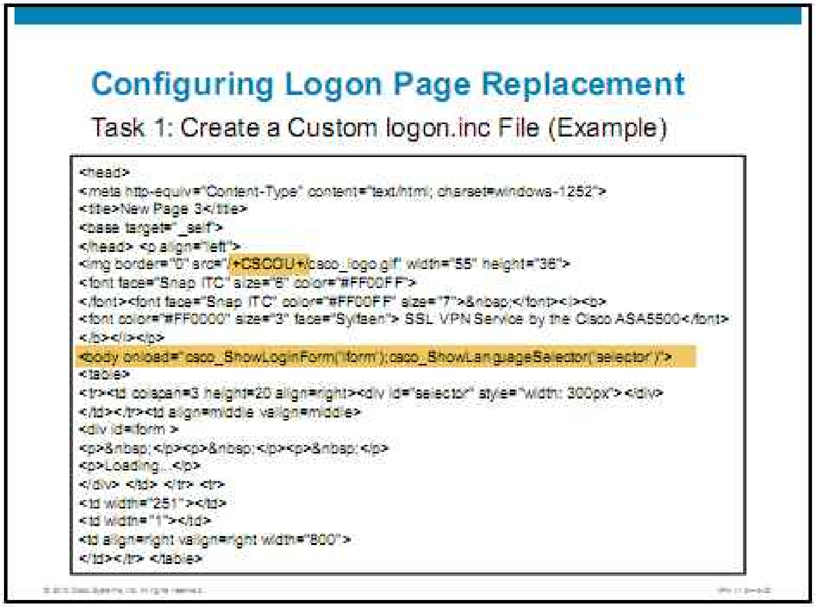
Replace the default bgon page with the custom logon.inc file.

This figure presents the configuration scenario that is used in upcoming configuration tasks.

The table lists the input parameters that are required to achieve this goal. Before you replace the logon page, you will need to gather the required portal parameters. Those parameters include the following:

- Name of the customization object. In this example, the name is MobileWorker.
- Name of the connection profile that must be associated with the customization object. In this case, its name is identical to the customization object.
- Name of the self-made logon page file. The name must be logon.inc.
- Directory, where the images are placed. The directory is referenced as /+CSCOU+/.

When the clients connect to the SSL VPN portal using the MobileWorker connection profile, they will see the pages that are defined by the customization object MobileWorker. This customization object will be configured to replace the default logon page by a self-made logon page.



## Configuring Logon Page Replacement

Task 1: Create a Custom logon.inc File (Example)

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head> <p align="left">
<img border="0" src="/+CSCOU+/csco_logo.gif" width="55" height="36">
<font face="Snap ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7">&nbsp;</font><i><b>
<font color="#FF0000" size="3" face="Sylfaen"> SSL VPN Service by the Cisco ASA5500</font>
</b></i></p>
<body onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">
<table>
<tr><td colspan=3 height=20 align=right><div id="selector" style="width: 300px"> </div>
</td></tr><td align=middle valign=middle>
<div id=lform >
<p>&nbsp;</p><p>&nbsp;</p><p>&nbsp;</p>
<p>Loading...</p>
</div> </td> </tr> <tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
</td></tr> </table>
```

In the first task of this configuration sequence, you create the code for the logon page. This figure illustrates a sample logon.inc file that contains the key elements that are necessary to provide the key logon functionality. The path to images is set to /+CSCOU+/, which represents a special area of the adaptive security appliance cache memory. Files that reside in this special memory can be displayed to remote users before completed authentication.

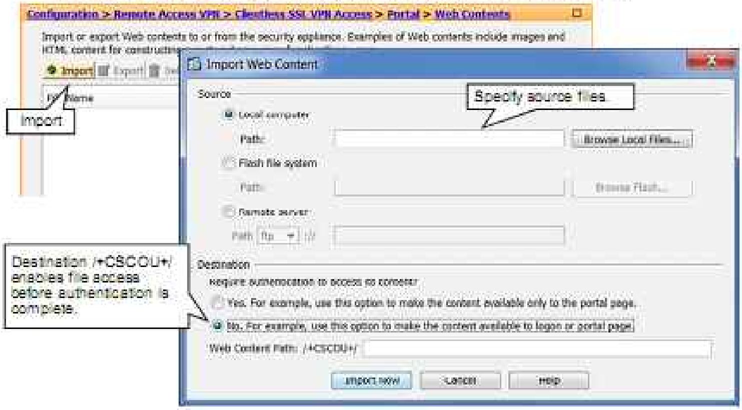
In addition, the logon.inc file invokes two functions: csco_ShowLoginForm, and csco_ShowLanguageSelector, that display the logon form and the language selector, respectively.

This logon.inc example contains this code:

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head> <p align="left">
<img border="0" src="/+CSCOU+/csco_logo.gif" width="55" height="36">
<font face="Snap ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7">&nbsp;</font><i><b>
<font color="#FF0000" size="3" face="Sylfaen"> SSL VPN Service by the Cisco
ASA5500</font>
</b></i></p>
<body
onload="csco_ShowLoginForm('lform');csco_ShowLanguageSelector('selector')">
<table>
<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div>
</td></tr><td align=middle valign=middle>
<div id=lform >
<p>&nbsp;</p><p>&nbsp;</p><p>&nbsp;</p>
<p>Loading...</p>
</div> </td> </tr> <tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">
</td></tr> </table>
```

## Configuring Logon Page Replacement

### Task 2: Import logon.inc and Images to Cisco ASA



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Web Contents

Import or export Web contents to or from the security appliance. Examples of Web contents include images and HTML content for constructing

Import Web Content

Source

● Local computer

Path:

○ Flash file system

Path:

○ Remote server

Path ftp :///

Destination

Require authentication to access its content?

○ Yes. For example, use this option to make the content available only to the portal page.

● No. For example, use this option to make the content available to logon or portal page.

Web Content Path: /+CSCOU+/

Import

Specify source files.

Destination /+CSCOU+/ enables file access before authentication is complete.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Web Contents

In the second task, you will import the logon.inc file and the images it references into the special area of cache memory. Complete the following steps for the logon.inc script and each file that is referenced in it:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Web Contents**.

**Step 2** Click the **Import** button.

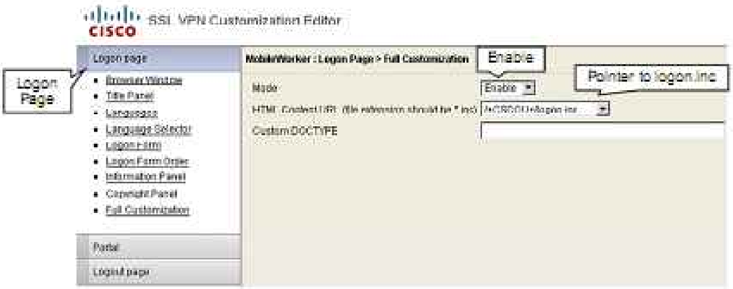
**Step 3** Click the appropriate radio button to point to the source from which to import the files and either locate the file or enter the required URL in the Path field.

**Step 4** In the Destination area, click the **No. For Example, Use This Option to Make the Content Available to Logon or Portal Page** radio button. Optionally, you may specify a subdirectory.

**Step 5** Click **Import Now**.

## Configuring Logon Page Replacement

### Task 3: Configure Replacement of Logon Page



SSL VPN Customization Editor

- Logon page
  - Browser Window
  - Title Panel
  - Languages
  - Language Selector
  - Logon Form
  - Logon Form Order
  - Information Panel
  - Copyright Panel
  - Full Customization
- Portal
- Logout page

MobileWorker : Logon Page > Full Customization

Mode: Enable

HTML Content URL (file extension should be *.inc): /+CSCOU+/logon.inc

Custom DOCTYPE:

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization > Edit

In the third task, you will configure the customization object to use the custom logon.inc file. Complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization**.

**Step 2** Select the appropriate customization object and click the **Edit** button. The SSL VPN Customization Editor opens.

**Step 3** Within the SSL VPN Customization Editor, navigate to **Logon Page > Full Customization.**

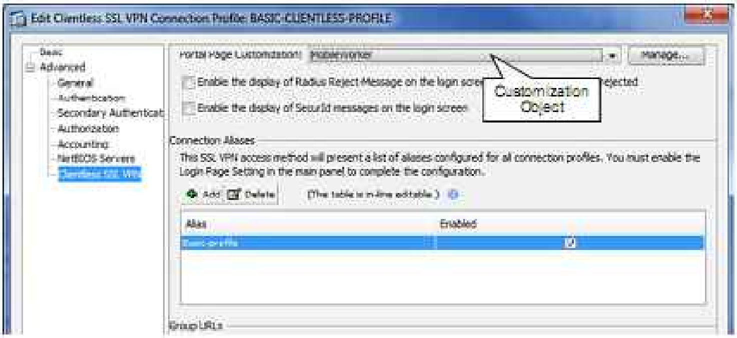
**Step 4** Choose **Enable** from the Mode drop-down menu.

**Step 5** Choose the /+CSCOU+/logon.inc entry from the HTML Content drop-down menu.

**Step 6** Save the customization object (not shown in this figure).

## Configuring Logon Page Replacement

Task 4: Attach Customization Object to Connection Profile



Edit Clientless SSL VPN Connection Profile: BASIC-CLIENTLESS-PROFILE

Portal Page Customization: MobileWorker

□ Enable the display of Radius Reject-Message on the login scre... rejected

□ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

(The table is in-line editable.)

| Alias | Enabled |
|---|---|
| Basic-profile | ☑ |

Group URLs

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

In the fourth task, you will assign the previously configured customization object to a connection profile. Complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

**Step 2** Select a desired connection profile and click **Edit**.

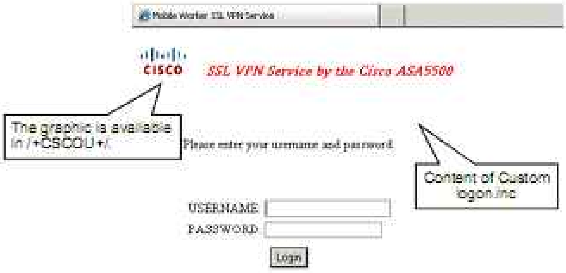
**Step 3** Choose **Advanced > Clientless SSL VPN** and choose the required customization object from the Portal Page Customization drop-down menu.

**Step 4** Click **OK**.

**Step 5** Click **Apply** to apply the configuration.

## Verifying Logon Page Replacement

### Logon Page Verification



Mobile Worker SSL VPN Service

SSL VPN Service by the Cisco ASA5500

Please enter your username and password.

USERNAME

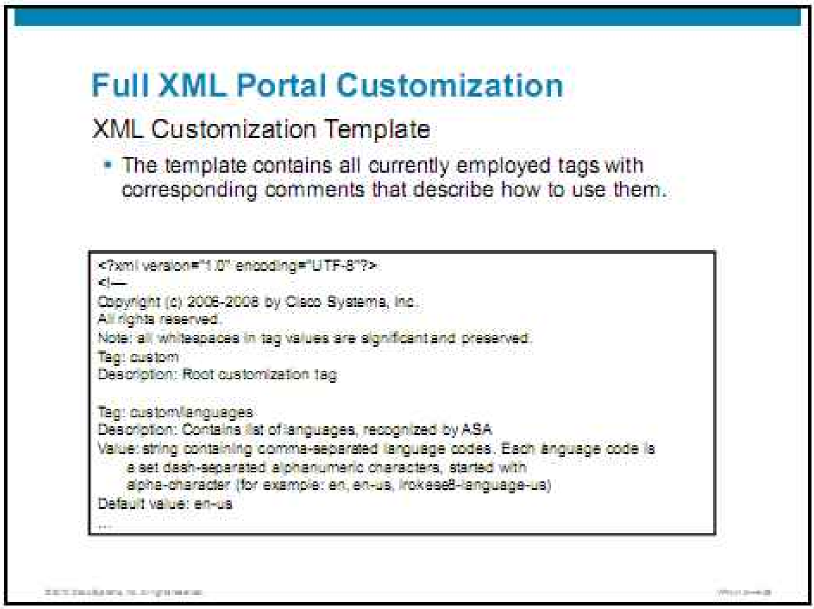
PASSWORD

Login

The graphic is available in /+CSCOU+/.

Content of Custom logon.inc

To verify the replaced logon page, connect to the SSL VPN portal using the connection profile that has the configured customization object associated with it. You should see a customized logon page that includes the previously configured elements, such as text, images, and the logon form. The language selector is not displayed, because it must be enabled using a procedure that is discussed in a later topic.



## Full XML Portal Customization

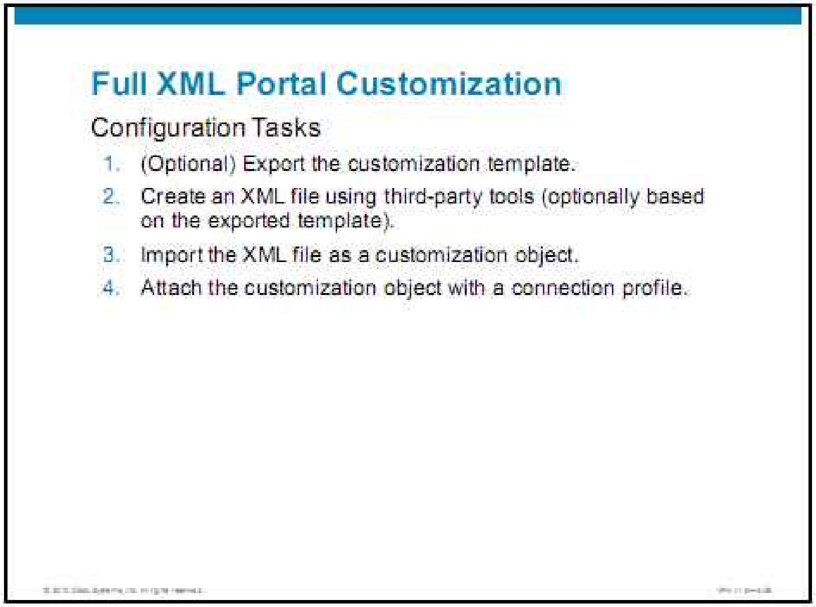
XML Customization Template

- The template contains all currently employed tags with corresponding comments that describe how to use them.

```
<?xml version="1.0" encoding="UTF-8"?>
<!—
Copyright (c) 2006-2008 by Cisco Systems, Inc.
All rights reserved.
Note: all whitespaces in tag values are significantand preserved.
Tag: custom
Description: Root customization tag

Tag: custom/languages
Description: Contains list of languages, recognized by ASA
Value: string containing comma-separated language codes. Each language code is
      a set dash-separated alphanumeric characters, started with
      alpha-character (for example: en, en-us, irokese8-language-us)
Default value: en-us
...
```

The security appliance allows you to perform a full portal customization using a completely self-made XML page. Cisco offers a customization template that will help you create a properly formatted page. The template contains all currently employed tags with corresponding comments that describe how to use them. An initial fragment is shown here:

```
<?xml version="1.0" encoding="UTF-8"?>
<!—
Copyright (c) 2006-2008 by Cisco Systems, Inc.
All rights reserved.
Note: all whitespaces in tag values are significant and
preserved.
Tag: custom
Description: Root customization tag

Tag: custom/languages
Description: Contains list of languages, recognized by ASA
Value: string containing comma-separated language codes. Each
language code is a set dash-separated alphanumeric characters,
started with alpha-character (for example: en, en-us,
irokese8-language-us)
Default value: en-us
```



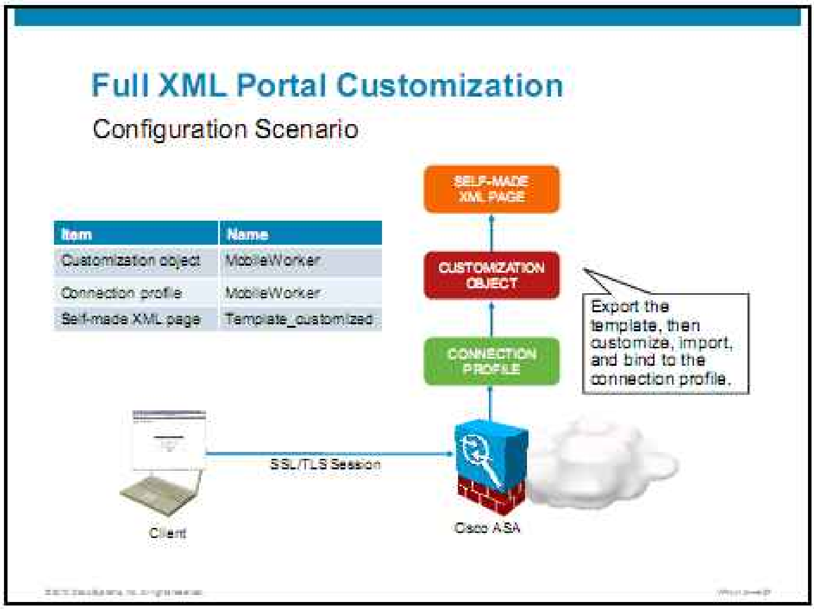
## Full XML Portal Customization

Configuration Tasks

1. (Optional) Export the customization template.
2. Create an XML file using third-party tools (optionally based on the exported template).
3. Import the XML file as a customization object.
4. Attach the customization object with a connection profile.

To perform a full portal customization using a completely self-made XML page, perform the following configuration tasks:

1. Optionally, export the customization template.
2. Create an XML file using third-party tools. This page may be based on the exported template.
3. Import the XML page as a customization object.
4. Associate the customization object with a connection profile.



## Full XML Portal Customization

Configuration Scenario

| Item | Name |
|---|---|
| Customization object | MobileWorker |
| Connection profile | MobileWorker |
| Self-made XML page | Template_customized |

SELF-MADE XML PAGE

CUSTOMIZATION OBJECT

CONNECTION PROFILE

Export the template, then customize, import, and bind to the connection profile.

This figure presents the configuration scenario that is used in upcoming configuration tasks.

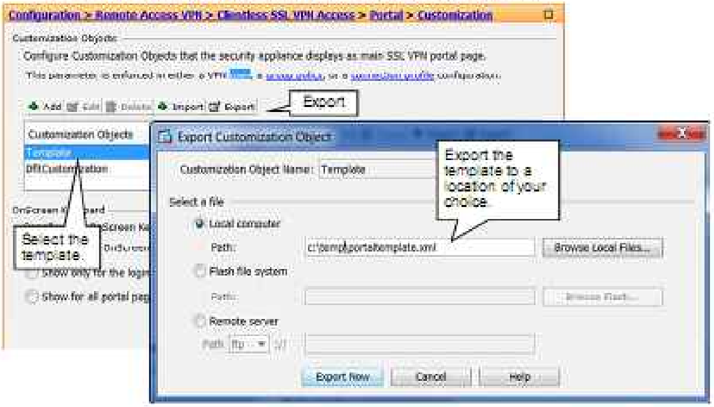
The table lists the input parameters that are required to achieve this goal. Before you perform the full portal customization, you will need to gather the required portal parameters. Those parameters include the following:

- Name of the customization object. In this example, the name is MobileWorker.
- Name of the connection profile that must be associated with the customization object. In this scenario, its name is identical to the customization object.
- Name of the self-made XML page. In this example, it is Template_customized, as it has been created based on the exported template.

When the clients connect to the SSL VPN portal using the MobileWorker connection profile, they will see the pages that are defined by the customization object MobileWorker. This customization object has been created by importing the self-made XML page Template_customized and saving it under the name MobileWorker.

## Full XML Portal Customization

Task 1: Export the Customization Template



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

Customization Objects

Configure Customization Objects that the security appliance displays as main SSL VPN portal page.

This parameter is enforced in either a VPN tunnel, a group policy, or a connection profile configuration.

Customization Object Name: Template

Select a file

● Local computer

Path: c:\temp\portaltemplate.xml

○ Flash file system

○ Remote server

Path: ftp

Export

Select the template.

Export the template to a location of your choice.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

In the first task, you will export the customization template by completing these steps:

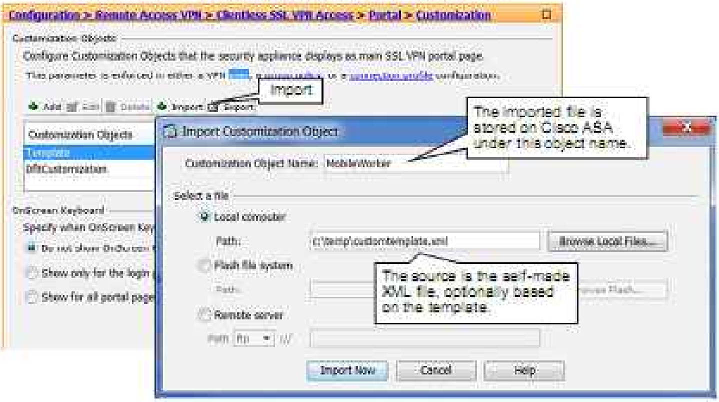
**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization**.

**Step 2** Select the template and click the **Export** button. Identify the destination file by clicking the appropriate radio button and entering the path in the Path field.

**Step 3** Click the **Export Now** button.

## Full XML Portal Customization

### Tasks 2-3: Edit Template and Import File



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

Customization Objects

Configure Customization Objects that the security appliance displays as main SSL VPN portal page.

Customization Object Name: MobileWorker

Path: c:\temp\customtemplate.xml

Import

The imported file is stored on Cisco ASA under this object name.

The source is the self-made XML file, optionally based on the template.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

In the second task, you will create the custom XML page using a third-party tool. This task is not depicted here. This figure illustrates the third task, which imports the custom file named template_customized. Import the file by completing these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization**.

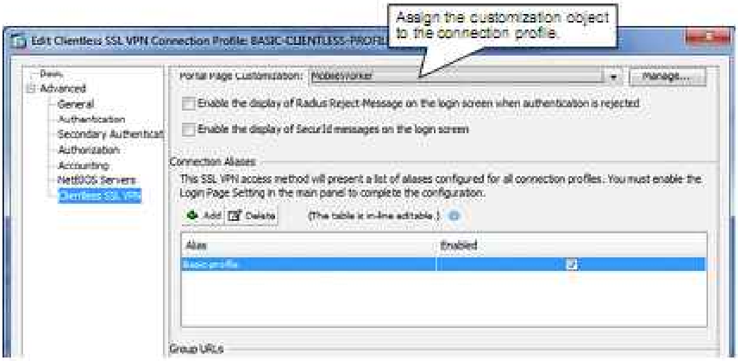
**Step 2** Click the **Import** button. The Import Customization Object window appears.

**Step 3** Provide the intended name of the customization object in the Customization Object Name field (MobileWorker in this example).

**Step 4** Select the source file for import and click **Import Now**.

## Full XML Portal Customization

### Task 4: Attach Customization Object to Connection Profile



Assign the customization object to the connection profile.

Edit Clientless SSL VPN Connection Profile: BASIC-CLIENTLESS-PROFILE

- Basic
- Advanced
  - General
  - Authentication
  - Secondary Authentication
  - Authorization
  - Accounting
  - NetBIOS Servers
  - Clientless SSL VPN

Portal Page Customization: MobileWorker

□ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

□ Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

(The table is in-line editable.)

| Alias | Enabled |
|---|---|
| Basic-profile | ☑ |

Group URLs

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

In the fourth task, you will associate the imported customization object with the connection profile by completing these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.**

**Step 2** Select a desired connection profile and click the **Edit** button. A new window opens.

**Step 3** Choose **Advanced > Clientless SSL VPN** and select the customization object from the Portal Page Customization drop-down list.

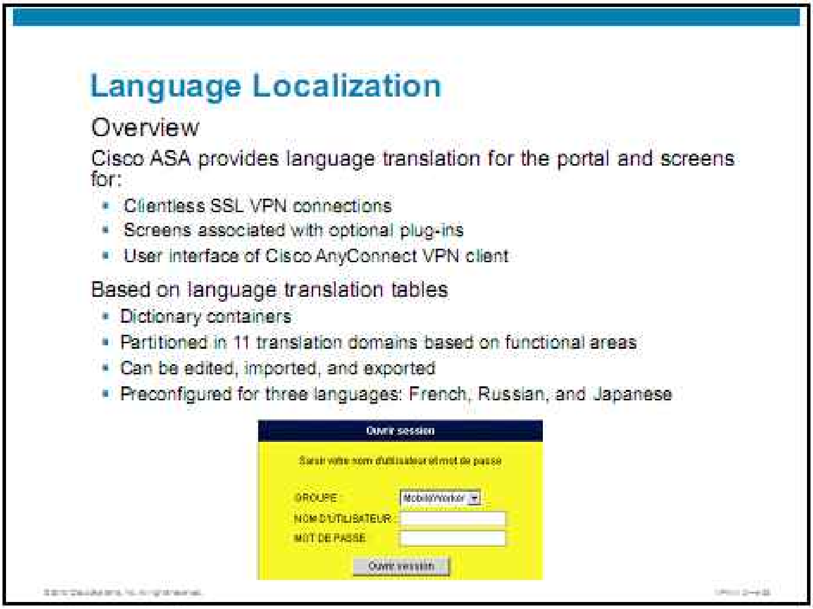
**Step 4** Click **OK**.

**Step 5** Click **Apply** to apply the configuration.

In this figure, the imported customization object MobileWorker is being assigned to the connection profile Basic-profile.

# Deploying Portal Localization

This topic describes how to configure and verify portal language localization.



## Language Localization

Overview

Cisco ASA provides language translation for the portal and screens for:

- Clientless SSL VPN connections
- Screens associated with optional plug-ins
- User interface of Cisco AnyConnect VPN client

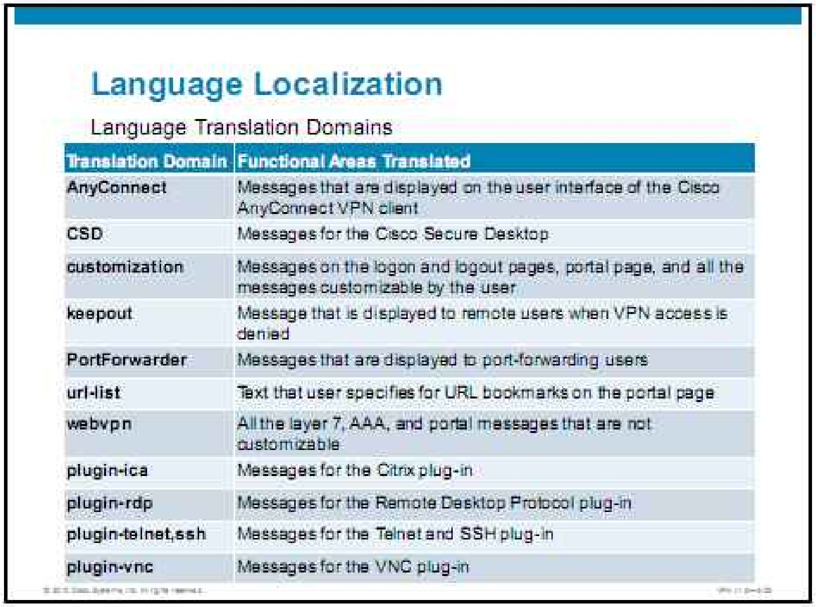
Based on language translation tables

- Dictionary containers
- Partitioned in 11 translation domains based on functional areas
- Can be edited, imported, and exported
- Preconfigured for three languages: French, Russian, and Japanese

The Cisco ASA adaptive security appliance provides language translation for the portal and the screens that are displayed to users. The screens include browser-based, clientless SSL VPN connections, screens that are associated with optional plug-ins, and the interface that is displayed to Cisco AnyConnect VPN client users.

To improve the manageability of the language localization, the language support is based on multiple translation tables that correspond to functional areas of the SSL VPN portal. A translation domain covers its functional area and the messages that are visible to remote users. There are 11 translation domains, and each of them can be edited, imported, and exported. This modular approach offers users the flexibility to modify the desired subsets of the dictionary.

Several translation domains have three preconfigured languages in addition to English. The preconfigured languages are French, Russian, and Japanese.



## Language Localization

Language Translation Domains

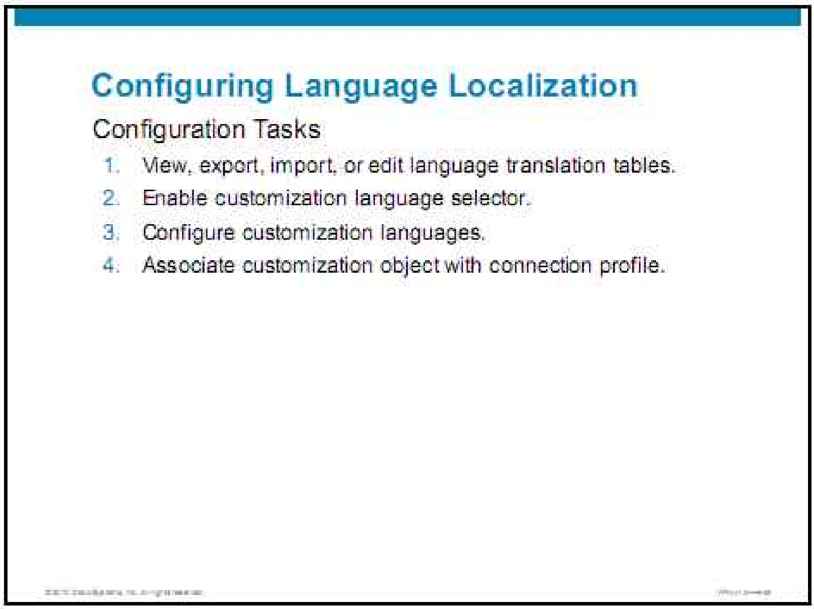
| Translation Domain | Functional Areas Translated |
|---|---|
| AnyConnect | Messages that are displayed on the user interface of the Cisco AnyConnect VPN client |
| CSD | Messages for the Cisco Secure Desktop |
| customization | Messages on the logon and logout pages, portal page, and all the messages customizable by the user |
| keepout | Message that is displayed to remote users when VPN access is denied |
| PortForwarder | Messages that are displayed to port-forwarding users |
| url-list | Text that user specifies for URL bookmarks on the portal page |
| webvpn | All the layer 7, AAA, and portal messages that are not customizable |
| plugin-ica | Messages for the Citrix plug-in |
| plugin-rdp | Messages for the Remote Desktop Protocol plug-in |
| plugin-telnet,ssh | Messages for the Telnet and SSH plug-in |
| plugin-vnc | Messages for the VNC plug-in |

This table lists the available translation domains and provides their description.

### Translation Domains

| Translation Domain | Functional Areas Translated |
|---|---|
| AnyConnect | Messages that are displayed on the user interface of the Cisco AnyConnect VPN client |
| CSD | Messages for the Cisco Secure Desktop |
| customization | Messages on the logon and logout pages, portal page, and all the messages customizable by the user |
| keepout | Message that is displayed to remote users when VPN access is denied |
| PortForwarder | Messages that are displayed to port-forwarding users |
| url-list | Text that user specifies for URL bookmarks on the portal page |
| webvpn | All the Layer 7, AAA, and portal messages that are not customizable |
| plugin-ica | Messages for the Citrix plug-in |
| plugin-rdp | Messages for the Remote Desktop Protocol (RDP) plug-in |
| plugin-telnet,ssh | Messages for the Telnet and SSH plug-in |
| plugin-vnc | Messages for the VNC plug-in |

The software image package for the adaptive security appliance includes a language localization template for each domain that is part of the standard functionality. The templates for plug-ins are included with the plug-ins and define their own translation domains.



## Configuring Language Localization

Configuration Tasks

1. View, export, import, or edit language translation tables.
2. Enable customization language selector.
3. Configure customization languages.
4. Associate customization object with connection profile.

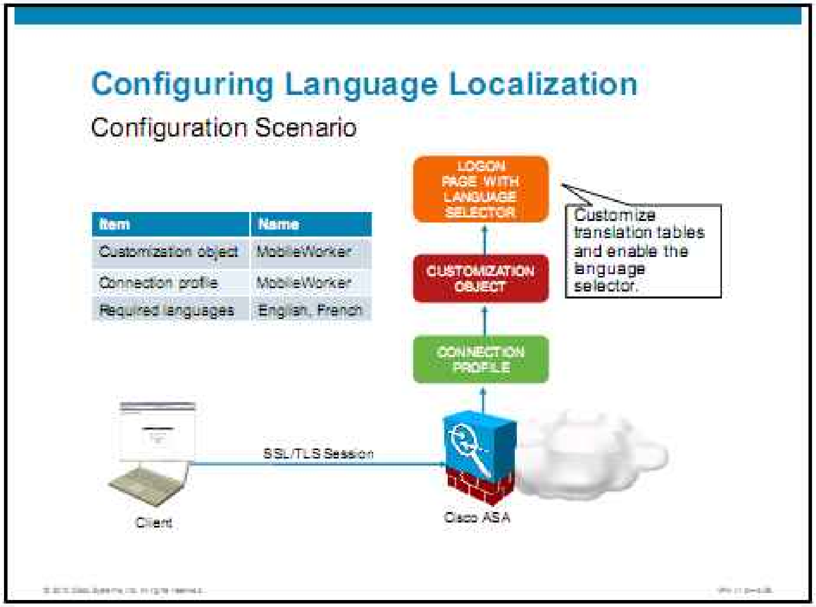
To configure language localization, you will perform the following configuration tasks:

1. View, export, import, or edit language translation tables.

2. Enable a customization language selector.

3. Configure customization languages.

4. Associate a customization object with connection profile.



## Configuring Language Localization

Configuration Scenario

| Item | Name |
|---|---|
| Customization object | MobileWorker |
| Connection profile | MobileWorker |
| Required languages | English, French |

LOGON PAGE WITH LANGUAGE SELECTOR
Customize translation tables and enable the language selector.
CUSTOMIZATION OBJECT
CONNECTION PROFILE
SSL/TLS Session
Client
Cisco ASA

This figure presents the configuration scenario that is used in upcoming configuration tasks.

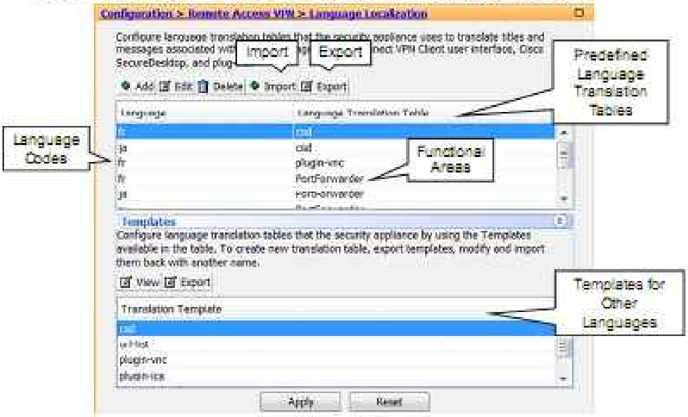
The table lists the input parameters that you will need to gather before deploying language localization. Those parameters include the following:

- **Name of the customization object:** In this example, the name is MobileWorker.
- **Name of the connection profile that must be associated with the customization object:** In this scenario, its name is identical to the customization object.
- **Required languages:** In this example, the languages include English (available by default) and French.

You will associate a connection profile with a specific customization object and configure that object to use a logon page with a language selector. VPN users connecting to the MobileWorker connection profile will see a language selector drop-down box and will be able to select their own language.

## Configuring Language Localization

### Task 1A: View, Import, Export Translation Tables



Configuration > Remote Access VPN > Language Localization

Configure language translation tables that the security appliance uses to translate titles and messages associated with … nect VPN Client user interface, Cisco SecureDesktop, and plug-…

● Add ☑ Edit 🗑 Delete ● Import ☑ Export

| Language | Language Translation Table |
|---|---|
| fr | csd |
| ja | csd |
| fr | plugin-vnc |
| fr | PortForwarder |
| ja | PortForwarder |

Templates

Configure language translation tables that the security appliance by using the Templates available in the table. To create new translation table, export templates, modify and import them back with another name.

☑ View ☑ Export

| Translation Template |
|---|
| csd |
| url-list |
| plugin-vnc |
| plugin-ica |

Import
Export
Predefined Language Translation Tables
Language Codes
Functional Areas
Templates for Other Languages
Apply
Reset

Configuration > Remote Access VPN > Language Localization

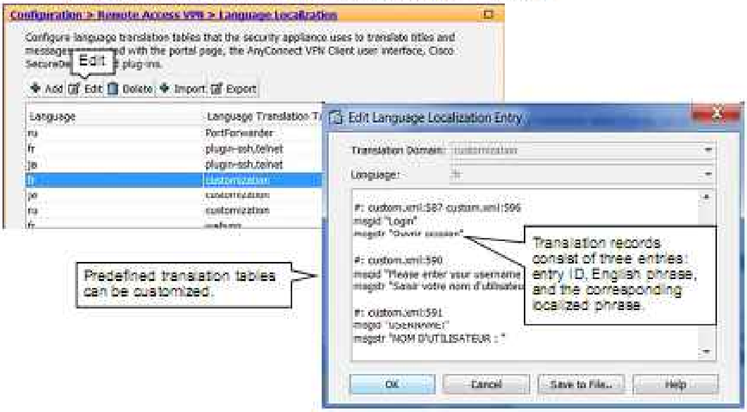
In the first configuration task of this configuration sequence, you will verify the list of preconfigured translation tables and either import or export them into or from the security appliance. These options can be selected if you navigate to the Configuration > Remote Access VPN > Language Localization submenu. The language translation tables are identified by their language code, and the functional area they describe. The lower area of the window contains translation templates that can be exported to create new translation tables on demand.

You can export the template for a translation domain, which creates an XML file of the template at the URL you provide. The message fields are empty in this file. You can customize the messages and import the template to create a new language localization table that resides in flash memory.

You can also export an existing language localization table. The XML file that is created displays the messages that you edited previously. Reimporting this XML file with the same language name creates a new version of the language localization table, overwriting previous messages.

## Configuring Language Localization

### Task 1B: Edit Predefined Translation Table



Configuration > Remote Access VPN > Language Localization

Configure language translation tables that the security appliance uses to translate titles and messages associated with the portal page, the AnyConnect VPN Client user interface, Cisco SecureDesktop and plug-ins.

| Language | Language Translation T... |
|---|---|
| ru | PortForwarder |
| fr | plugin-ssh,telnet |
| ja | plugin-ssh,telnet |
| fr | customization |
| ja | customization |
| ru | customization |
| fr | webvpn |

Edit Language Localization Entry

Translation Domain: customization

Language: fr

```
#: custom.xml:587 custom.xml:596
msgid "Login"
msgstr "Ouvrir session"

#: custom.xml:590
msgid "Please enter your username
msgstr "Saisir votre nom d'utilisateu

#: custom.xml:591
msgid "USERNAME:"
msgstr "NOM D'UTILISATEUR : "
```

Predefined translation tables can be customized.

Translation records consist of three entries: entry ID, English phrase, and the corresponding localized phrase.

Configuration > Remote Access VPN > Language Localization

As an optional part of the first configuration task, you can edit one or more of the existing translation tables.

To modify the existing translation table, complete the following steps:

**Step 1** Choose **Configuration > Remote Access VPN > Language Localization** and select the desired translation table.

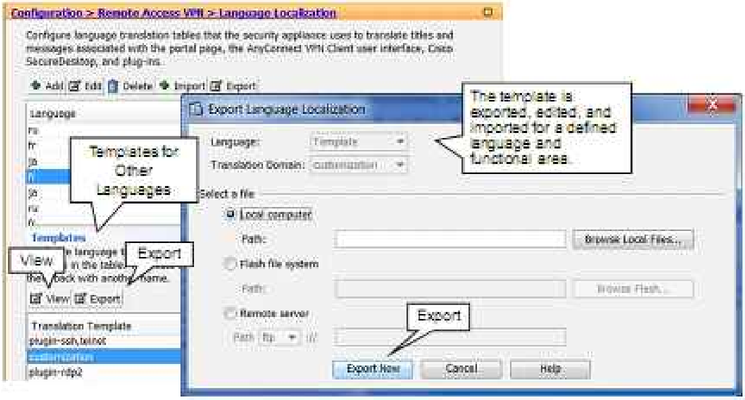
**Step 2** Click **Edit** to edit the translation table.

**Step 3** Update the required records. The translation records include an entry identifier, the English text, and the translated text.

**Step 4** Click **OK**.

## Configuring Language Localization

### Task 1C: Export Template



Configuration > Remote Access VPN > Language Localization

Configure language translation tables that the security appliance uses to translate titles and messages associated with the portal page, the AnyConnect VPN Client user interface, Cisco SecureDesktop, and plug-ins.

Export Language Localization

Language: Template

Translation Domain: customization

Select a file

● Local computer

Path:

○ Flash file system

○ Remote server

Path: ftp ://

The template is exported, edited, and imported for a defined language and functional area.

Configuration > Remote Access VPN > Language Localization

As an optional part of the first configuration task, you can export a language localization template. In the same menu, select a template from the Templates area and click **Export** to save the template as the specified destination file.

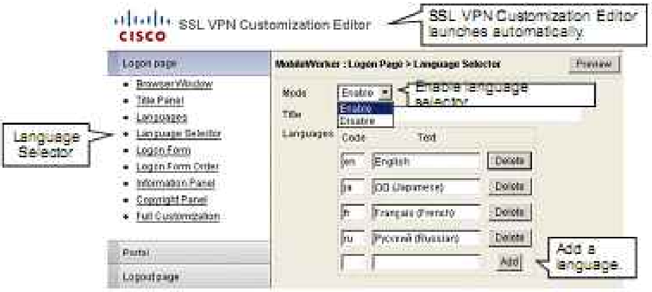
This figure depicts how the View button is used to display the contents of a language localization template for the Customization domain.

After the template is exported, you will edit it and then reimport it into the Cisco ASA adaptive security appliance. The import procedure is invoked using the Import button and requires that you specify the language and functional area that is described by the given translation table.

Some templates are static, but some change based on the configuration of the adaptive security appliance. Because you can customize the logon and logout pages, portal page, and URL bookmarks for clientless sessions, the adaptive security appliance generates the customization and url-list translation domain templates dynamically, and the template automatically reflects your changes to these functional areas.

## Configuring Language Localization

### Task 2: Enable Customization Language Selector



SSL VPN Customization Editor

MobileWorker : Logon Page > Language Selector

Mode: Enable

Title:

Languages:

| Code | Text |
|---|---|
| en | English |
| ja | OO (Japanese) |
| fr | Français (French) |
| ru | Русский (Russian) |

SSL VPN Customization Editor launches automatically.

Enable language selector

Language Selector

Add a language.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization > Edit

After you create language localization tables, they are available to customization objects that you create and apply to group policies or user attributes. A language localization table has no affect and messages are not translated on user screens until you create the customization object, identify a language localization table to use in that object, and specify the customization for the group policy or user.

In the second configuration task, you enable the customization language selector by completing these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access**

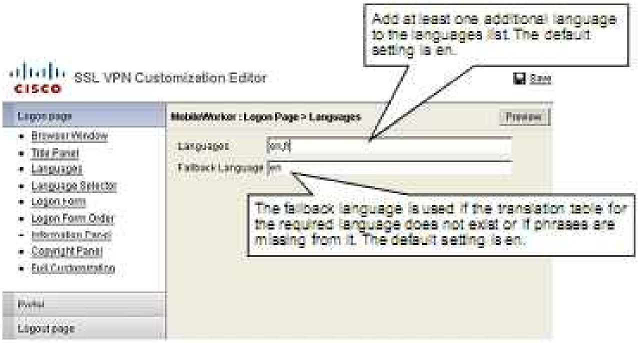
**Step 2** Highlight the desired customization object and click **Edit** to start the SSL VPN Customization Editor.

**Step 3** In the SSL VPN Customization Editor, choose **Logon Page > Language Selector** and choose **Enable** from the Mode drop-down menu.

**Step 4** Edit the languages list by deleting unnecessary languages by clicking the **Delete** button or adding new ones by clicking the **Add** button.

## Configuring Language Localization

### Task 3: Configure Customization Languages



Languages: en,fr

Fallback Language: en

Add at least one additional language to the languages list. The default setting is en.

The fallback language is used if the translation table for the required language does not exist or if phrases are missing from it. The default setting is en.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization > Edit

In the third configuration task, you configure the languages that are used in the customization object by completing these steps:

**Step 1** In the SSL VPN Customization Editor, choose **Logon Page > Languages** and add at least one language code in addition to the default English language (code: en). Use a comma to separate the language codes. This list does not need to include all languages that you want to activate.

**Step 2** Save the settings of the customization object.

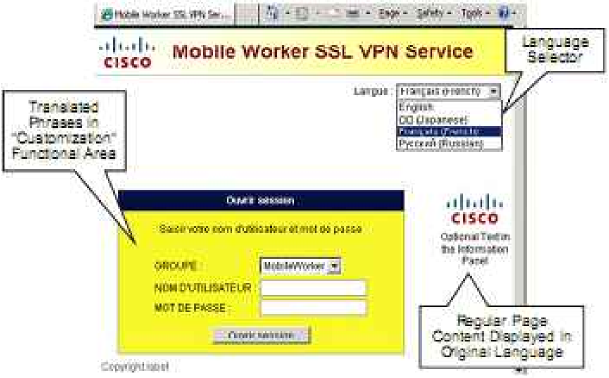
---

**Note** The customization object must be associated with a connection profile. This task is omitted here because it has been shown in earlier configuration procedures.

---

## Verifying Language Localization

Logon Page Verification

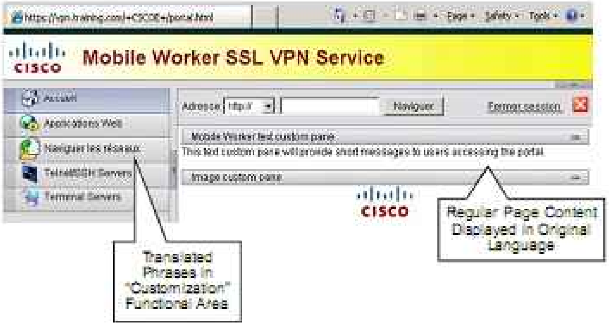


Saisir votre nom d'utilisateur et mot de passe

To verify language localization, connect to the SSL VPN portal using the connection profile that is associated with the tuned customization object. The language selector appears in the upper right corner. After a language is selected, all functional text fields are translated using the appropriate translation tables. This figure illustrates the logon page that is translated into French.

## Verifying Language Localization

Portal Verification


https://vpn.training.com/+CSCOE+/portal.html
Page
Safety
Tools
CISCO
Mobile Worker SSL VPN Service
Accueil
Applications Web
Naviguer les réseaux
Telnet/SSH Servers
Terminal Servers
Adresse
http://
Naviguer
Fermer session
Mobile Worker text custom pane
Image custom pane
CISCO
Translated Phrases in "Customization" Functional Area
Regular Page Content Displayed in Original Language

This text custom pane will provide short messages to users accessing the portal

When the users successfully authenticate, they see the text fields in the portal also translated into their local language. The content of the HTML pages is presented in the language in which it is written.

# Deploying Portal Help Customization

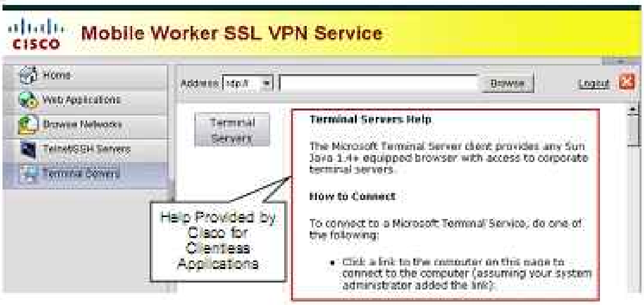
This topic describes how to configure and verify portal help customization.

## Portal Help Customization

Overview

Customization areas

- Customization of help files provided by Cisco
- Creating help files for languages not provided by Cisco



**Terminal Servers Help**

The Microsoft Terminal Server client provides any Sun Java 1.4+ equipped browser with access to corporate terminal servers.

**How to Connect**

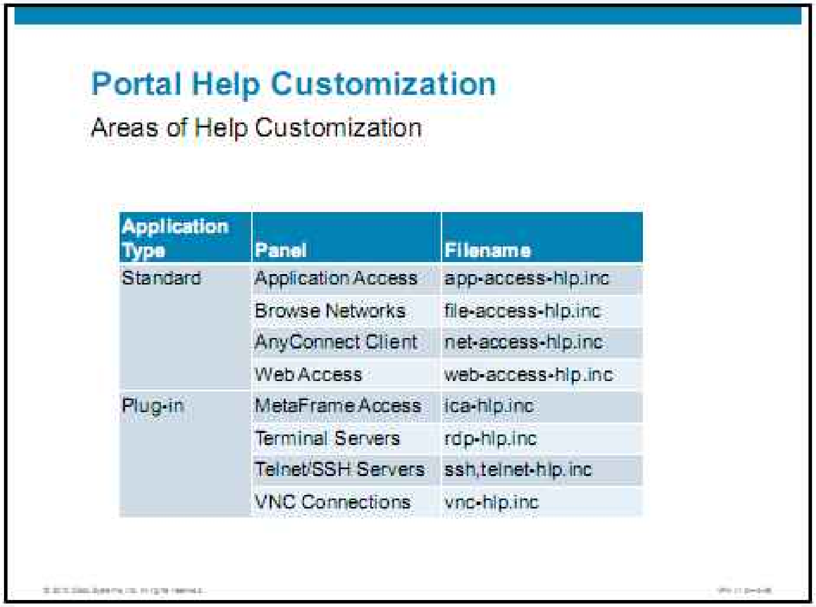
To connect to a Microsoft Terminal Service, do one of the following:

- Click a link to the computer on this page to connect to the computer (assuming your system administrator added the link).

Help Provided by Cisco for Clientless Applications

The Cisco ASA adaptive security appliance displays help content on the application panes during clientless sessions. Each clientless application pane displays its own help file content using a predetermined filename. For example, the help text that is shown in the figure comes from the file rdp-hlp.inc because it displays information that is related to the Terminal Servers plug-in.

You can modify the help files that are preinstalled on the security appliance and create new help files for languages that are not predefined.



## Portal Help Customization

Areas of Help Customization

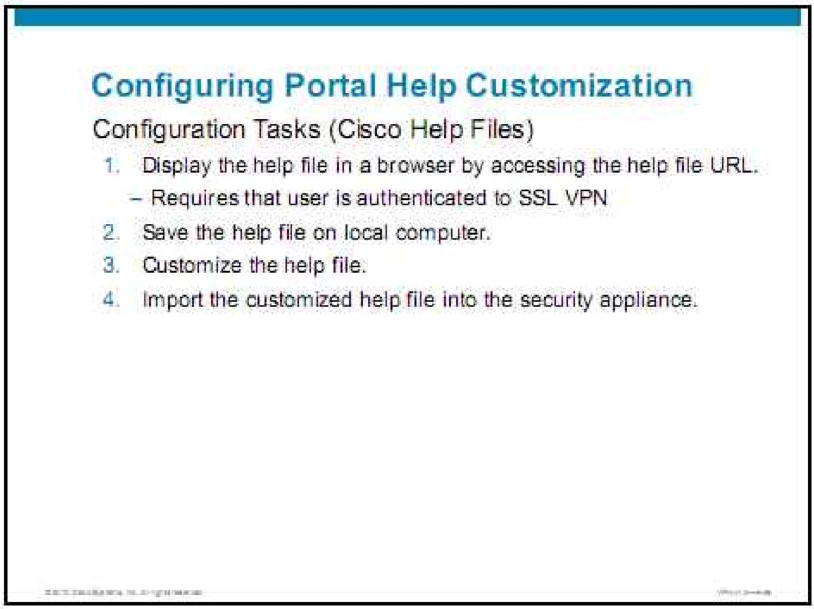
| Application Type | Panel | Filename |
|---|---|---|
| Standard | Application Access | app-access-hlp.inc |
| | Browse Networks | file-access-hlp.inc |
| | AnyConnect Client | net-access-hlp.inc |
| | Web Access | web-access-hlp.inc |
| Plug-in | MetaFrame Access | ica-hlp.inc |
| | Terminal Servers | rdp-hlp.inc |
| | Telnet/SSH Servers | ssh,telnet-hlp.inc |
| | VNC Connections | vnc-hlp.inc |

The help files are organized into functional areas, just as language translation tables are. The table shows the clientless application panels and predetermined filenames for the help content.

**Clientless Application Panels and Predetermined Filenames for the Help Content**

| Application Type | Panel | Filename |
|---|---|---|
| Standard | Application Access | app-access-hlp.inc |
| | Browse Networks | file-access-hlp.inc |
| | AnyConnect Client | net-access-hlp.inc |
| | Web Access | web-access-hlp.inc |
| Plug-in | MetaFrame Access | ica-hlp.inc |
| | Terminal Servers | rdp-hlp.inc |
| | Telnet/SSH Servers | ssh,telnet-hlp.inc |
| | VNC Connections | vnc-hlp.inc |

You can display the help file for an application panel by accessing the SSL VPN server using the help file URL in the format https://<ssl-server>/+CSCOE+/help/language/<filename>, where language is the language code.



## Configuring Portal Help Customization

Configuration Tasks (Cisco Help Files)

1. Display the help file in a browser by accessing the help file URL.
   - Requires that user is authenticated to SSL VPN
2. Save the help file on local computer.
3. Customize the help file.
4. Import the customized help file into the security appliance.

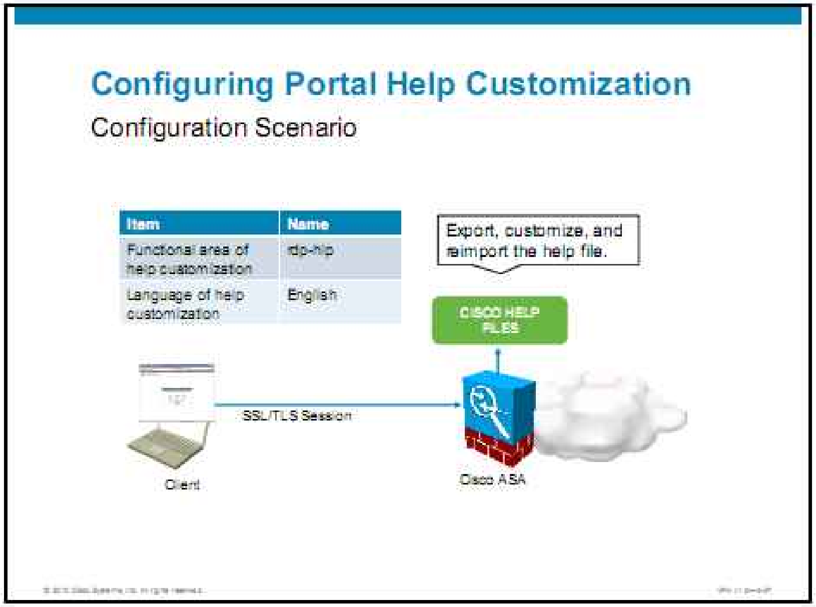
To customize Cisco help files, you will perform the following configuration tasks:

1. Display the help file in a browser by accessing the help file URL. Access to that URL requires that user is successfully authenticated.

2. Save the help file on the local computer.

3. Customize the help file.

4. Import the customized help file into the security appliance.



## Configuring Portal Help Customization

Configuration Scenario

| Item | Name |
|---|---|
| Functional area of help customization | rdp-hlp |
| Language of help customization | English |

Export, customize, and reimport the help file.

This figure presents the configuration scenario that is used in upcoming configuration tasks.

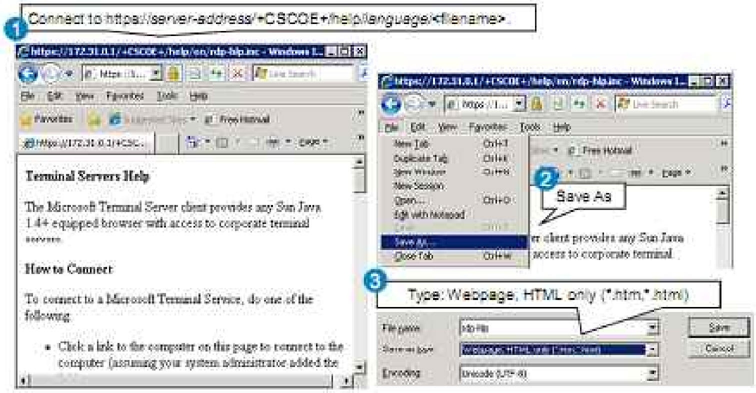
The table lists the input parameters that you will need to gather before performing help file customization. Those parameters include the following:

- Functional area of help customization. In this scenario, you customize the help information for the RDP plug-in.
- Language of help customization. In this scenario, you customize the help file in English.

You obtain the RDP-related help file by connecting to the SSL VPN and then accessing the help file URL. You download the help file to the user PC, modify it, reimport it into the Cisco ASA adaptive security appliance, and verify the results.

## Configuring Portal Help Customization

### Tasks 1-2: Display Help File in Browser and Save



1 Connect to https://server-address/+CSCOE+/help/language/<filename>.

2 Save As

3 Type: Webpage, HTML only (*.htm,*.html)

https://172.31.0.1/+CSCOE+/help/en/rdp-hlp.inc - Windows I...

**Terminal Servers Help**

The Microsoft Terminal Server client provides any Sun Java 1.4+ equipped browser with access to corporate terminal servers.

**How to Connect**

To connect to a Microsoft Terminal Service, do one of the following:

- Click a link to the computer on this page to connect to the computer (assuming your system administrator added the

File name: rdp-hlp

Save as type: Webpage, HTML only (*.htm;*.html)

Encoding: Unicode (UTF-8)

In the first task, you display the desired help file in the client browser by connecting to the URL: https://server-address/+CSCOE+/help/language/<filename>. In this example, the URL was https://172.31.0.1/+CSCOE+/help/en/rdp-hlp.inc

In the second task, you save the help file on the client computer by completing these tasks:

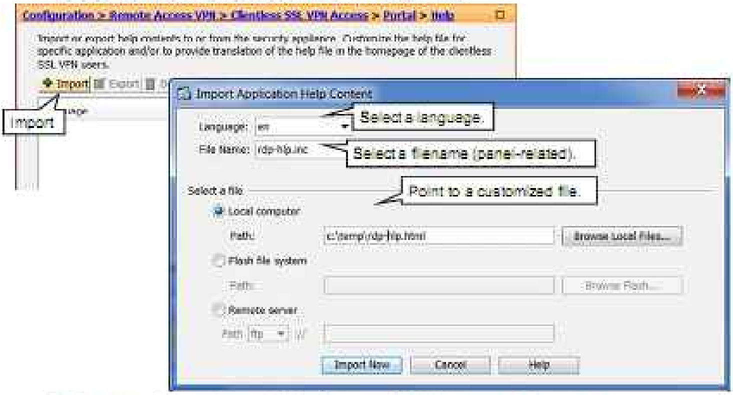
**Step 1** In the browser, choose **File > Save As**. (This menu may differ depending on the browser you use.)

**Step 2** Set the file type to **Webpage, HTML only (*.htm, *.html)** and save.

In the third task (not shown in the figure), you modify the help file according to the requirements.

## Configuring Portal Help Customization

### Task 4: Import Customized Help File



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help

Import or export help contents to or from the security appliance. Customize the help file for specific application and/or to provide translation of the help file in the homepage of the clientless SSL VPN users.

Import Application Help Content

Language: en

File Name: rdp-hlp.inc

Select a file

● Local computer

Path: c:\temp\rdp-hlp.html

○ Flash file system

○ Remote server

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization

In the fourth task, after the help file has been customized, you will import the file into the security appliance:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help**.

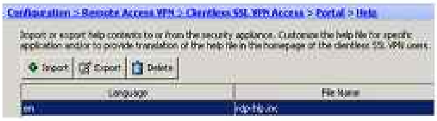
**Step 2** Choose the appropriate language code from the Language drop-down menu.

**Step 3** Choose the appropriate panel from the File Name drop-down menu.

**Step 4** Locate the customized file using a suitable option and click **Import Now**.

## Verifying Portal Help Customization

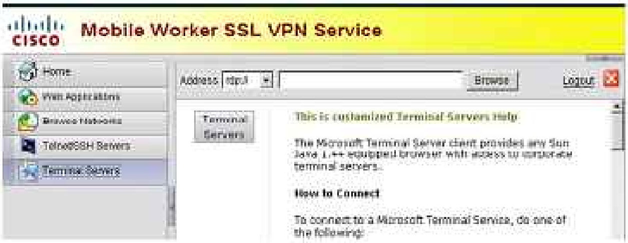
### Portal Help Verification



Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help

Import or export help contents to or from the security appliance. Customize the help file for specific application and/or to provide translation of the help file in the homepage of the clientless SSL VPN users.

| Language | File Name |
|---|---|
| en | rdp-hlp.inc |



This is customized Terminal Servers Help

The Microsoft Terminal Server client provides any Sun Java 1.++ equipped browser with access to corporate terminal servers.

How to Connect

To connect to a Microsoft Terminal Service, do one of the following:

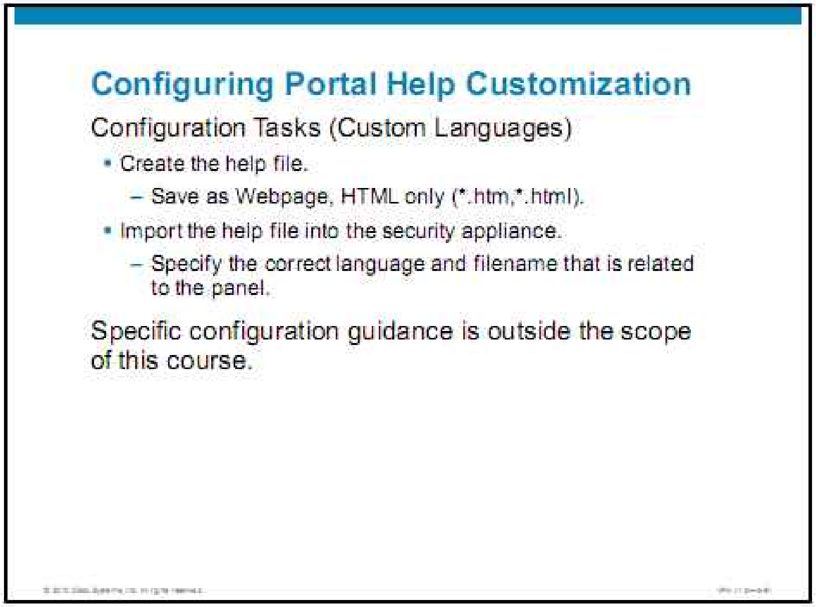
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help Customization

To verify the help file customization, you will first validate that the import procedure was successful by completing these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Help**.

**Step 2** Verify that an entry was created in the help file list. It should specify the configured language code and filename.

To verify the results that are visible to the client, connect to the SSL VPN portal, optionally select the local language, access the appropriate panel, and view the help text. It should reflect the changes that you applied during the file customization.



## Configuring Portal Help Customization

Configuration Tasks (Custom Languages)

- Create the help file.
  - Save as Webpage, HTML only (*.htm,*.html).
- Import the help file into the security appliance.
  - Specify the correct language and filename that is related to the panel.

Specific configuration guidance is outside the scope of this course.

The procedure for creating help files in other languages, not provided by Cisco, represents a subset of the help file customization, because you do not need to obtain the existing help file before customizing it.

Therefore, it consists of two tasks:

1. Create the help file. The file should be saved as Webpage, HTML only (*htm, *.html).

2. Import the customized help file into the security appliance. The import procedure requires that you select the appropriate language code and panel-related filename.

This configuration procedure is not discussed further here, because it contains tasks that have been performed when the help files provided by Cisco were customized.

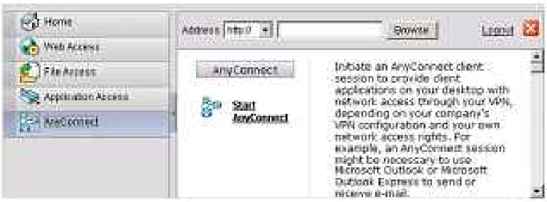
# Cisco AnyConnect Portal Integration

This topic describes how to configure and verify the integration of the clientless SSL VPN portal with the Cisco AnyConnect client.

## Cisco AnyConnect Portal Integration

WebLaunch

- Clientless SSL VPN access can be combined with AnyConnect client.
- AnyConnect panel appears automatically when both access types are enabled.
- Client software can be installed from the portal.



Initiate an AnyConnect client session to provide client applications on your desktop with network access through your VPN, depending on your company's VPN configuration and your own network access rights. For example, an AnyConnect session might be necessary to use Microsoft Outlook or Microsoft Outlook Express to send or receive e-mail.

SSL VPN portal includes the Cisco AnyConnect panel that allows the clients to start the Cisco AnyConnect client from the clientless session that is initiated from the browser. The pane appears in the portal automatically when Cisco AnyConnect access has been enabled on the security appliance.

When users click the Cisco AnyConnect button in the Cisco AnyConnect pane, they trigger one of two actions:

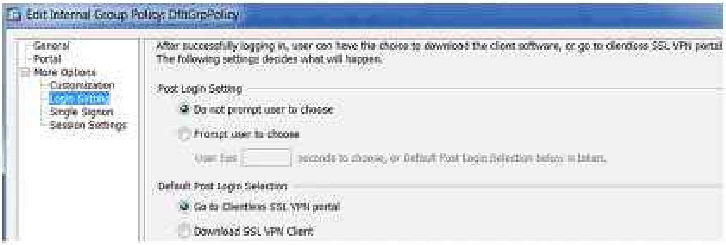
- The Cisco AnyConnect client software is launched if it is installed on the client computer. The Cisco AnyConnect tunnel is established while the clientless session remains active. Only a single SSL VPN license is consumed in this approach.
- If the Cisco AnyConnect client software is not installed on the client computer, the installer is downloaded from the security appliance and the installation procedure begins. When the installation procedure completes, the Cisco AnyConnect tunnel is set up. Also, in this situation, the clientless session remains active and only one license unit is consumed.

## Cisco AnyConnect Portal Integration

Configuring WebLaunch

Configurable behavior after user logs into clientless portal

- Group policy or per-user setting.
- By default, the user remains connected to the clientless portal.
- When the user starts Cisco AnyConnect, the clientless session is active.



Edit Internal Group Policy: DfltGrpPolicy

After successfully logging in, user can have the choice to download the client software, or go to clientless SSL VPN portal
The following settings decides what will happen.

Post Login Setting

● Do not prompt user to choose

○ Prompt user to choose

User has [ ] seconds to choose, or Default Post Login Selection below is taken.

Default Post Login Selection

● Go to Clientless SSL VPN portal

○ Download SSL VPN Client

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

You can configure the security appliance to take certain actions after the user successfully connects to the SSL VPN portal. To configure the postlogin behavior, complete these steps:

**Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies.**

**Note** To assign a postlogin behavior to an individual user, choose **Configuration > Remote Access VPN > AAA/Local Users > Local Users**.

**Step 2** Select a desired group policy and click **Edit.**

**Step 3** Choose **More Options > Login Setting**.

**Step 4** Locate the Post Login Setting area and either leave the default option **Do Not Prompt User to Choose** or choose the option **Prompt User to Choose** and configure the timeout (in seconds) after which the postlogin selection will be made automatically.

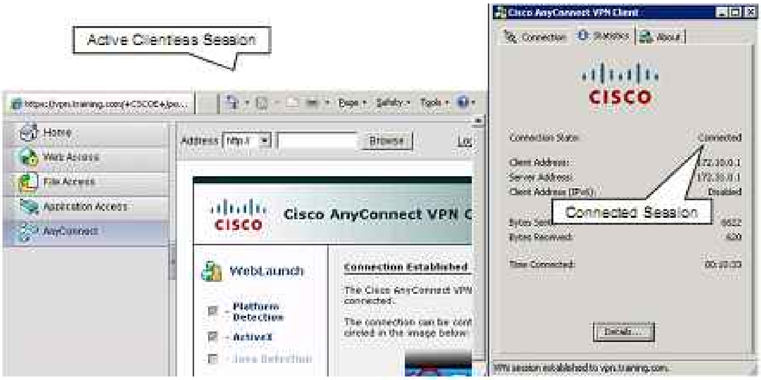
**Step 5** Locate the Default Post Login Selection area and leave the default option **Go to Clientless SSL VPN Portal** or click the **Download SSL VPN Client** radio button. The latter starts the Cisco AnyConnect tunnel, if the client software is already installed on the client computer.

**Step 6** Click **OK**.

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

## Cisco AnyConnect Portal Integration

### Verifying WebLaunch



Active Clientless Session

Connected Session

Cisco AnyConnect VPN Client

Connection State: Connected

Client Address: 172.30.0.1

Server Address: 172.30.0.1

Client Address (IPv6): Disabled

Bytes Sent: 9022

Bytes Received: 420

Time Connected: 00:10:00

VPN session established to vpn.training.com.

https://vpn.training.com/+CSCOE+/po...

Address http:// Browse

Cisco AnyConnect VPN C

WebLaunch

☑ - Platform Detection

☑ - ActiveX

☐ - Java Detection

Connection Established

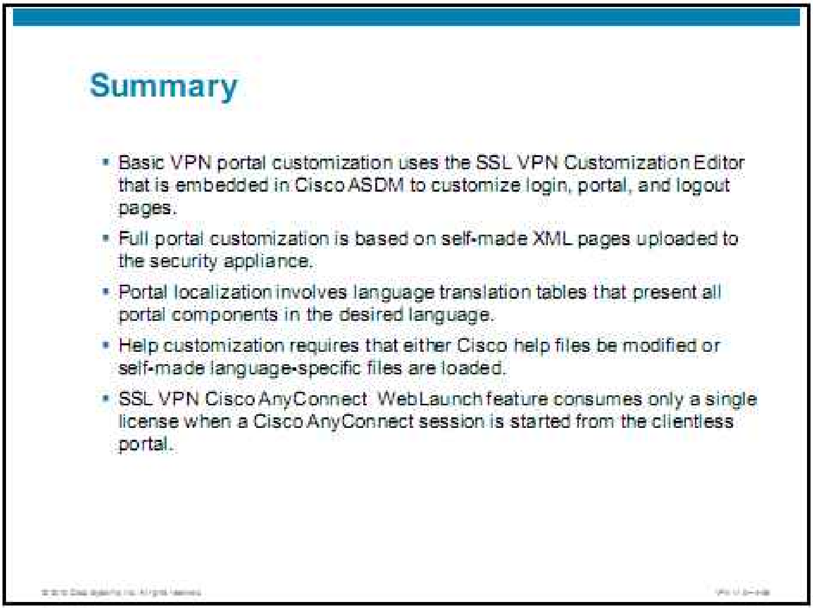
The Cisco AnyConnect VPN connected.

The connection can be cont circled in the image below

You can verify the Cisco AnyConnect WebLaunch feature by accessing the SSL VPN portal and clicking the Cisco AnyConnect button that is available in the Cisco AnyConnect pane. If the Cisco AnyConnect client is already installed on the client computer, the Cisco AnyConnect tunnel will be established. You can verify the tunnel status by examining the Statistics tab of the Cisco AnyConnect client. The browser, from which the clientless SSL VPN was started, displays an indication that the tunnel connection is established. For the license count, it is important that only one session is active at a time. You can verify that only one Cisco AnyConnect session is active in the Monitoring > VPN > VPN Statistics > Sessions submenu. The clientless session does not appear in the session database. Only one license unit is consumed when the Cisco AnyConnect WebLaunch feature is used.

# Summary

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



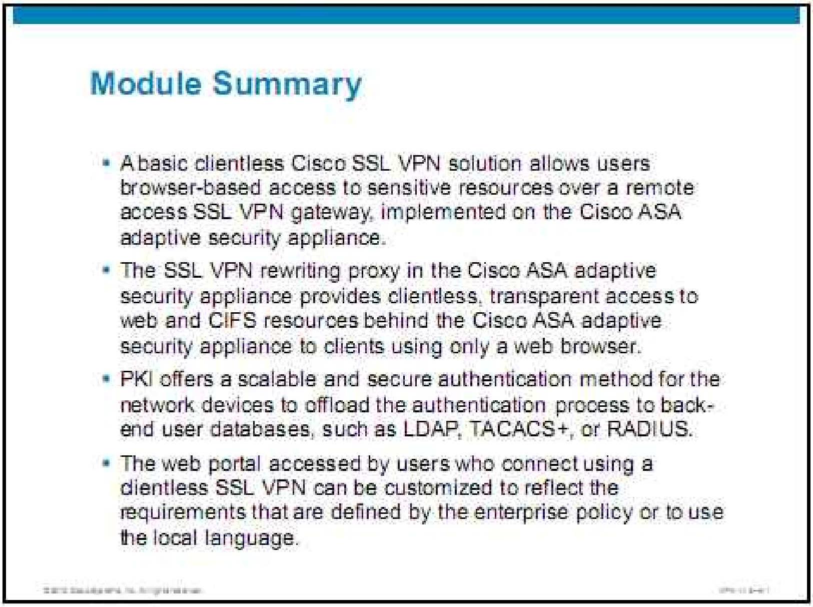
## Summary

- Basic VPN portal customization uses the SSL VPN Customization Editor that is embedded in Cisco ASDM to customize login, portal, and logout pages.
- Full portal customization is based on self-made XML pages uploaded to the security appliance.
- Portal localization involves language translation tables that present all portal components in the desired language.
- Help customization requires that either Cisco help files be modified or self-made language-specific files are loaded.
- SSL VPN Cisco AnyConnect WebLaunch feature consumes only a single license when a Cisco AnyConnect session is started from the clientless portal.

VPN v1.0—4-88

# Module Summary

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



## Module Summary

- A basic clientless Cisco SSL VPN solution allows users browser-based access to sensitive resources over a remote access SSL VPN gateway, implemented on the Cisco ASA adaptive security appliance.
- The SSL VPN rewriting proxy in the Cisco ASA adaptive security appliance provides clientless, transparent access to web and CIFS resources behind the Cisco ASA adaptive security appliance to clients using only a web browser.
- PKI offers a scalable and secure authentication method for the network devices to offload the authentication process to back-end user databases, such as LDAP, TACACS+, or RADIUS.
- The web portal accessed by users who connect using a clientless SSL VPN can be customized to reflect the requirements that are defined by the enterprise policy or to use the local language.