Clientless SSL VPN Users

- Manage Passwords, on page 1
- Use Single Sign-On with Clientless SSL VPN, on page 2
- Use Auto Sign-On , on page 8
- Username and Password Requirements, on page 9
- Communicate Security Tips, on page 10
- Configure Remote Systems to Use Clientless SSL VPN Features, on page 10

Manage Passwords

Optionally, you can configure the ASA to warn end users when their passwords are about to expire.

The ASA supports password management for the RADIUS and LDAP protocols. It supports the "password-expire-in-days" option for LDAP only.

You can configure password management for IPsec remote access and SSL VPN tunnel-groups.

When you configure password management, the ASA notifies the remote user at login that the user's current password is about to expire or has expired. The ASA then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password.

This command is valid for AAA servers that support such notification.

The ASA, releases 7.1 and later, generally supports password management for the following connection types when authenticating with LDAP or with any RADIUS configuration that supports MS-CHAPv2:

- AnyConnect VPN Client
- IPsec VPN Client
- Clientless SSL VPN

The RADIUS server (for example, Cisco ACS) could proxy the authentication request to another authentication server. However, from the ASA perspective, it is talking only to a RADIUS server.

Before you begin

- Native LDAP requires an SSL connection. You must enable LDAP over SSL before attempting to do password management for LDAP. By default, LDAP uses port 636.

- If you are using an LDAP directory server for authentication, password management is supported with the Sun Java System Directory Server (formerly named the Sun ONE Directory Server) and the Microsoft Active Directory.
  - Sun—The DN configured on the ASA to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.
  - Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.
- Some RADIUS servers that support MSCHAP currently do not support MSCHAPv2. This command requires MSCHAPv2 so check with your vendor.
- Password management is *not* supported for any of these connection types for Kerberos/Active Directory (Windows password) or NT 4.0 Domain.
- For LDAP, the method to change a password is proprietary for the different LDAP servers on the market. Currently, the ASA implements the proprietary password management logic only for Microsoft Active Directory and Sun LDAP servers.
- The ASA ignores this command if RADIUS or LDAP authentication has not been configured.

Procedure

Step 1 Navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > Add or Edit > Advanced > General > Password Management**.

Step 2 Click the Enable password management option.

Use Single Sign-On with Clientless SSL VPN

Configure SSO Authentication Using SiteMinder

This section describes configuring the ASA to support SSO with SiteMinder. You would typically choose to implement SSO with SiteMinder if your website security infrastucture already incorporates SiteMinder. With this method, SSO authentication is separate from AAA and happens once the AAA process completes.

Before you begin

- Specifying the SSO server.
- Specifying the URL of the SSO server to which the ASA makes SSO authentication requests.
- Specifying a secret key to secure the communication between the ASA and the SSO server. This key is similar to a password: you create it, save it, and enter it on both the ASA and the SiteMinder policy server using the Cisco Java plug-in authentication scheme.

Optionally, you can do the following configuration tasks in addition to the required tasks:

- Configuring the authentication request timeout.
- Configuring the number of authentication request retries.

Note To configure SSO for a user or group for Clientless SSL VPN access, you must first configure a AAA server, such as a RADIUS or LDAP server.

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode:

webvpn

Step 2 Create an SSO server named Example of type siteminder:

sso-server *name* **type** *type*

Example:

```
ciscoasa(config-webvpn)# sso-server Example type siteminder
```

Step 3 Switch to site minder configuration mode:

config-webvpn-sso-siteminder

Step 4 Specify the authentication URL of the SSO server, as http://www.Example.com/webvpn:

web-agent-url

Example:

```
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.Example.com/webvpn
```

Step 5 Specify a secret key to secure the authentication communication between the ASA and SiteMinder:

policy-server-secret *secret*

You can create a key of any length using any regular or shifted alphanumeric character, but you must enter the same key on both the ASA and the SSO server.

Example:

This creates a secret key AtaL8rD8!.

```
hostname(config-webvpn-sso-siteminder)# policy-server-secret AtaL8rD8!
```

Step 6 Configure the number of seconds before a failed SSO authentication attempt times out:

request-timeout *seconds*

The default number of seconds is 5, and the possible range is 1 to 30.

Example:

This examples changes the number of seconds before a request times out to 8.

```
hostname(config-webvpn-sso-siteminder)# request-timeout 8
```

Step 7 Configures the number of times the ASA retries a failed SSO authentication attempt before the authentication times out:

max-retry-attempts *number*

The default is 3 retry attempts, and the possible range is 1 to 5 attempts.

Example:

This example configures the number of retries to 4.

```
hostname(config-webvpn-sso-siteminder)# max-retry-attempts 4
```

Step 8 Specify the SSO authentication for either a group or a user:

- If specifying authentication for a user.

  username-webvpn

- If specifying authentication for a group.

  group-policy-webvpn

Step 9 Assign the SSO server to the user:

sso-server value *value*

Example:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value Example
```

This example assigns SSO server named Example to the user named Anyuser.

Step 10 Test the SSO server configuration:

test sso-server *server* **username** *username*

Example:

This example tests the SSO server named Example using the username Anyuser.

```
hostname# test sso-server Example username Anyuser
INFO: Attempting authentication request to sso-server Example for user Anyuser
INFO: STATUS: Success
hostname#
```

Add the Cisco Authentication Scheme to SiteMinder

In addition to configuring the ASA for SSO with SiteMinder, you must also configure your CA SiteMinder policy server with the Cisco authentication scheme, a Java plug-in you download from the Cisco website.

Before you begin

Configuring the SiteMinder policy server requires experience with SiteMinder.

Procedure

Step 1 With the SiteMinder Administration utility, create a custom authentication scheme, being sure to use the following specific arguments:

- In the Library field, enter **smjavaapi**.
- In the Secret field, enter the same secret configured on the ASA.

You configure the secret on the ASA using the **policy-server-secret** command at the command-line interface.

- In the Parameter field, enter **CiscoAuthApi**.

Step 2 Using your Cisco.com login, download the file **cisco_vpn_auth.jar** from http://www.cisco.com/cisco/software/navigator.html and copy it to the default library directory for the SiteMinder server. This .jar file is also available on the Cisco ASA CD.

Configure SSO Authentication Using SAML Browser Post Profile

This section describes configuring the ASA to support Security Assertion Markup Language (SAML), Version 1.1 POST profile Single Sign-On (SSO) for authorized users.

After a session is initiated, the ASA authenticates the user against a configured AAA method. Next, the ASA (the asserting party) generates an assertion to the relying party, the consumer URL service provided by the SAML server. If the SAML exchange succeeds, the user is allowed access to the protected resource.

Before you begin

To configure SSO with an SAML Browser Post Profile, you must perform the following tasks:

- Specify the SSO server with the **sso-server** command.
- Specify the URL of the SSO server for authentication requests (the **assertion-consumer-url** command)
- Specify the ASA hostname as the component issuing the authentication request (the **issuer** command)
- Specify the trustpoint certificates use for signing SAML Post Profile assertions (the **trustpoint** command)

Optionally, in addition to these required tasks, you can do the following configuration tasks:

- Configure the authentication request timeout (the **request-timeout** command)
- Configure the number of authentication request retries (the **max-retry-attempts** command)
- SAML SSO is supported only for Clientless SSL VPN sessions.
- The ASA currently supports only the Browser Post Profile type of SAML SSO Server.
- The SAML Browser Artifact method of exchanging assertions is not supported.

Procedure

Step 1 Switch to Clientless SSL VPN configuration mode:

webvpn

Step 2 Create an SSO server:

sso-server type type

Example:

```
hostname(config-webvpn)# sso-server sample type SAML-V1.1-post
```

This example creates an SSO server named Sample of type SAML-V1.1-POST.

Step 3 Switch to Clientless SSL VPN sso-saml configuration mode:

sso saml

Step 4 Specify the authentication URL of the SSO server:

assertion-consumer-url url

Example:

```
hostname(config-webvpn-sso-saml)# assertion-consumer-url http://www.example.com/webvpn
hostname(config-webvpn-sso-saml)#
```

This example sends authentication requests to the URL http://www.Example.com/webvpn.

Step 5 Identify the ASA itself when it generates assertions:

issuer string

Example:

```
hostname(config-webvpn-sso-saml)# issuer myasa
```

Typically, this issuer name is the hostname for the ASA.

Step 6 Specify the identification certificate for signing the assertion:

trust-point

Example:

```
hostname(config-webvpn-sso-saml)# trust-point mytrustpoint
```

Step 7 Configure the number of seconds before a failed SSO authentication attempt times out:

request-timeout

Example:

```
hostname(config-webvpn-sso-saml)# request-timeout 8
```

This example sets the number of seconds before a request times out to 8.

The default number of seconds is 5, and the possible range is 1 to 30 seconds.

Step 8 Configures the number of times the ASA retries a failed SSO authentication attempt before the authentication times out:

max-retry-attempts

Example:

```
hostname(config-webvpn-sso-saml)# max-retry-attempts 4
```

This example sets the number of retries to 4.

The default is 3 retry attempts, and the possible range is 1 to 5 attempts.

Step 9 Switch to Clientless SSL VPN configuration mode:

webvpn

If assigning an SSO server to a group policy.

group-policy-webvpn

If assigning an SSO server to a user policy.

username-webvpn

Step 10 Specify SSO authentication for either a group or a user:

sso-server value

Example:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value sample
```

This example assigns the SSO server named Example to the user named Anyuser.

Step 11 (Privileged exec mode) Test the SSO server configuration:

test sso-server

Example:

```
hostname# test sso-server Example username Anyuser
INFO: Attempting authentication request to sso-server sample for user Anyuser
INFO: STATUS: Success
```

This example tests the SSO server Example using the username Anyuser.

Configure the SAML POST SSO Server

Use the SAML server documentation provided by the server software vendor to configure the SAML server in Relying Party mode.

Procedure

Step 1 Configure the SAML server parameters to represent the asserting party (the ASA):

- Recipient consumer URL (same as the assertion consumer URL configured on the ASA)
- Issuer ID, a string, usually the hostname of appliance
- Profile type -Browser Post Profile

Step 2 Configure certificates.

Step 3 Specify that asserting party assertions must be signed.

Step 4 Select how the SAML server identifies the user:

- Subject Name Type is DN
- Subject Name format is uid=<user>

Use Auto Sign-On

The Auto Sign-on window or tab lets you configure or edit auto sign-on for users of Clientless SSL VPN. Auto sign-on is a simplified single sign-on method that you can use if you do not already have an SSO method deployed on your internal network. With auto sign-on configured for particular internal servers, the ASA passes the login credentials that the user of Clientless SSL VPN entered to log on to the ASA (username and password) to those particular internal servers. You configure the ASA to respond to a specific authentication method for a particular range of servers. The authentication methods you can configure the ASA to respond to consists of authentication using Basic (HTTP), NTLM, FTP and CIFS, or all of these methods.

If the lookup of the username and password fails on the ASA, an empty string is substituted, and the behavior converts back as if no auto sign-on is available.

Auto sign-on is a straight-forward method for configuring SSO for particular internal servers. This section describes the procedure for setting up SSO with auto sign-on. If you already have SSO deployed using Computer Associates SiteMinder SSO server, or if you have Security Assertion Markup Language (SAML) Browser Post Profile SSO. To configure the ASA to support this solution, see SSO Servers.

The following fields are displayed:

- IP Address—In conjunction with the following Mask, displays the IP address range of the servers to be authenticated to as configured with the Add/Edit Auto Sign-on dialog box. You can specify a server using either the server URI or the server IP address and mask.
- Mask—In conjunction with the preceding IP Address, displays the IP address range of the servers configured to support auto sign-on with the Add/Edit Auto Sign-on dialog box.
- URI—Displays a URI mask that identifies the servers configured with the Add/Edit Auto Sign-on dialog box.
- Authentication Type—Displays the type of authentication—Basic (HTTP), NTLM, FTP and CIFS, or all of these methods—as configured with the Add/Edit Auto Sign-on dialog box.

Before you begin

- Do not enable auto sign-on for servers that do not require authentication or that use credentials different from the ASA. When auto sign-on is enabled, the ASA passes on the login credentials that the user entered to log on to the ASA regardless of what credentials are in user storage.
- If you configure one method for a range of servers (for example, HTTP Basic) and one of those servers attempts to authenticate with a different method (for example, NTLM), the ASA does not pass the user login credentials to that server.

Procedure

Step 1 Click to add or edit an auto sign-on instruction. An auto sign-on instruction defines a range of internal servers using the auto sign-on feature and the particular authentication method.

Step 2 Click to delete an auto sign-on instruction selected in the Auto Sign-on table.

Step 3 Click **IP Block** to specify a range of internal servers using an IP address and mask.

- IP Address—Enter the IP address of the first server in the range for which you are configuring auto sign-on.
- Mask—From the subnet mask menu, choose the subnet mask that defines the server address range of the servers supporting auto sign-on.

Step 4 Click URI to specify a server supporting auto sign-on by URI, then enter the URI in the field next to this button.

Step 5 Determine the authentication method assigned to the servers. For the specified range of servers, the ASA can be configured to respond to Basic HTTP authentication requests, NTLM authentication requests, FTP and CIFS authentication requests, or requests using any of these methods.

- Basic—Click this button if the servers support basic (HTTP) authentication.
- NTLM—Click this button if the servers support NTLMv1 authentication.
- FTP/CIFS—Click this button if the servers support FTP and CIFS authentication
- Basic, NTLM, and FTP/CIFS—Click this button if the servers support all of the above.

Username and Password Requirements

Depending on your network, during a remote session users may have to log on to any or all of the following: the computer itself, an Internet service provider, Clientless SSL VPN, mail or file servers, or corporate applications. Users may have to authenticate in many different contexts, requiring different information, such as a unique username, password, or PIN. The following table lists the type of usernames and passwords that Clientless SSL VPN users may need to know:

Login Username/ Password Type		Entered When
Computer	Access the computer	Starting the computer

Login Username/ Password Type		Entered When
Internet Service Provider	Access the Internet	Connecting to an Internet service provider
Clientless SSL VPN	Access remote network	Starting Clientless SSL VPN
File Server	Access remote file server	Using the Clientless SSL VPN file browsing feature to access a remote file server
Corporate Application Login	Access firewall-protected internal server	Using the Clientless SSL VPN Web browsing feature to access an internal protected website
Mail Server	Access remote mail server via Clientless SSL VPN	Sending or receiving email messages

Communicate Security Tips

Advise users to always click the logout icon on the toolbar to close the Clientless SSL VPN session. (Closing the browser window does not close the session.)

Clientless SSL VPN ensures the security of data transmission between the remote PC or workstation and the ASA on the corporate network. Advise users that using Clientless SSL VPN does not ensure that communication with every site is secure. If a user then accesses a non-HTTPS Web resource (located on the Internet or on the internal network), the communication from the corporate ASA to the destination Web server is not private because it is not encrypted.

Configure Remote Systems to Use Clientless SSL VPN Features

This section describes how to set up remote systems to use Clientless SSL VPN.

- About Clientless SSL VPN, on page 11
- Prerequisites for Clientless SSL VPN, on page 11
- Use the Clientless SSL VPN Floating Toolbar, on page 11
- Browse the Web, on page 12
- Browse the Network (File Management), on page 12
- Use Port Forwarding, on page 13
- Use email Via Port Forwarding, on page 15
- Use email Via Web Access, on page 15
- Use email Via email Proxy, on page 15
- Use Smart Tunnel, on page 16

You may configure user accounts differently and different Clientless SSL VPN features can be available to each user.

About Clientless SSL VPN

You can connect to the internet using any supported connection including:

- Home DSL, cable, or dial-ups.
- Public kiosks.
- Hotel hotspots.
- Airport wireless nodes.
- Internet cafes.

Note See the Supported VPN Platforms, Cisco ASA 5500 Series for the list of Web browsers supported by Clientless SSL VPN.

Prerequisites for Clientless SSL VPN

- Cookies must be enabled on the browser in order to access applications via port forwarding.
- You must have a URL for Clientless SSL VPN. The URL must be an https address in the following form: https://*address*, where *address* is the IP address or DNS hostname of an interface of the ASA (or load balancing cluster) on which SSL VPN is enabled. For example, https://cisco.example.com.
- You must have a Clientless SSL VPN username and password.

Note Clientless SSL VPN supports local printing, but it does not support printing through the VPN to a printer on the corporate network.

Use the Clientless SSL VPN Floating Toolbar

A floating toolbar is available to simplify the use of Clientless SSL VPN. The toolbar lets you enter URLs, browse file locations, and choose preconfigured Web connections without interfering with the main browser window.

The floating toolbar represents the current Clientless SSL VPN session. If you click the **Close** button, the ASA prompts you to close the Clientless SSL VPN session.

Tip To paste text into a text field, use Ctrl-V. (Right-clicking is switched off on the toolbar displayed during the Clientless SSL VPN session.)

Note If you configure your browser to block popups, the floating toolbar cannot display.

Browse the Web

Using Clientless SSL VPN does not ensure that communication with every site is secure. See Communicate Security Tips, on page 10.

The look and feel of Web browsing with Clientless SSL VPN may be different from what users are accustomed to. For example:

- The title bar for Clientless SSL VPN appears above each Web page.
- You access websites by:
  - Entering the URL in the **Enter Web Address** field on the Clientless SSL VPN Home page
  - Clicking on a preconfigured website link on the Clientless SSL VPN Home page
  - Clicking a link on a webpage accessed via one of the previous two methods
  - You need the username and password for protected websites

Depending on how you configured a particular account, it may be that:

- Some websites are blocked
- Only the websites that appear as links on the Clientless SSL VPN Home page are available

Also, depending on how you configured a particular account, it may be that:

- Some websites are blocked
- Only the websites that appear as links on the Clientless SSL VPN Home page are available

Browse the Network (File Management)

Users may not be familiar with how to locate their files through your organization network.

Note Do not interrupt the **Copy File to Server** command or navigate to a different screen while the copying is in progress. Interrupting the operation can cause an incomplete file to be saved on the server.

It is important to remember that

- You must configure file permissions for shared remote access.
- You must have the server names and passwords for protected file servers.
- You must have the domain, workgroup, and server names where folders and files reside.

Note Only shared folders and files are accessible via Clientless SSL VPN.

Use the Remote File Explorer

The Remote File Explorer provides the user with a way to browse the corporate network from their Web browser. When the users clicks the Remote File System icon on the Cisco SSL VPN portal page, an applet is launched on the user's system displaying the remote file system in a tree and folder view.

Note This functionality requires that the Oracle Java Runtime Environment (JRE) is installed on the user's machine and that Java is enabled in the Web browser. Launching remote files requires JRE 1.6 or later.

The browser enables the user to:

- Browse the remote file system.
- Rename files.
- Move or copy files within the remote file system and between the remote and local file systems.
- Perform bulk uploads and downloads of files.

  You can download a file by clicking it in the browser, selecting Operations > Download, and providing a location and name to save the file in the Save dialog.

  You can upload a file by clicking the destination folder, selecting Operations > Upload, and providing the location and name of the file in the Open dialog,

  This functionality has the following restrictions:

  - The user cannot view sub-folders for which they are not permitted access.
  - Files that the user is not permitted to access cannot be moved or copied, even though they are displayed in the browser.
  - The maximum depth of nested folders is 32.
  - The tree view does not support drag and drop copying.
  - When moving files between multiple instances of the Remote File Explorer, all instances must be exploring the same server (root share).
  - The Remote File Explorer can display a maximum of 1500 files and folders in a single folder. If a folder exceeds this limit the folder cannot be displayed.

Use Port Forwarding

To use port forwarding, you must configure the client application, using the server's locally mapped IP address and port number.

- Users should always close the Application Access window when they finish using applications by clicking the **Close** icon. Failure to quit the window properly can cause Application Access or the applications themselves to be switched off.

Before you begin

- On Mac OS X, only the Safari browser supports this feature.
- You must have client applications installed.
- You must have Cookies enabled on the browser.
- You must have administrator access on the PC if you use DNS names to specify servers, because modifying the hosts file requires it.
- You must have Oracle Java Runtime Environment (JRE) installed.

  If JRE is not installed, a pop-up window displays, directing users to a site where it is available. On rare occasions, the port forwarding applet fails with Java exception errors. If this happens, do the following:

  1. Clear the browser cache and close the browser.
  2. Verify that no Java icons are in the computer task bar.
  3. Close all instances of Java.
  4. Establish a Clientless SSL VPN session and launch the port forwarding Java applet.

- You must have JavaScript enabled on the browser. By default, it is enabled.
- If necessary, you must configure client applications.

Note The Microsoft Outlook client does not require this configuration step. All non-Windows client applications require configuration. To determine if configuration is necessary for a Windows application, check the value of the Remote Server field. If the Remote Server field contains the server hostname, you do not need to configure the client application. If the Remote Server field contains an IP address, you must configure the client application.

Procedure

Step 1 Start a Clientless SSL VPN session and click the **Application Access** link on the Home page. The Application Access window appears.

Step 2 In the Name column, find the name of the server to use, then identify its corresponding client IP address and port number (in the Local column).

Step 3 Use this IP address and port number to configure the client application. Configuration steps vary for each client application.

Note Clicking a URL (such as one in an -email message) in an application running over a Clientless SSL VPN session does not open the site over that session. To open a site over the session, paste the URL into the Enter Clientless SSL VPN (URL) Address field.

Use email Via Port Forwarding

To use email, start Application Access from the Clientless SSL VPN home page. The mail client is then available for use.

Note If you are using an IMAP client and you lose your mail server connection or are unable to make a new connection, close the IMAP application and restart Clientless SSL VPN.

You must fulfill requirements for application access and other mail clients.

We have tested Microsoft Outlook Express versions 5.5 and 6.0.

Clientless SSL VPN should support other SMTPS, POP3S, or IMAP4S email programs via port forwarding, such as Lotus Notes and Eudora, but we have not verified them.

Use email Via Web Access

The following email applications are supported:

- Microsoft Outlook Web App to Exchange Server 2010.

  OWA requires Internet Explorer 7 or later, or Firefox 3.01 or later.

- Microsoft Outlook Web Access to Exchange Server 2007, 2003, and 2000.

  For best results, use OWA on Internet Explorer 8.x or later, or Firefox 8.x.

- Lotus iNotes

  

  Note You must have the web-based email product installed and other web-based email applications should also work, but we have not verified them.

Use email Via email Proxy

The following legacy email applications are supported:

- Microsoft Outlook 2000 and 2002
- Microsoft Outlook Express 5.5 and 6.0

See the instructions and examples for your mail application in Use Email over Clientless SSL VPN.

Before You Begin

You must have the SSL-enabled mail application installed.

Do not set the ASA SSL version to TLSv1 Only. Outlook and Outlook Express do not support TLS.

You must have your mail application properly configured.

Other SSL-enabled clients should also work, but we have not verified them.

Use Smart Tunnel

Administration privileges are not required to use Smart Tunnel.

Note Java is not automatically downloaded for you as in port forwarder.

- Smart tunnel requires either ActiveX or JRE on Windows and Java Web Start on Mac OS X.
- You must ensure cookies enabled on the browser.
- You must ensure JavaScript is enabled on the browser.
- Mac OS X does not support a front-side proxy.
- Use only supported operating systems and browsers.
- Only TCP socket-based applications are supported.