Clientless SSL VPN Users

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

SSO Using SAML 2.0

About SSO and SAML 2.0

The ASA supports SAML 2.0 so that Clientless VPN end users will be able to input their credentials only one time when they switch between Clientless VPN and other SAAS applications outside of the private network.

For instance, an enterprise customer has enabled PingIdentity as their SAML Identity Provider (IdP) and has accounts on Rally, Salesforce, Oracle OEM, Microsoft ADFS, onelogin, or Dropbox which have been SAML 2.0 SSO enabled. When you configure the ASA to support SAML 2.0 SSO as a Service Provider (SP), end users are able to sign in once and have access to all these services including Clientless VPN.

The ASA is SP enabled when SAML is configured as the authentication method for a tunnel group, the default tunnel group or any other. The Clientless VPN end user initiates Single sign-on by accessing an enabled ASA or the SAML IdP. Each of these scenarios is described below.

SAML SP-initiated SSO

When the end user initiates login by accessing the ASA using Clientless VPN, sign-on behavior proceeds as follows:

1. When the Clientless VPN end user accesses or chooses a SAML enabled tunnel group, the end user will be redirected to the SAML idP for Authentication. The user will be prompted unless the user access the group-url directly, in which case the redirect is silent.

   The ASA generates a SAML Authentication Request which the browser redirects to the SAML IdP.

2. The IdP challenges the end user for credential and the end user logs in. The entered credentials must satisfy the IdP authentication configuration.

3. The IdP Response is sent back to the browser and posted to the ASA's sign-in URL. The ASA verifies the response to complete the login.

SAML IdP-initiated SSL

When the user initiates login by accessing the IdP, sign-on behavior proceeds as follows:

1. An end user accesses the IdP. The IdP challenges the end user for credentials according to the IdP's authentication configuration. The end user submits credentials and logs in to the IdP.
2. In general, the end user gets a list of SAML enabled services that have been configured with the IdP. The end user chooses the ASA.

3. A SAML response is sent back to the browser, and posted to the ASA sign-in URL. The ASA verifies the response to complete the login.

Circle of Trust

The trust relationship between the ASA and the SAML Identity Provider is established through configured certificates (ASA trustpoints).

The trust relationship between the end user and SAML Identity Provider is established through the authentication configured on IdP.

SAML Timeouts

In SAML assertion, there are NotBefore and NotOnOrAfter as follows: <saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

A SAML timeout configured on the ASA will override NotOnOrAfter if the sum of NotBefore and timeout is earlier than NotOnOrAfter. If NotBefore + timeout is later than NotOnOrAfter, then NotOnOrAfter will take effect.

The timeout should be very short to prevent the assertion from being re-used after the timeout. You must synchronize your ASA's Network Time Protocol (NTP) server with the IdP NTP server in order to use the SAML feature.

Guidelines and Limitations for SAML 2.0

- ASA supports the following signatures for SAML authentication:
  - SHA1 with RSA and HMAC
  - SHA2 with RSA and HMAC

- SAML 2.0 SSO support applies to Clientless VPN only. AnyConnect is not supported.
- ASA supports SAML 2.0 Redirect-POST binding , which is supported by all SAML IdPs.
- The ASA functions as a SAML SP only. It cannot act as an Identity Provider in gateway mode or peer mode.
- This SAML SSO SP feature is a mutual exclusion authentication method. It cannot be used with AAA and certificate together.
- Features that are based on username/password authentication, certificate authentication, and KCD are not supported. For instance, username/password pre-filling feature, form-based Auto sign-on, Macro Substitution based Auto sign-on, KCD SSO, and so on.
- Having SAML authentication attributes available in DAP evaluation (similar to RADIUS attributes sent in RADIUS auth response from AAA server) is not supported. ASA supports SAML enabled tunnel-group on DAP policy; however, you cannot check the username attribute while using SAML authentication, because the username attribute is masked by the SAML Identity provider.
- Existing Clientless VPN timeout settings still apply to SAML sessions.
- ASA administrators need to ensure clock synchronization between the ASA and the SAML IdP for proper handling of authentication assertions and proper timeout behavior.
- ASA administrators have the responsibility to maintain a valid signing certificate on both ASA and IdP considering the following:
  - The IdP signing certificate is mandatory when configuring an IdP on the ASA.
  - The ASA does not do a revocation check on the signing certificate received from the IdP.
- In SAML assertions, there are NotBefore and NotOnOrAfter conditions. The ASA SAML configured **timeout** interacts with these conditions as follows:
  - Timeout overrides NotOnOrAfter if the sum of NotBefore and timeout is earlier than NotOnOrAfter.
  - If NotBefore + timeout is later than NotOnOrAfter, then NotOnOrAfter takes effect.
  - If the NotBefore attribute is absent, the ASA denies the login request. If the NotOnOrAfter attribute is absent and SAML timeout is not set, ASA denies the login request.
- ASA does not work with Duo in a deployment using an internal SAML, which forces the ASA to proxy for the client to authenticate, due to the FQDN change that occurs during challenge/response for Two-factor authentication (push, code, password).

Configure a SAML 2.0 Identity Provider (IdP)

Before you begin

Get the Sign-in and Sign-out URLs for your SAML (IdP) provider. You can get the URLs from the provider's website, or they may provide that information in a metadata file.

Procedure

Step 1 In ASDM, go to **Configuration > Remote Access VPN > Clientless SSL VPN Access> Advanced > Single Sign On Servers**

Any previously configured SAML 2.0 IdPs is listed here which you may **Edit** as described next for **Add**, or **Delete**.

Step 2 Click **Add** to add a new IdP entity.

Step 3 Fill in the following fields as described:

- **Sign In URL**—URL for signing into the IdP. The url value must contain 4 to 500 characters.
- **Sign Out URL**—(Optional) URL for redirecting to when signing out of the IdP. The url value must contain 4 to 500 characters.
- **Base URL**—(Optional) URL is provided to third-party IdPs to redirect end-users back to the ASA.

  When base-url is configured, we use it as the base URL of the AssertionConsumerService and SingleLogoutService attribute in **show saml metadata**.

  When base-url is not configured, the URL is determined by the ASA's hostname and domain-name. For example, we use `https://ssl-vpn.cisco.com` when hostname is `ssl-vpn` and domain-name is `cisco.com`.

  An error occurs if neither base-url nor the hostname/domain-name are configured when entering **show saml metadata**.
- **Identity Provider Certificate**—Specifies the trustpoint that contains the IdP certificate for the ASA to verify SAML assertions. Choose a previously configured trustpoint.
- **Service Provider Certificate**—(Optional) Specifies the trustpoint that contains the ASA (SP)'s certificate for the IdP to verify ASA's signature or encrypted SAML assertion. Choose a previously configured trustpoint.
- **Request Timeout**—(Optional) Timeout of the SAML request.

  If specified, this overrides NotOnOrAfter if the sum of NotBefore and timeout-in-seconds is earlier than NotOnOrAfter.

  If not specified, NotBefore and NotOnOrAfter in the assertion is used to determine the validity.
- **Enable the Signature**—Enable or disable (default setting) the signature in SAML request.

Step 4 Click **OK**.
The new IdP entity is listed on this page.

Example

The following web page shows an example of how to get URLs for Onelogin,

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

The following web page is an example of how to use metadata to find the URLs from OneLogin.

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

What to do next

Apply SAML authentication to connection profiles, as described in Configure ASA as a SAML 2.0 Service Provider (SP), on page 6.

Configure ASA as a SAML 2.0 Service Provider (SP)

Follow this procedure to configure a particular tunnel group as a SAML SP.

Note If you are using SAML authentication with AnyConnect 4.4 or 4.5 and you deploy ASA version 9.7.1.24 (or later), 9.8.2.28 (or later), or 9.9.2.1 (or later) (Release Date: 18-APR-2018), the defaulted SAML behavior is the embedded browser, which is not supported on AnyConnect 4.4 and 4.5. Therefore, you must enable the **SAML External Browser** checkbox in the Connection Profiles area so AnyConnect 4.4 and 4.5 clients can authenticate with SAML using the external (native) browser.

The **SAML External Browser** checkbox is for migration purposes for those upgrading to AnyConnect 4.6 or later. Because of security limitations, use this solution only as part of a temporary migration while upgrading AnyConnect software. The checkbox itself will be depreciated in the future.

Procedure

Step 1 In ASDM, go to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > Add/Edit**.

Step 2 Choose **Saml** as the **Authentication Method** for this tunnel group.

Step 3 In the **SAML Identity Provider** section, choose a previously configured **SAML Server**, or click **Manage** to add a new one.
If you modified an existing SAML configuration, this action re-enables the IdP for the tunnel group.

Step 4 Click **OK**.
A Preview CLI Commands window appears that tells you what CLI commands are generated based on the changes you accepted. You can then click **Send** to send the commands to the ASA.

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.

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
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 9

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 8.

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.

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.