# SSL VPN

**First Published: February 27, 2006**
**Last Updated: January 23, 2009**

The SSL VPN feature (also known as WebVPN) provides support, in Cisco IOS software, for remote user access to enterprise networks from anywhere on the Internet. Remote access is provided through a Secure Socket Layer- (SSL-) enabled SSL VPN gateway. The SSL VPN gateway allows remote users to establish a secure Virtual Private Network (VPN) tunnel using a web browser. This feature provides a comprehensive solution that allows easy access to a broad range of web resources and web-enabled applications using native HTTP over SSL (HTTPS) browser support. SSL VPN delivers three modes of SSL VPN access: clientless, thin-client, and full-tunnel client support.

This document is primarily for system administrators. If you are a remote user, see the document *SSL VPN Remote User Guide*.

**Note** The Cisco AnyConnect VPN Client is introduced in Cisco IOS Release 12.4(15)T. This feature is the next-generation SSL VPN Client. If you are using Cisco software before Cisco IOS Release 12.4(15)T, you should be using SSL VPN Client and see GUI for the SSL VPN Client when you are web browsing. However, if you are using Cisco software Release 12.4(15)T or later, you should be using Cisco AnyConnect VPN Client and see GUI for Cisco AnyConnect VPN Client when you are web browsing.

For "What's New" information about SSL VPN features by release, see the section "Finding Feature Information in This Module," which follows.

## Finding Feature Information in This Module

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for SSL VPN" section on page 215.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Contents



# Prerequisites for SSL VPN

- To securely access resources on a private network behind an SSL VPN gateway, the remote user of an SSL VPN service must have the following:
  - An account (login name and password)
  - An SSL-enabled browser (for example, Internet Explorer, Netscape, Mozilla, or FireFox)
  - Operating system support

**Note** Later versions of the following software are also supported.

  - Microsoft Windows 2000, Windows XP, or Windows Vista
  - Macintosh OS X 10.4.6
  - Linux (Redhat RHEL 3.0 +, FEDORA 5, or FEDORA 6)
  - SSL VPN-supported browser—The following browsers have been verified for SSL VPN. Other browsers might not fully support SSL VPN features.

**Note** Later versions of the following software are also supported.

    - Internet Explorer 6.0 or 7.0
    - Firefox 2.0 (Windows and Linux)
    - Safari 2.0.3
- “Thin Client” support used for TCP port-forwarding applications requires administrative privileges on the computer of the remote user.
- “Tunnel mode” for Cisco SSL VPN requires administrative privileges for initial installation of the full tunnel client.
- The remote user must have local administrative privileges to use thin client or full tunnel client features.

- The SSL VPN gateway and context configuration must be completed before a remote user can access resources on a private network behind an SSL VPN. This configuration is shown in the section "How to Configure SSL VPN Services on a Router."

### ACL Support

- Before configuring this feature, the time range should have already been configured.

### Single SignOn (SSO) Netegrity Cookie Support

- A Cisco plug-in must be installed on a Netegrity SiteMinder server.

# Restrictions for SSL VPN

- URLs referred by the Macromedia Flash player cannot be modified for secure retrieval by the SSL VPN gateway.

### Cisco AnyConnect VPN Client

CiscoAnyConnect VPN Client does not support the following:

- Datagram Transport Layer Security (DTLS) with SSL connections
- Standalone Mode
- IPv6 VPN access
- Compression support
- Language Translation (localization)
- Client-side authentication
- Adaptive Security Appliance (ASA) and Adaptive Security Device Manager (ASDM) and any command-line interface (CLI) associated with the them
- Adjusting Maximum Transmission Unit (MTU) size
- Sequencing

### Thin Client Control List Support

- Although there is no limitation on the maximum number of filtering rules that can be applied for each access control list (ACL) entry, keeping the number below 50 should have no impact on router performance.

### HTTP Proxy

- This feature works only with Microsoft Internet Explorer.
- This feature will not work if the browser proxy setup cannot be modified because of any security policies that have been placed on the client workstation.

# Information About SSL VPN

To configure SSL VPN, you should understand the following concepts:

- SSL VPN Overview, page 4
- Modes of Remote Access, page 5

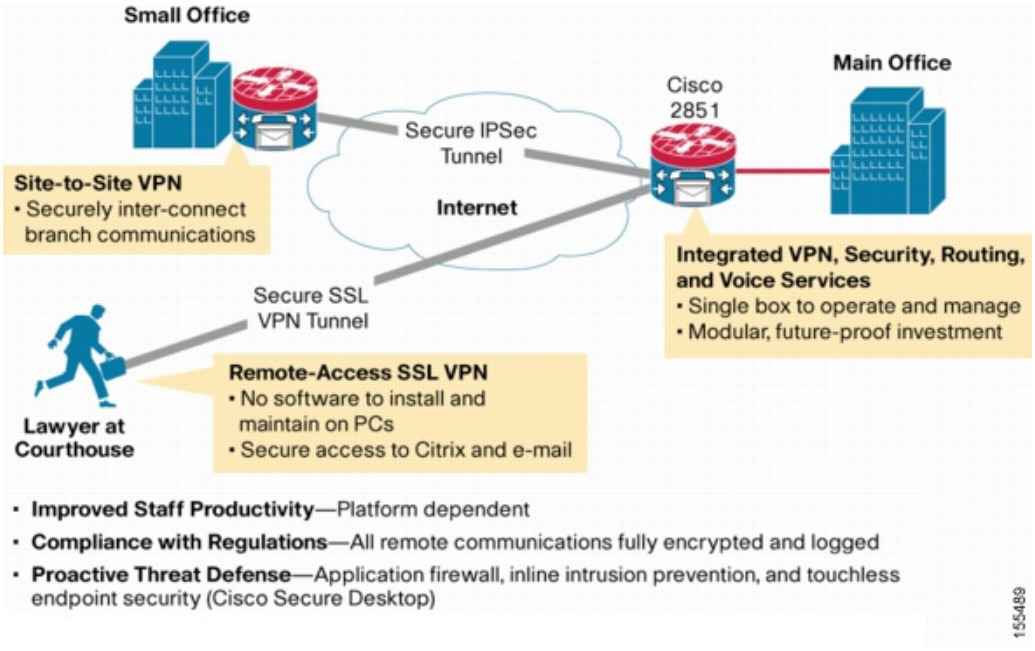
# SSL VPN Overview

Cisco IOS SSL VPN provides SSL VPN remote-access connectivity from almost any Internet-enabled location using only a web browser that natively supports SSL encryption. This feature allows your company to extend access to its secure enterprise network to any authorized user by providing remote-access connectivity to corporate resources from any Internet-enabled location.

Cisco IOS SSL VPN can also support access from noncorporate-owned machines, including home computers, Internet kiosks, and wireless hot spots. These locations are difficult places to deploy and manage VPN client software and remote configuration required to support IPsec VPN connections.

Figure 1 shows how a mobile worker (the lawyer at the courthouse) can access protected resources from the main office and branch offices. Site-to-site IPsec connectivity between the main and remote sites is unaltered. The mobile worker needs only Internet access and supported software (web browser and operating system) to securely access the corporate network.

***Figure 1 Secure SSL VPN Access Model***



SSL VPN delivers the following three modes of SSL VPN access:

- *Clientless*—Clientless mode provides secure access to private web resources and will provide access to web content. This mode is useful for accessing most content that you would expect to access in a web browser, such as Internet access, databases, and online tools that employ a web interface.
- *Thin Client* (port-forwarding Java applet)—Thin client mode extends the capability of the cryptographic functions of the web browser to enable remote access to TCP-based applications such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, and Secure Shell (SSH).
- *Tunnel Mode*—Full tunnel client mode offers extensive application support through its dynamically downloaded Cisco AnyConnect VPN Client (next-generation SSL VPN Client) for SSL VPN. Full tunnel client mode delivers a lightweight, centrally configured and easy-to-support SSL VPN tunneling client that provides network layer access to virtually any application.

SSL VPN application accessibility is somewhat constrained relative to IPsec VPNs; however, SSL-based VPNs provide access to a growing set of common software applications, including web page access, web-enabled services such as file access, e-mail, and TCP-based applications (by way of a downloadable thin-client applet). SSL-based VPN requires slight changes to user workflow because some applications are presented through a web browser interface, not through their native GUI. The advantage for SSL VPN comes from accessibility from almost any Internet-connected system without needing to install additional desktop software.

# Modes of Remote Access

This section includes the following:



## Remote Access Overview

End-user login and authentication is performed by the web browser to the secure gateway using an HTTP request. This process creates a session that is referenced by a cookie. After authentication, the remote user is shown a portal page that allows access to the SSL VPN networks. All requests sent by the browser include the authentication cookie. The portal page provides all the resources available on the internal networks. For example, the portal page could provide a link to allow the remote user to download and install a thin-client Java applet (for TCP port forwarding) or a tunneling client.

Figure 2 shows an overview of the remote access modes.

*Figure 2 Modes of Remote Access Overview*

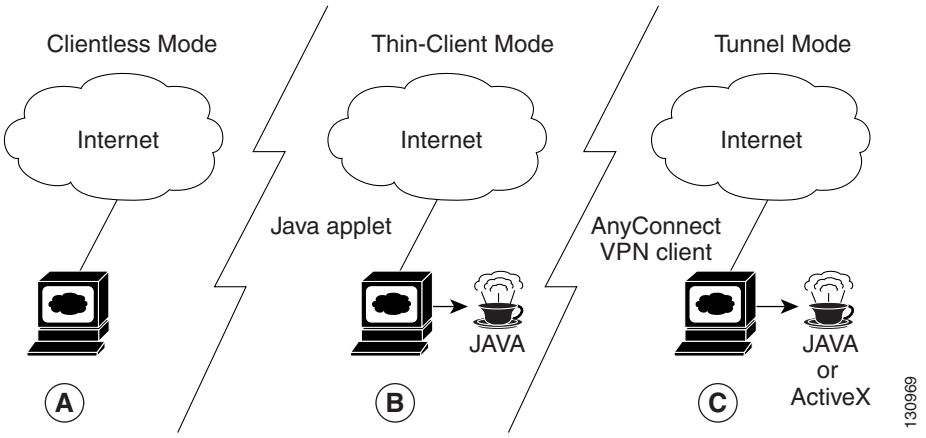



Table 1 summarizes the level of SSL VPN support that is provided by each access mode.

*Table 1 Access Mode Summary*

| A | Clientless Mode | B | Thin-Client Mode | C | Tunnel Mode |
|---|---|---|---|---|---|
| • Browser-based (clientless)<br>• Microsoft Windows or Linux<br>• Web-enabled applications, file sharing, Outlook Web Access<br>• Gateway performs address or protocol conversion and content parsing and rewriting | | • TCP port forwarding<br>• Uses Java Applet<br>• Extends application support<br>• Telnet, e-mail, SSH, Meeting Maker, Sametime Connect<br>• Static port-based applications | | • Works like “clientless” IPsec VPN<br>• Tunnel client loaded through Java or ActiveX (approximately 500 kB)<br>• Application agnostic—supports all IP-based applications<br>• Scalable<br>• Local administrative permissions required for installation | |

## Clientless Mode

In clientless mode, the remote user accesses the internal or corporate network using the web browser on the client machine. The PC of the remote user must run the Windows 2000, Windows XP, or Linux operating systems.

The following applications are supported in clientless mode:

- Web browsing (using HTTP and secure HTTP [HTTPS])—provides a URL box and a list of web server links in the portal page that allows the remote user to browse the web.
- File sharing (using common Internet file system [CIFS])—provides a list of file server links in the portal page that allows the remote user to do the following operations:
  - Browse a network (listing of domains)
  - Browse a domain (listing of servers)
  - Browse a server (listing of shares)
  - List the files in a share

  - Create a new file
  - Create a directory
  - Rename a directory
  - Update a file
  - Download a file
  - Remove a file
  - Rename a file

**Note** Linux requires that the Samba application is installed before CIFS file shares can be remotely accessed.

- Web-based e-mail, such as Microsoft Outlook Web Access (OWA) 2003 (using HTTP and HTTPS) with Web Distributed Authoring and Versioning (WebDAV) extensions—provides a link that allows the remote user to connect to the exchange server and read web-based e-mail.

## Thin-Client Mode

Thin-client mode, also called TCP port forwarding, assumes that the client application uses TCP to connect to a well-known server and port. In thin-client mode, the remote user downloads a Java applet by clicking the link provided on the portal page, or the Java applet is downloaded automatically (see "Options for Configuring HTTP Proxy and the Portal Page" and "Options for Configuring HTTP Proxy and the Portal Page"). The Java applet acts as a TCP proxy on the client machine for the services that you configure on the gateway.

The applications that are supported in thin-client mode are mainly e-mail-based (SMTP, POP3, and Internet Map Access Protocol version 4 [IMAP4] applications.

**Note** The TCP port-forwarding proxy works only with the Sun MicroSystems Java Runtime Environment (JRE) version 1.4 or later versions. A Java applet is loaded through the browser that verifies the JRE version. The Java applet will refuse to run if a compatible JRE version is not detected.

The Java applet initiates an HTTP request from the remote user client to the SSL VPN gateway. The name and port number of the internal e-mail server is included in the HTTP request (POST or CONNECT). The SSL VPN gateway creates a TCP connection to that internal e-mail server and port.

The Java applet starts a new SSL connection for every client connection.

You should observe the following restrictions when using thin-client mode:

- The remote user must allow the Java applet to download and install.
- You cannot use thin-client mode for applications such as FTP, where the ports are negotiated dynamically. You can use TCP port forwarding only with static ports.

**Note** There is a known compatibility issue with the encryption type and Java. If the Java port-forwarding applet does not download properly and the configuration line **ssl encryption 3des-sha1 aes-sha1** is present, you should remove the line from the webvpn gateway subconfiguration.

## Options for Configuring HTTP Proxy and the Portal Page

Effective with Cisco IOS Release 12.4(11)T, administrators have more options for configuring the HTTP proxy and the portal page. If HTTP proxy is enabled, the Java applet acts as the proxy for the browser of the user, thereby connecting the client workstation with the gateway. The home page of the user (as defined by the user group) is opened automatically or, if configured by the administrator, the user is directed to a new website.

HTTP proxy supports both HTTP and HTTPS.

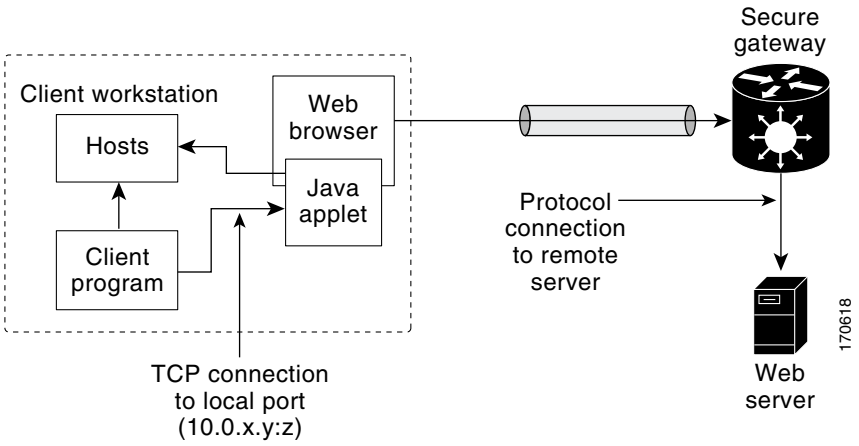
### Benefits of Configuring HTTP Proxy

HTTP supports all client-side web technologies (including HTML, Cascading Style Sheets [CSS], JavaScript, VBScript, ActiveX, Java, and flash), HTTP Digest authentication, and client certificate authentication. Remote users can use their own bookmarks, and there is no limit on cookies. Because there is no mangling involved and the client can cache the objects, performance is much improved over previous options for configuring the HTTP proxy and portal page.

### Illustrations of Port Forwarding with and Without an HTTP Proxy Configuration

Figure 3 illustrates TCP port forwarding without HTTP proxy configured.

***Figure 3 TCP Port Forwarding Without HTTP Proxy Configured***



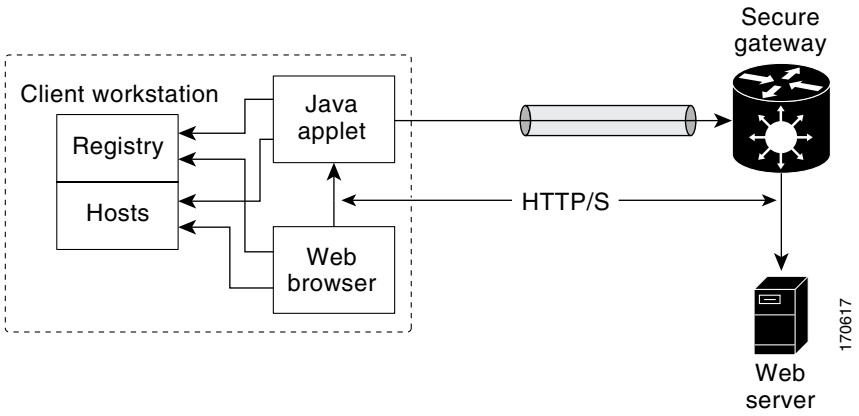

In Figure 3, the following steps must occur:

1. User downloads the proxy applet.
2. Applet updates the registry to add HTTP as a Remote Procedure Call (RPC) transport.
3. Applet examines the registry to determine the exchange (and local catalog) server and create server entries that refer to those servers.
4. Applet opens local port 80 and listens for connections.
5. User starts Outlook, and Outlook connects to 10.0.0.254:80.
6. Applet opens a connection to the secure gateway and delivers the requests from Outlook.
7. Secure gateway examines the requests to determine the end-point exchange server.
8. Data flows from Outlook, through the applet and the secure gateway, to the exchange server.
9. User terminates Outlook.

10. User closes the applet. Before closing, the applet undoes configuration Steps 3 and 4.

Figure 4 illustrates TCP port forwarding when HTTP proxy is configured.

***Figure 4 HTTP Proxy***




In Figure 4, the following steps occur:

1. Proxy applet is downloaded automatically.
2. Applet saves the original proxy configuration of the browser.
3. Applet updates the proxy configuration of the browser to be the local loopback address with an available local port (by default, port 8080).
4. Applet opens the available local port and listens for connections.
5. Applet, if so configured, opens the home page of the user, or the user browses to a new website.
6. Applet accepts and looks at the HTTP or HTTPS request to determine the destination web server.
7. Applet opens a connection to the secure gateway and delivers the requests from the browser.
8. Secure gateway examines the requests to determine the end-point web server.
9. Data flows from the browser, through the applet and the secure gateway, to the web server.
10. User closes applet. Before closing, the applet undoes configuration Steps 2 and 3.

**Note** HTTP proxy can also be enabled on a AAA server. See the section "SSL VPN RADIUS Attribute-Value Pairs" (port-forward-http-proxy and port-forward-http-proxy-url attributes).

## Tunnel Mode

In a typical clientless remote access scenario, remote users establish an SSL tunnel to move data to and from the internal networks at the application layer (for example, web and e-mail). In tunnel mode, remote users use an SSL tunnel to move data at the network (IP) layer. Therefore, tunnel mode supports most IP-based applications. Tunnel mode supports many popular corporate applications (for example, Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail, and Telnet).

The tunnel connection is determined by the group policy configuration. The Cisco AnyConnect VPN Client is downloaded and installed on the remote user PC, and the tunnel connection is established when the remote user logs into the SSL VPN gateway.

By default, the Cisco AnyConnect VPN Client is removed from the client PC after the connection is closed. However, you have the option to keep the Cisco AnyConnect VPN Client installed on the client PC.

# SSL VPN Features

SSL VPN includes the following features:



## Application ACL Support

Effective with Cisco IOS Release 12.4(11)T, this feature provides administrators with the flexibility to fine-tune access control on the application layer level, for example, on the basis of a URL.

For information about configuring this feature, see the sections "Configuring ACL Rules" and "Associating an ACL Attribute with a Policy Group."

## Automatic Applet Download

Effective with Cisco IOS Release 12.4(9)T, administrators have the option of automatically downloading the port-forwarding Java applet. This feature must be configured on a group policy basis.

**Note** Users still have to allow the Java applet to be downloaded. The dialog box pops up, asking for permission.

To configure the automatic download, see the section "Configuring an SSL VPN Policy Group."

## Front-Door VRF Support

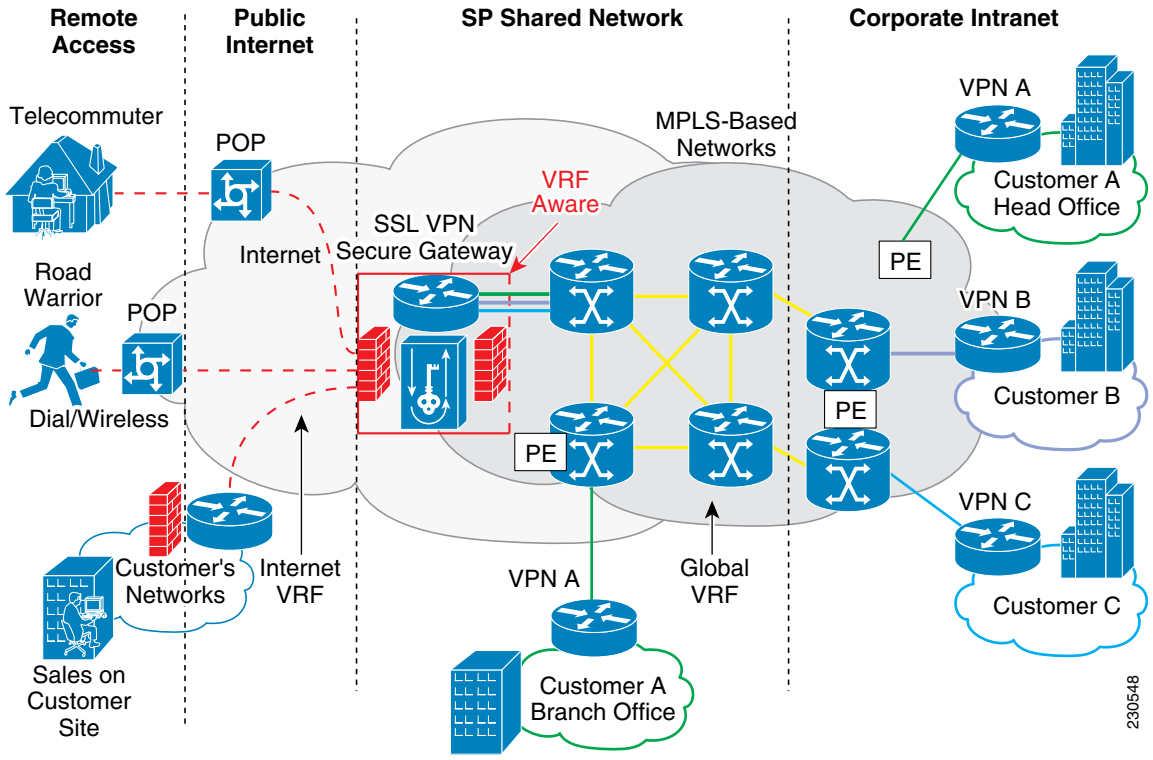
Effective with Cisco IOS Release 12.4(15)T, front-door virtual routing and forwarding (FVRF) support, coupled with the already supported internal virtual routing and forwarding (IVRF), provides for increased security. The feature allows the SSL VPN gateway to be fully integrated into a Multiprotocol Label Switching (MPLS) or non-MPLS network (wherever the VRFs are deployed). The virtual gateway can be placed into a VRF that is separate from the Internet to avoid internal MPLS and IP network

exposure. This placement reduces the vulnerability of the router by separating the Internet routes or the global routing table. Clients can now reach the gateway by way of the FVRF, which can be separate from the global VRF. The backend, or IVRF, functionality remains the same.

This FVRF feature provides for overlapping IP addresses.

Figure 5 is a scenario in which FVRF has been applied.

***Figure 5 Scenario in Which FVRF Has Been Applied***




To configure FVRF, see "Configuring FVRF" section on page 73.

## GUI Enhancements

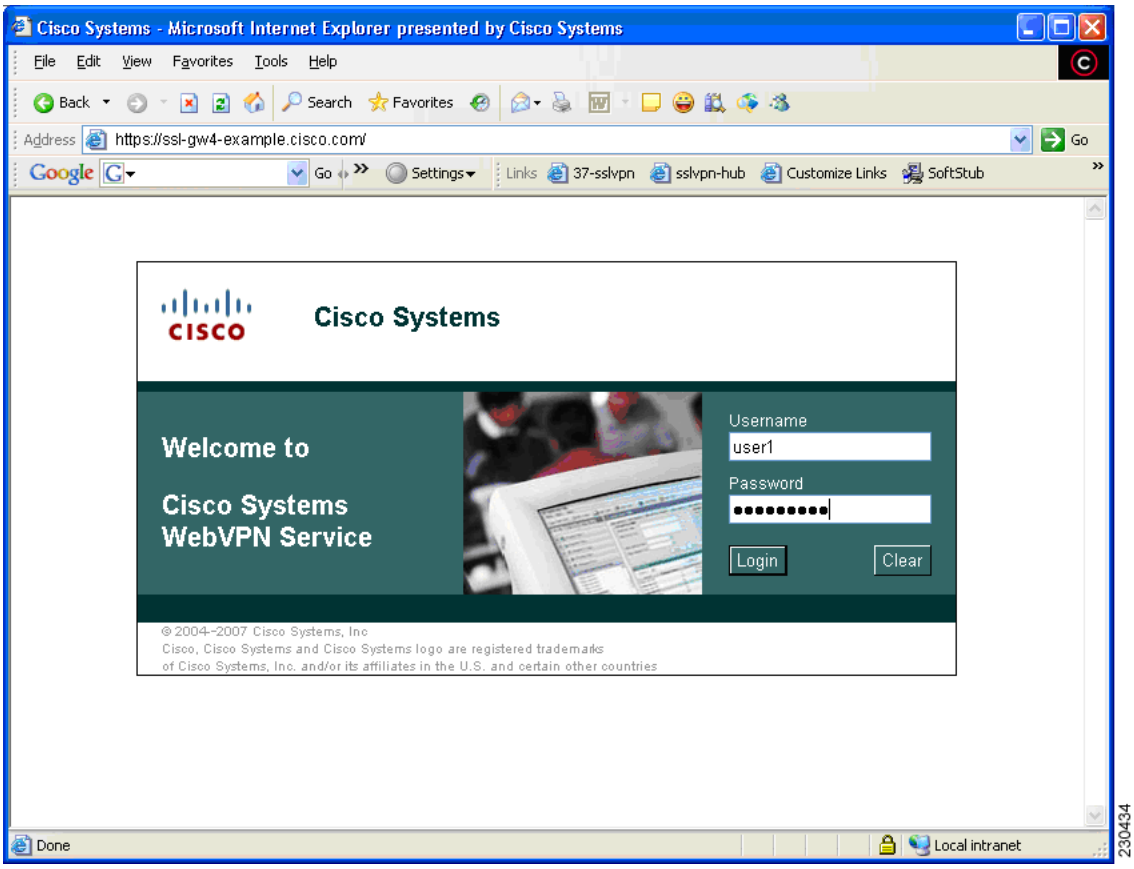
In Cisco IOS Release 12.4(15)T, ergonomic improvements were made to the GUI user interface of the Cisco IOS SSL VPN gateway. The improved customization of the user interface provides for greater flexibility and the ability to tailor portal pages for individualized looks. Enhancements were made to the following web screens:

- Login screen
- Portal page

### Login Screen

Figure 6 is an example of a typical login screen.

*Figure 6 Typical Login Screen*




## Banner

The banner is a small pop-up box (see Figure 7) that appears after the user is logged in and before the portal page appears.

The message in the pop-up box is configured using the **banner** command.

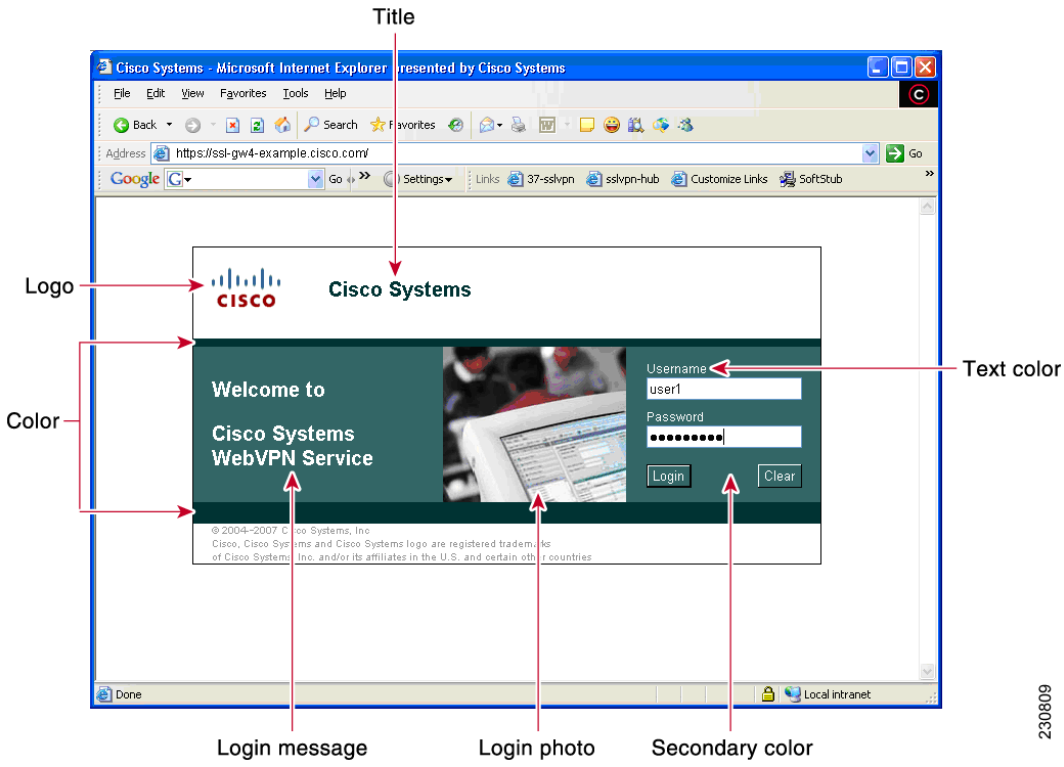
*Figure 7 Banner*

## Customizing a Login Page

Login screens can be customized by an administrator. Figure 8 shows the fields that can be customized.

For information about setting various elements of the login page, see the document *Cisco IOS Security Command Reference*, Release 12.4T, for the **logo**, **title**, **title-color**, **login-message**, **text-color**, **secondary-color**, **login-photo**, and **color** commands.

***Figure 8 Login Page with Callouts of the Fields That Can Be Customized***




## Portal Page

The portal page (Figure 9) is the main page for the SSL VPN functionality. You can customize this page to contain the following:

- Custom logo (the default is the Cisco bridge logo)
- Custom title (the default is “WebVPN Services”)
- Custom banner (the default is an empty string)
- Custom colors (the default is a combination of white and greens)
- List of web server links (can be customized)

**Note** The Bookmark links are listed under the Personal folder, and the server links are listed under Network File in Figure 9.

- URL entry box (may be present or can be hidden using the **hide-url-bar** command)
- Thin Client link (may or may not be present)

**Note** The Application Access box allows you to download and install the Tunnel Connection and Thin Client Application.

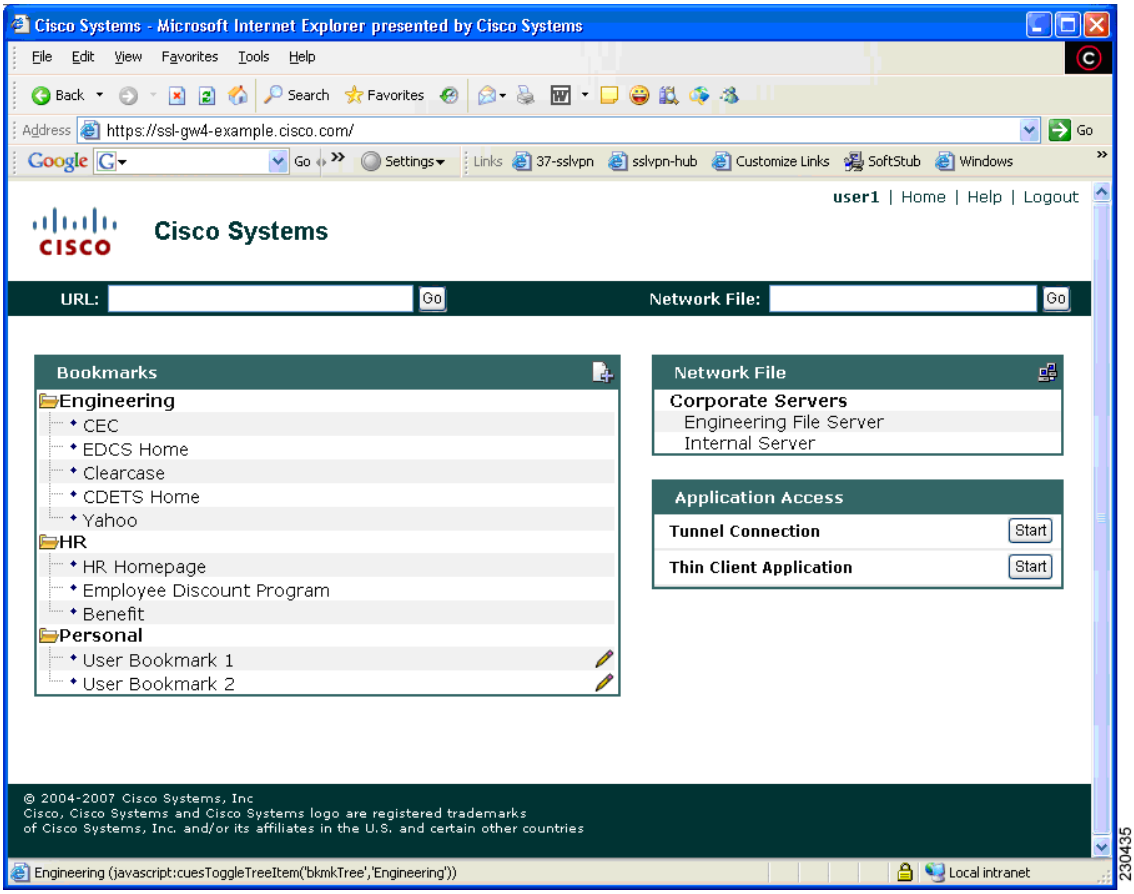
- Links for Help, Home (that is, the portal page), and Logout

Items that you have not configured are not displayed on the portal page.

**Note** E-mail access is supported by thin-client mode, which is downloaded using the Thin Client link.

Figure 9 is an example of a typical portal page.

***Figure 9 Typical Portal Page***




### Customizing a Portal Page

Portal pages can be customized by an administrator. Figure 10 shows various fields, including the fields that can be customized by an administrator. The fields that can be customized by an administrator are as follows:

- Title
- Logo
- Secondary color
- Administrator-defined bookmarks
- Color

***Figure 10 Portal Page with Callouts of Various Fields, Including Those That Can Be Customized***

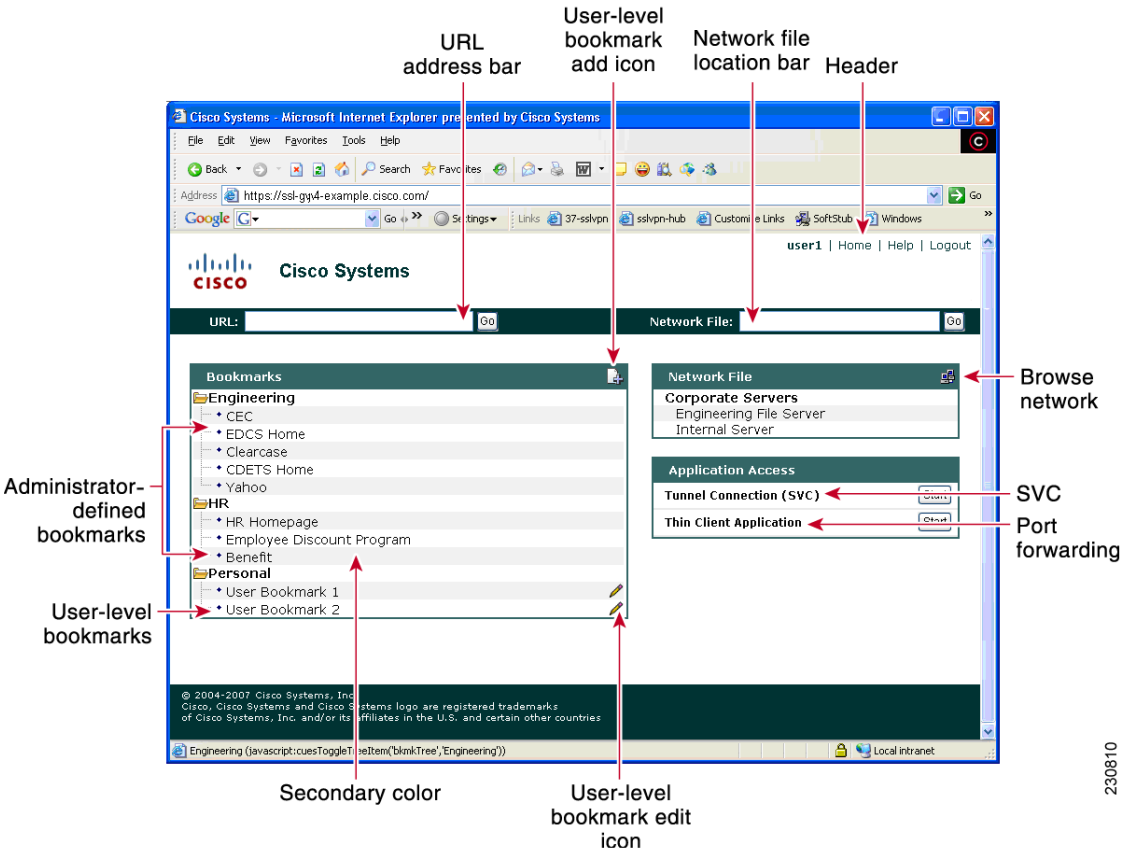



Table 2 provides information about various fields on the portal page. For information about setting elements such as color or titles, see command information in the *Cisco IOS Security Command Reference*, Release 12.4T, for the **logo**, **title**, **title-color**, **functions**, **port-forward**, **color**, **secondary-text-color**, **url-list**, **secondary-color**, and **hide-url-bar** commands.

***Table 2 Information About Fields on the Portal Page***

| Field | Description |
|---|---|
| User-level bookmark add icon | If a user clicks it, a dialog box is added so that a new bookmark can be added to the Personal folder. |
| Network File location bar | A user can enter the file server here. Both of the **functions file-access** and **functions file-entry** commands must be configured for the input box to appear. |
| Header | Shares the same color value as the title. |

*Table 2 Information About Fields on the Portal Page (continued)*

| Field | Description |
|---|---|
| Last login | Timestamp of the last login. |
| Browse network | Allows a user to browse the file network. Both commands **functions file-access** and **functions file-browse** must be configured for the icon to appear. |
| Tunnel Connection | A user can choose when to start the tunnel connection by configuring the **functions svc-enabled** command. |
| Port forwarding | Downloads the applet and starts port forwarding. |
| User-level bookmark edit icon | Allows a user to edit or delete an existing bookmark. |
| User-level bookmarks | A user can add a bookmark by using the plus icon (see below)<br>  <br>on the bookmark panel or toolbar. See the document *SSL VPN Remote User Guide* for information about the toolbar. A new window is opened when the link is clicked. |
| Administrator-defined bookmarks | Administrator-defined URL lists cannot be edited by the user. |
| URL address bar | A new window is opened when a user clicks Go. |

## Netegrity Cookie-Based Single SignOn Support

The Netegrity SiteMinder product provides a Single SignOn (SSO) feature that allows a user to log on a single time for various web applications. The benefit of this feature is that users are prompted to log on only once. This feature is accomplished by setting a cookie in the browser of a user when the user initially logs on.

Effective with Cisco IOS Release 12.4(11)T, Netegrity cookie-based SSO is integrated with SSL VPN. It allows administrators to configure an SSO server that sets a SiteMinder cookie in the browser of a user when the user initially logs on. This cookie is validated by a SiteMinder agent on subsequent user requests to resources that are protected by a SiteMinder realm. The agent decrypts the cookie and verifies whether the user has already been authenticated.

For information about configuring SSO Netegrity Cookie Support and associating it with a policy group using the CLI, see the sections "Configuring SSO Netegrity Cookie Support for a Virtual Context" and "Associating an SSO Server with a Policy Group," respectively.

An SSO server can also be associated with a policy group using RADIUS attributes, as in the following example:

```
webvpn:sso-server-name=server1
```

For a list of RADIUS attribute-value (AV) pairs that support SSL VPN, see the section "Configuring RADIUS Attribute Support for SSL VPN."

## NTLM Authentication

NT LAN Manager (NTLM) is supported for SSL VPN effective with Cisco IOS Release 12.4(9)T. The feature is configured by default.

## RADIUS Accounting

Effective with Cisco IOS Release 12.4(9)T, this feature provides for RADIUS accounting of SSL VPN user sessions.

For information about configuring SSL VPN RADIUS accounting for SSL VPN user sessions, see the section "Configuring RADIUS Accounting for SSL VPN User Sessions."

For more information about configuring RADIUS accounting, see the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part10/ch05/index.htm

For a list of RADIUS AV pairs that support SSL VPN, see the section "Configuring RADIUS Attribute Support for SSL VPN."

## TCP Port Forwarding and Thin Client

**Note** This feature requires the JRE version 1.4 or later releases to properly support SSL connections.

**Note** Because this feature requires installing JRE and configuring the local clients, and because doing so requires administrator permissions on the local system, it is unlikely that remote users will be able to use applications when they connect from public remote systems.

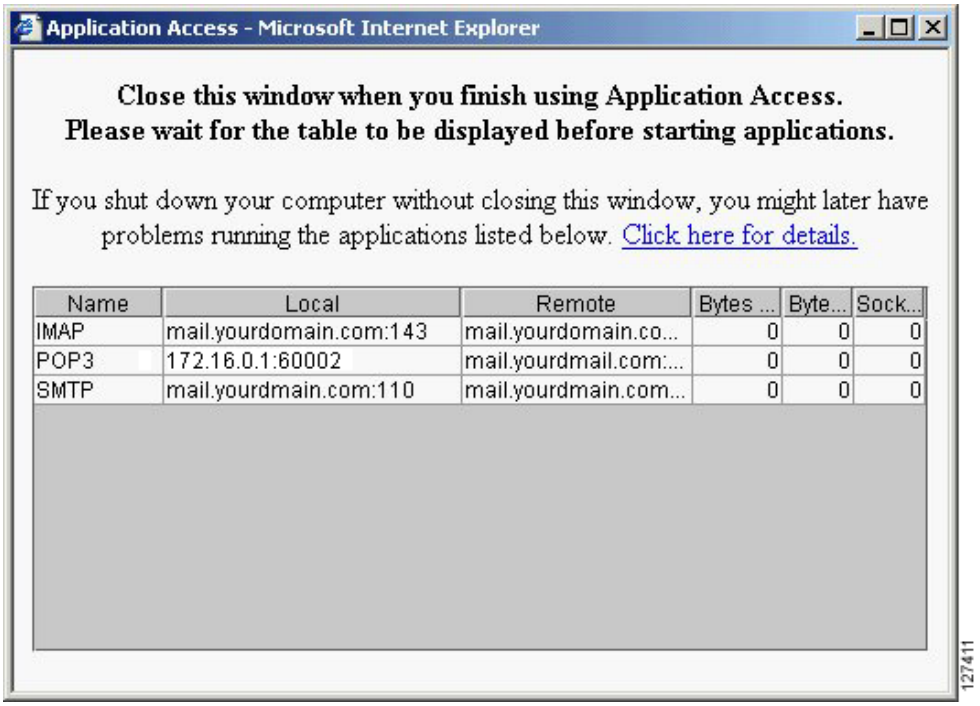
When the remote user clicks the Start button of the Thin Client Application (under "Application Access), a new window is displayed. This window initiates the downloading of a port-forwarding applet. Another window is then displayed. This window asks the remote user to verify the certificate with which this applet is signed. When the remote user accepts the certificate, the applet starts running, and port-forwarding entries are displayed (see Figure 11). The number of active connections and bytes that are sent and received is also listed on this window.

**Note** When remote users launch Thin Client, their system may display a dialog box regarding digital certificates, and this dialog box may appear behind other browser windows. If the remote user connection hangs, tell the remote user to minimize the browser windows to check for this dialog box.

You should have configured IP addresses, Domain Name System (DNS) names, and port numbers for the e-mail servers. The remote user can then launch the e-mail client, which is configured to contact the above e-mail servers and send and receive e-mails. POP3, IMAP, and SMTP protocols are supported.

The window attempts to close automatically if the remote user is logged out using JavaScript. If the session terminated and a new port forwarding connection is established, the applet displays an error message.

*Figure 11 TCP Port Forwarding Page*




**Caution** Users should always close the Thin Client window when finished using applications by clicking the close icon. Failure to quit the window properly can cause Thin Client or the applications to be disabled. See the section "Application Access—Recovering from Hosts File Errors" in the document SSL VPN Remote User Guide.

Table 3 lists remote system requirements for Thin Client.

*Table 3 SSL VPN Remote System Thin Client Requirements*

| Remote User System Requirements | Specifications or Use Suggestions |
|---|---|
| Client applications installed. | — |
| Cookies enabled on browser. | — |
| Administrator priviliges. | You must be the local administrator on your PC. |
| Sun Microsystems JRE version 1.4 or later installed. | SSL VPN automatically checks for JRE whenever the remote user starts Thin Client. If it is necessary to install JRE, a pop-up window displays directing remote users to a site where it is available. |

*Table 3 SSL VPN Remote System Thin Client Requirements (continued)*

| Remote User System Requirements | Specifications or Use Suggestions |
|---|---|
| Client applications configured, if necessary.<br>**Note** The Microsoft Outlook client does not require this configuration step. | To configure the client application, use the locally mapped IP address and port number of the server. To find this information, do the following:<br>• Start SSL VPN on the remote system and click the Thin Client link on the SSL VPN home page. The Thin Client window is displayed.<br>• In the Name column, find the name of the server that you want to use, and then identify its corresponding client IP address and port number (in the Local column).<br>• Use this IP address and port number to configure the client application. The configuration steps vary for each client application. |
| Windows XP SP2 patch. | If you are running Windows XP SP2, you must install a patch from Microsoft that is available at the following address:<br>http://support.microsoft.com/?kbid=884020<br>This problem is a known Microsoft issue. |

## URL Obfuscation

The URL Obfuscation feature provides administrators with the ability to obfuscate, or mask, sensitive portions of an enterprise URL, such as IP addresses, hostnames, or part numbers. For example, if URL masking is configured for a user, the URL in the address bar could have the port and hostname portion garbled, as in this example:

https://slvpn-gateway.examplecompany.com/http/cF9HxnBjRmSFEzBWpDtfXfigzL559MQo51Qj/cgi-bin/submit.p

For information about configuring this feature, see the section "Associating an SSO Server with a Policy Group."

## User-Level Bookmarking

Effective with Cisco IOS Release 12.4(15)T, users can bookmark URLs while connected through an SSL VPN tunnel. Users can access the bookmarked URLs by clicking the URLs.

User-level bookmarking is turned by default. There is no way to turn it off. To set the storage location, administrators can use the **user-profile location** command. If the **user-profile location** command is not configured, the location flash:/webvpn/{*context name*}/ is used.

# Other SSL VPN Features

Table 4 lists the requirements for various SSL VPN features.

***Table 4 SSL VPN Remote User System Requirements***

| Task | Remote User System Requirements | Additional Information |
|---|---|---|
| Web Browsing | Usernames and passwords for protected websites | Users should log out on SSL VPN sessions when they are finished. |
| | | The look and feel of web browsing with SSL VPN might be different from what users are accustomed to. For example, when they are using SSL VPN, the following should be noted:<br>• The SSL VPN title bar appears above each web page.<br>• Websites can be accessed as follows:<br>– Entering the URL in the Enter Web Address field on the SSL VPN home page<br>– Clicking a preconfigured website link on the SSL VPN home page<br>– Clicking a link on a webpage accessed by one of the previous two methods<br>Also, depending on how a particular account was configured, the following might have occurred:<br>• Some websites are blocked.<br>• Only the websites that appear as links on the SSL VPN home page are available. |
| Network Browsing and File Management | File permissions configured for shared remote access | Only shared folders and files are accessible through SSL VPN. |
| | Server name and passwords are necessary for protected file servers | |
| | Domain, workgroup, and server names where folders and files reside | A user might not be familiar with how to locate his or her files through the network of an organization. |
| | **Note** The user should not interrupt the Copy File to Server operation or navigate to a different window while the copying is in progress. Interrupting this operation can cause an incomplete file to be saved on the server. | |

*Table 4 SSL VPN Remote User System Requirements (continued)*

| Task | Remote User System Requirements | Additional Information |
|---|---|---|
| Using e-mail:<br>Thin Client | Same requirements as for Thin Client (see the "TCP Port Forwarding and Thin Client" section on page 17) | To use e-mail, users must start Thin Client from the SSL VPN home page. The e-mail client is then available for use. |
| | **Note** If a user is using an IMAP client and loses the e-mail server connection or is unable to make a new connection, the user should close the IMAP application and restart SSL VPN. | |
| | Other Mail Clients | Microsoft Outlook Express versions 5.5 and 6.0 have been tested.<br><br>SSL VPN should support other SMTPS, POP3S, or IMAP4S e-mail programs, such as Netscape Mail, Lotus Notes, and Eudora, but they have not been verified. |

*Table 4 SSL VPN Remote User System Requirements (continued)*

| Task | Remote User System Requirements | Additional Information |
|---|---|---|
| Using e-mail:<br>Web Access | Web-based e-mail product installed | Supported products are as follows:<br>• OWA 5.5, 2000, and 2003<br>Netscape, Mozilla, and Internet Explorer are supported with OWA 5.5 and 2000.<br>Internet Explorer 6.0 or later version is required with OWA 2003. Netscape and Mozilla are supported with OWA 2003.<br>• Lotus Notes<br>Operating system support:<br>**Note** Later versions of the following browsers are also supported.<br>• Microsoft Windows 2000, Windows XP, or Windows Vista<br>• Macintosh OS X 10.4.6<br>• Linux (Redhat RHEL 3.0 +, FEDORA 5, or FEDORA 6)<br>SSL VPN-supported browser:<br>The following browsers have been verified for SSL VPN. Other browsers might not fully support SSL VPN features.<br>**Note** Later versions of the following software are also supported.<br>• Internet Explorer 6.0 or 7.0<br>• Firefox 2.0 (Windows and Linux)<br>• Safari 2.0.3<br>Other web-based e-mail products should also work, but they have not been verified. |
| Using the Cisco Tunnel Connection | | To retrieve Tunnel Connection log messages using the Windows Event Viewer, go to Program Files > Administrative Tools > Event Viewer in Windows. |
| Using Secure Desktop Manager | A Secure Desktop Manager-supported browser | On Microsoft Windows:<br>• Internet Explorer version 6.0 or 7.0<br>• Netscape version 7.2<br>On Linux:<br>• Netscape version 7.2 |

*Table 4 SSL VPN Remote User System Requirements (continued)*

| Task | Remote User System Requirements | Additional Information |
|---|---|---|
| Using Cache Cleaner or Secure Desktop | A Cisco Secure Desktop-supported browser | Any browser supported for Secure Desktop Manager. |

# Platform Support

For information about platform support for the SSL VPN feature, see the data sheet *Cisco IOS SSL VPN* ("Feature Availability" section).

## Licensing

Cisco IOS SSL VPN is a licensed feature available on Cisco routers running the Cisco IOS Advanced Security feature set. Each security bundle entitles you to a certain number of free users. Beyond that, you need to purchase additional feature licenses. For more information about licensing, see the bulletin *Cisco IOS SSL VPN Licensing Information*.

# How to Configure SSL VPN Services on a Router

This section contains the following tasks:

### Configuring and Enabling SSL VPN Services

- Configuring an SSL VPN Gateway, page 24 (required)
- Configuring a Generic SSL VPN Gateway, page 26 (optional)
- Configuring an SSL VPN Context, page 27 (required)
- Configuring an SSL VPN Policy Group, page 31 (required)

### Configuring AAA-Related Features for SSL VPN

- Configuring Local AAA Authentication for SSL VPN User Sessions, page 34 (optional)
- Configuring AAA for SSL VPN Users Using a Secure Access Control Server, page 35 (optional)
- Configuring RADIUS Accounting for SSL VPN User Sessions, page 37 (optional)
- Monitoring and Maintaining RADIUS Accounting for an SSL VPN Session, page 38 (optional)
- Configuring RADIUS Attribute Support for SSL VPN, page 39 (optional)

### Customizing and Enabling SSL VPN Features

- Configuring a URL List for Clientless Remote Access, page 42 (optional)
- Configuring Microsoft File Shares for Clientless Remote Access, page 43 (optional)
- Configuring Citrix Application Support for Clientless Remote Access, page 47 (optional)
- Configuring Application Port Forwarding, page 48 (optional)
- Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files, page 51 (optional)
- Configuring Cisco Secure Desktop Support, page 53 (optional)

- Configuring Cisco AnyConnect VPN Client Full Tunnel Support, page 54 (optional)
- Configuring Advanced SSL VPN Tunnel Features, page 59 (optional)
- Configuring VRF Virtualization, page 62 (optional)
- Configuring ACL Rules, page 63 (optional)
- Associating an ACL Attribute with a Policy Group, page 66 (optional)
- Configuring SSO Netegrity Cookie Support for a Virtual Context, page 67 (optional)
- Associating an SSO Server with a Policy Group, page 69 (optional)
- Configuring URL Obfuscation (Masking), page 69 (optional)
- Adding a CIFS Server URL List to an SSL VPN Context and Attaching It to a Policy Group, page 70 (optional)
- Configuring User-Level Bookmarks, page 72 (optional)
- Configuring FVRF, page 73 (optional)

#### Monitoring and Maintaining SSL VPN Features

- Using SSL VPN Clear Commands, page 74 (optional)
- Verifying SSL VPN Configurations, page 75 (optional)
- Using SSL VPN Debug Commands, page 76 (optional)

# Configuring an SSL VPN Gateway

The SSL VPN gateway acts as a proxy for connections to protected resources. Protected resources are accessed through an SSL-encrypted connection between the gateway and a web-enabled browser on a remote device, such as a personal computer. Entering the **webvpn gateway** command places the router in SSL VPN gateway configuration mode. The following are accomplished in this task:

- The gateway is configured with an IP address.
- A port number is configured to carry HTTPS traffic (443 is default).
- A hostname is configured for the gateway.
- Crypto encryption and trust points are configured.
- The gateway is configured to redirect HTTP traffic (port 80) over HTTPS.
- The gateway is enabled.

## SSL VPN Encryption

The SSL VPN provides remote-access connectivity from almost any Internet-enabled location using only a web browser and its native SSL encryption. The **ssl encryption** command is configured to restrict the encryption algorithms that SSL uses in Cisco IOS software.

**Note** There is a known compatibility issue with the encryption type and Java. If the Java port-forwarding applet does not download properly and the configuration line **ssl encryption 3des-sha1 aes-sha1** is present, you should remove the line from the webvpn gateway subconfiguration.

## SSL VPN Trustpoints

The configuration of the **ssl trustpoint** command is required only if you need to configure a specific CA certificate. A self-signed certificate is automatically generated when an SSL VPN gateway is put in service.

### SUMMARY STEPS

#### Required Steps

1. **enable**
2. **configure terminal**
3. **webvpn gateway** *name*

#### Optional Steps

4. **hostname** *name*
5. **ip address** *number* [**port** *number*] [**secondary**]
6. **http-redirect** [**port** *number*]
7. **ssl encryption** [**3des-sha1**] [**aes-sha1**] [**rc4-md5**]
8. **ssl trustpoint** *name*
9. **inservice**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn gateway** *name*<br><br>**Example:**<br>`Router(config)# webvpn gateway GW_1` | Enters webvpn gateway configuration mode to configure an SSL VPN gateway.<br>• Only one gateway is configured in an SSL VPN-enabled network. |
| **Step 4** | **hostname** *name*<br><br>**Example:**<br>`Router(config-webvpn-gateway)# hostname VPN_1` | Configures the hostname for an SSL VPN gateway. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **ip address** *number* [**port** *number*] [**secondary**]<br><br>**Example:**<br>`Router(config-webvpn-gateway)# ip address 10.1.1.1` | Configures a proxy IP address on an SSL VPN gateway.<br>• A secondary address must be configured if the proxy IP address is not on a directly connected network.<br>• A secondary address does not reply to Address Resolution Protocol (ARP) or Internet Control Message Protocol (ICMP) messages. |
| **Step 6** | **http-redirect** [**port** *number*]<br><br>**Example:**<br>`Router(config-webvpn-gateway)# http-redirect` | Configures HTTP traffic to be carried over HTTPS.<br>• When this command is enabled, the SSL VPN gateway listens on port 80 and redirects HTTP traffic over port 443 or the port number specified with the **port** keyword. |
| **Step 7** | **ssl encryption** [**3des-sha1**] [**aes-sha1**] [**rc4-md5**]<br><br>**Example:**<br>`Router(config-webvpn-gateway)# ssl encryption rc4-md5` | Specifies the encryption algorithm that the SSL protocol uses for SSL VPN connections.<br>• The ordering of the algorithms specifies the preference. |
| **Step 8** | **ssl trustpoint** *name*<br><br>**Example:**<br>`Router(config-webvpn-gateway)# ssl trustpoint CA_CERT` | (Optional if a self-signed certificate is to be used.) Configures the certificate trust point on an SSL VPN gateway.<br>**Tip** Entering the **no** form of this command configures the SSL VPN gateway to revert to using an autogenerated self-signed certificate. |
| **Step 9** | **inservice**<br><br>**Example:**<br>`Router(config-webvpn-gateway)# inservice` | Enables an SSL VPN gateway.<br>A gateway cannot enabled or put "in service" until a proxy IP address has been configured. |

## What to Do Next

SSL VPN context and policy group configurations must be configured before an SSL VPN gateway can be operationally deployed. Proceed to the section "Configuring an SSL VPN Context" to see information on SSL VPN context configuration.

# Configuring a Generic SSL VPN Gateway

To configure a generic SSL VPN gateway, perform the following steps in privileged EXEC mode.

**Note** The advantage of this configuration over the one in the configuration task "Configuring an SSL VPN Gateway" is that basic commands and context can be configured quickly using just the **webvpn enable** command.

### SUMMARY STEPS

1. **enable**
2. **webvpn enable** *gateway_IP-address*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **webvpn enable name** *gateway_IP-address*<br><br>**Example:**<br>`Router# configure terminal` | Enables an SSL VPN gateway. |

# Configuring an SSL VPN Context

The SSL VPN context defines the virtual configuration of the SSL VPN. Entering the **webvpn context** command places the router in SSL VPN configuration mode. The following are accomplished in this task:

- A gateway and domain is associated.
- The AAA authentication method is specified.
- A group policy is associated.
- The remote user portal (web page) is customized.
- A limit on the number users sessions is configured.
- The context is enabled.

## Context Defaults

The **ssl authenticate verify all** command is enabled by default when a context configuration is created. The context cannot be removed from the router configuration while an SSL VPN gateway is in an enabled state (in service).

## Configuring a Virtual Host

A virtual hostname is specified when multiple virtual hosts are mapped to the same IP address on the SSL VPN gateway (similar to the operation of a canonical domain name). The virtual hostname differentiates host requests on the gateway. The host header in the HTTP message is modified to direct traffic to the virtual host. The virtual hostname is configured with the **gateway** command in webvpn context configuration mode.

## Prerequisites

The SSL VPN gateway configuration has been completed.

### SUMMARY STEPS

**Required Steps**

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*

**Optional Steps**

4. **aaa authentication** {**domain** *name* | **list** *name*}
5. **policy group** *name*
6. **exit**
7. **default-group-policy** *name*
8. **exit**
9. **gateway** *name* [**domain** *name* | **virtual-host** *name*]
10. **inservice**
11. **login-message** [*message-string*]
12. **logo** [**file** *filename* | **none**]
13. **max-users** *number*
14. **secondary-color** *color*
15. **secondary-text-color** {**black** | **white**}
16. **title** [*title-string*]
17. **title-color** *color*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context.<br><br>**Tip** The context can be optionally named using the domain or virtual hostname. This is recommended as a best practice. It simplifies the management of multiple context configurations. |
| **Step 4** | **aaa authentication** {**domain** *name* \| **list** *name*}<br><br>**Example:**<br>`Router(config-webvpn-context)# aaa authentication domain SERVER_GROUP` | Specifies a list or method for SSL VPN remote-user authentication.<br><br>**Tip** If this command is not configured, the SSL VPN gateway will use global authentication, authorization, and accounting (AAA) parameters (if configured) for remote-user authentication. |
| **Step 5** | **policy group** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# policy group ONE` | Creates a policy group within the SSL VPN context and enters webvpn group policy configuration mode.<br><br>• Used to define a policy that can be applied to the user. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Router(webvpn-group-policy)# exit` | Exits webvpn group policy configuration mode. |
| **Step 7** | **default-group-policy** *name*<br><br>**Example:**<br>`Router(webvpn-group-policy)# default-group-policy ONE` | Associates a a group policy with an SSL VPN context configuration.<br><br>• This command is configured to attach the policy group to the SSL VPN context when multiple group policies are defined under the context.<br>• This policy will be used as default, unless a AAA server pushes an attribute that specifically requests another group policy. |
| **Step 8** | **exit**<br><br>**Example:**<br>`Router(webvpn-group-policy)# exit` | Exits webvpn group policy configuration mode. |
| **Step 9** | **gateway** *name* [**domain** *name* \| **virtual-host** *name*]<br><br>**Example:**<br>`Router(config-webvpn-context)# gateway GW_1 domain cisco.com` | Associates an SSL VPN gateway with an SSL VPN context.<br><br>• The gateway configured in the first configuration task table is associated with the SSL VPN context in this configuration step. |
| **Step 10** | **inservice**<br><br>**Example:**<br>`Router(config-webvpn-gateway)# inservice` | Enables an SSL VPN context configuration.<br><br>• The context is put “in service” by entering this command. However, the context is not operational until it is associated with an enabled SSL VPN gateway. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **login-message** [*message-string*]<br><br>**Example:**<br>`Router(config-webvpn-context)# login-message "Please enter your login credentials"` | Configures a message for the user login text box displayed on the login page. |
| **Step 12** | **logo** [**file** *filename* \| **none**]<br><br>**Example:**<br>`Router(config-webvpn-context)# logo file flash:/mylogo.gif` | Configures a custom logo to be displayed on the login and portal pages of an SSL VPN.<br>• The source image file for the logo is a gif, jpg, or png file that is up to 255 characters in length (filename) and up to 100 KB in size.<br>• The file is referenced from a local file system, such as flash memory. An error message will be displayed if the file is not referenced from a local file system.<br>• No logo will be displayed if the image file is removed from the local file system. |
| **Step 13** | **max-users** *number*<br><br>**Example:**<br>`Router(config-webvpn-context)# max-users 500` | Limits the number of connections to an SSL VPN that will be permitted. |
| **Step 14** | **secondary-color** *color*<br><br>**Example:**<br>`Router(config-webvpn-context)# secondary-color darkseagreen`<br>`Router(config-webvpn-context)# secondary-color #8FBC8F`<br>`Router(config-webvpn-context)# secondary-color 143,188,143` | Configures the color of the secondary title bars on the login and portal pages of an SSL VPN.<br>• The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a pound sign [#]), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):<br>– \#/x{6}<br>– \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255)<br>– \w+<br>• The default color is purple.<br>• The example shows the three forms that the color can be configured. |
| **Step 15** | **secondary-text-color** {**black** \| **white**}<br><br>**Example:**<br>`Router(config-webvpn-context)# secondary-text-color white` | Configures the color of the text on the secondary bars of an SSL VPN.<br>• The color of the text on the secondary bars must be aligned with the color of the text on the title bar.<br>• The default color is black. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 16** | **title** [*title-string*]<br><br>**Example:**<br>`Router(config-webvpn-context)# title "Secure Access: Unauthorized users prohibited"` | Configures the HTML title string that is shown in the browser title and on the title bar of an SSL VPN.<br>• The optional form of the **title** command is entered to configure a custom text string. If this command is issued without entering a text string, a title will not be displayed in the browser window. If the **no** form of this command is used, the default title string "WebVPN Service" is displayed. |
| **Step 17** | **title-color** *color*<br><br>**Example:**<br>`Router(config-webvpn-context)# title-color darkseagreen`<br>`Router(config-webvpn-context)# title-color #8FBC8F`<br>`Router(config-webvpn-context)# title-color 143,188,143` | Specifies the color of the title bars on the login and portal pages of an SSL VPN.<br>• The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a pound sign [#]), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):<br>– \#/x{6}<br>– \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255)<br>– \w+<br>• The default color is purple.<br>• The example shows the three forms that can be used to configure the title color. |

## What to Do Next

an SSL VPN policy group configuration must be defined before an SSL VPN gateway can be operationally deployed. Proceed to the next section to see information on SSL VPN policy group configuration.

# Configuring an SSL VPN Policy Group

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of remote users. Entering the **policy group** command places the router in webvpn group policy configuration mode. After it is configured, the group policy is attached to the SSL VPN context configuration by configuring the **default-group-policy** command. The following tasks are accomplished in this configuration:

- The presentation of the SSL VPN portal page is configured.
- A NetBIOS server list is referenced.
- A port-forwarding list is referenced.
- The idle and session timers are configured.
- A URL list is referenced.

## Outlook Web Access 2003

OWA 2003 is supported by the SSL VPN gateway upon competition of this task. The Outlook Exchange Server must be reachable by the SSL VPN gateway via TCP/IP.

## URL-List Configuration

A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual URL list configurations must have unique names.

### SUMMARY STEPS

#### Required Steps

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*

#### Optional Steps

5. **banner** *string*
6. **hide-url-bar**
7. **nbns-list** *name*
8. **port-forward** *name* [**auto-download**] | [**http-proxy** [**proxy-url** {*homepage-url*}]]
9. **timeout** {**idle** *seconds* | **session** *seconds*}
10. **url-list** *name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **Step 4** | **policy group** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# policy group ONE` | Enters webvpn group policy configuration mode to configure a group policy. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **banner** *string*<br><br>**Example:**<br>`Router(config-webvpn-group)# banner "Login Successful"` | Configures a banner to be displayed after a successful login. |
| **Step 6** | **hide-url-bar**<br><br>**Example:**<br>`Router(config-webvpn-group)# hide-url-bar` | Prevents the URL bar from being displayed on the SSL VPN portal page. |
| **Step 7** | **nbns-list** *name*<br><br>**Example:**<br>`Router(config-webvpn-group)# nbns-list SERVER_LIST` | Attaches a NetBIOS Name Service (NBNS) server list to a policy group configuration.<br>• The NBNS server list is first defined in SSL VPN NBNS list configuration mode. |
| **Step 8** | **port-forward** *name* [**auto-download**] \| [**http-proxy** [**proxy-url** {*homepage-url*}]]<br><br>Example:<br>`Router(config-webvpn-group)# port-forward EMAIL auto-download http-proxy proxy-url "http://www.example.com"` | Attaches a port-forwarding list to a policy group configuration.<br>• **auto-download**—(Optional) Allows for automatic download of the port-forwarding Java applet on the portal page of a website.<br>• **http-proxy**—(Optional) Allows the Java applet to act as a proxy for the browser of the user.<br>• **proxy-url**—(Optional) Page at this URL address opens as the portal (home) page of the user.<br>• *homepage-url*—URL of the homepage. |
| **Step 9** | **timeout** {**idle** *seconds* \| **session** *seconds*}<br><br>**Example:**<br>`Router(config-webvpn-group)# timeout idle 1800`<br>`Router(config-webvpn-group)# timeout session 36000` | Configures the length of time that a remote user session can remain idle or the total length of time that the session can remain connected.<br>• Upon expiration of either timer, the remote user connection is closed. The remote user must login (reauthenticate) to access the SSL VPN. |
| **Step 10** | **url-list** *name*<br><br>**Example:**<br>`Router(config-webvpn-group)# url-list ACCESS` | Attaches a URL list to policy group configuration. |

## What to Do Next

At the completion of this task, the SSL VPN gateway and context configurations are operational and enabled (in service), and the policy group has been defined. The SSL VPN gateway is operational for clientless remote access (HTTPS only). Proceed to the next section to see information about configuring AAA for remote-user connections.

# Configuring Local AAA Authentication for SSL VPN User Sessions

The steps in this task show how to configure a local AAA database for remote-user authentication. AAA is configured in global configuration mode. In this task, the **aaa authentication** command is not configured under the SSL VPN context configuration. Omitting this command from the SSL VPN context configuration causes the SSL VPN gateway to use global authentication parameters by default.

## Prerequisites

SSL VPN gateway and context configurations are enabled and operational.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **username** {*name* **secret** [**0** | **5**] *password*}
5. **aaa authentication login default local**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Router(config)# aaa new-model` | Enables the AAA access control model. |
| **Step 4** | **username** {*name* **secret** [**0** \| **5**] *password*}<br><br>**Example:**<br>`Router(config)# username USER1 secret 0 PsW2143` | Establishes a username based authentication system.<br>• Entering **0** configures the password as clear text. Entering **5** encrypts the password. |
| **Step 5** | **aaa authentication login default local**<br><br>**Example:**<br>`Router(config)# aaa authentication login default local` | Configures local AAA authentication. |

## What to Do Next

The database that is configured for remote-user authentication on the SSL VPN gateway can be a local database, as shown in this task, or the database can be accessed through any RADIUS or TACACS+ AAA server.

It is recommended that you use a separate AAA server, such as a Cisco ACS. A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions. Proceed to the next section to see more information.

# Configuring AAA for SSL VPN Users Using a Secure Access Control Server

The steps in this task show how to configure AAA using a separate RADIUS or TACACS+ server. AAA is configured in global configuration mode. The authentication list/method is referenced in the SSL VPN context configuration with the **aaa authentication** command. The steps in this task configure AAA using a RADIUS server.

## Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- A RADIUS or TACACS+ AAA server is operational and reachable from the SSL VPN gateway.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server** {**radius** *group-name* | **tacacs+** *group-name*}
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **exit**
7. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
8. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias**{*hostname* | *ip-address*}]
9. **webvpn context** *name*
10. **aaa authentication** {**domain** *name* | **list** *name*}

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Router(config)# aaa new-model` | Enables the AAA access control model. |
| **Step 4** | **aaa group server** {**radius** *group-name* \| **tacacs+** *group-name*}<br><br>**Example:**<br>`Router(config)# aaa group server radius myServer` | Configures a RADIUS or TACACS+ server group and specifies the authentication list or method, and enters server-group configuration mode. |
| **Step 5** | **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]<br><br>**Example:**<br>`Router(config-sg-radius)# server 10.1.1.20 auth-port 1645 acct-port 1646` | Configures the IP address of the AAA group server. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Router(config-sg-radius)# exit` | Exits server-group configuration mode. |
| **Step 7** | **aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*]<br><br>**Example:**<br>`Router(config)# aaa authentication login default local group myServer` | Sets AAA login parameters. |
| **Step 8** | **radius-server host** {*hostname* \| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* \| *ip-address*}]<br><br>**Example:**<br>`Router(config)# radius-server host 10.1.1.20 auth-port 1645 acct-port 1646` | Specifies a host as the group server. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters SSL VPN configuration mode to configure the SSL VPN context. |
| **Step 10** | **aaa authentication** {**domain** *name* \| **list** *name*}<br><br>**Example:**<br>`Router(config-webvpn-context)# aaa authentication domain myServer` | Configures AAA authentication for SSL VPN sessions. |

## What to Do Next

Proceed to the section "Configuring RADIUS Attribute Support for SSL VPN" to see RADIUS attribute-value pair information introduced to support this feature.

# Configuring RADIUS Accounting for SSL VPN User Sessions

To configure RADIUS accounting for SSL VPN user sessions, perform the following steps.

## Prerequisites

- Before configuring RADIUS accounting for SSL VPN user sessions, you should first have configured AAA-related commands (in global configuration mode) and have set the accounting list.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **webvpn aaa accounting list** *aaa-list*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Router(config)# aaa new-model` | Enables the AAA access control model. |
| **Step 4** | **webvpn aaa accounting-list** *aaa-list*<br><br>**Example:**<br>`Router(config)# webvpn aaa accounting-list SSL VPNaaa` | Enables AAA accounting when you are using RADIUS for SSL VPN sessions. |

# Monitoring and Maintaining RADIUS Accounting for an SSL VPN Session

To monitor and maintain your RADIUS accounting configuration, perform the following steps (the **debug** commands can be used together or individually).

### SUMMARY STEPS

1. **enable**
2. **debug webvpn aaa**
3. **debug aaa accounting**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **debug webvpn aaa**<br><br>**Example:**<br>`Router# debug webvpn aaa` | Enables SSL VPN session monitoring for AAA. |
| **Step 3** | **debug aaa accounting**<br><br>**Example:**<br>`Router# debug aaa accounting` | Displays information on accountable events as they occur. |

# Configuring RADIUS Attribute Support for SSL VPN

This section lists RADIUS attribute-value (AV) pair information introduced to support SSL VPN. For information on using RADIUS AV pairs with Cisco IOS software, see the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4 at the following URL:

http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_chapter09186a00804ec61e.html

Table 5 shows information about SSL VPN RADIUS attribute-value pairs.

**Note** All SSL VPN attributes (except for the standard IETF RADIUS attributes) start with **webvpn:** as follows:

webvpn:urllist-name=cisco
webvpn:nbnslist-name=cifs
webvpn:default-domain=cisco.com

***Table 5 SSL VPN RADIUS Attribute-Value Pairs***

| Attribute | Type of Value | Values | Default |
|---|---|---|---|
| addr (Framed-IP-Address[1]) | ipaddr | *IP_address* | |
| addr-pool | string | *name* | |
| auto-applet-download | integer | 0 (disable)<br>1 (enable)[2] | 0 |
| banner | string | | |
| citrix-enabled | integer | 0 (disable)<br>1 (enable)[3] | 0 |
| default-domain | string | | |
| dns-servers | ipaddr | *IP_address* | |

*Table 5 SSL VPN RADIUS Attribute-Value Pairs (continued)*

| Attribute | Type of Value | Values | Default |
|---|---|---|---|
| dpd-client-timeout | integer (seconds) | 0 (disabled)–3600 | 300 |
| dpd-gateway-timeout | integer (seconds) | 0 (disabled)–3600 | 300 |
| file-access | integer | 0 (disable)<br>1 (enable)[3] | 0 |
| file-browse | integer | 0 (disable)<br>1 (enable)[3] | 0 |
| file-entry | integer | 0 (disable)<br>1 (enable)[3] | 0 |
| hide-urlbar | integer | 0 (disable)<br>1 (enable)[3] | 0 |
| home-page | string | | |
| idletime (Idle-Timeout[1]) | integer (seconds) | 0–3600 | 2100 |
| ie-proxy-exception | string | *DNS_name* | |
| | ipaddr | *IP_address* | |
| ie-proxy-server | ipaddr | *IP_address* | |
| inacl | integer | 1–199,<br>1300–2699 | |
| | string | *name* | |
| keep-svc-installed | integer | 0 (disable)<br>1 (enable)[3] | 1 |
| nbnslist-name | string | *name* | |
| netmask (Framed-IP-Netmask[1]) | ipaddr | *IP_address_mask* | |
| port-forward-auto | integer | 0 (disable)<br>1 (enable) | If this AV pair is not configured, the default is whatever was configured for the group policy.<br>If this AV pair is configured with an integer of 1, the 1 will override a group policy value of 0. |

*Table 5 SSL VPN RADIUS Attribute-Value Pairs (continued)*

| Attribute | Type of Value | Values | Default |
|---|---|---|---|
| port-forward-http-proxy | integer | 0 (disable)<br>1 (enable) | HTTP proxy is not enabled.<br>If this AV pair is configured with an integer of 1, the 1 will override a group policy value of 0. |
| port-forward-http-proxy-url | string | URL address (for example, http://example.com) | |
| port-forward-name | string | *name* | |
| primary-dns | ipaddr | *IP_address* | |
| rekey-interval | integer (seconds) | 0–43200 | 21600 |
| secondary-dns | ipaddr | *IP_address* | |
| split-dns | string | | |
| split-exclude[4] | ipaddr ipaddr | *IP_address IP_address_mask* | |
| | word | local-lans | |
| split-include[4] | ipaddr ipaddr | *IP_address IP_address_mask* | |
| sso-server-name | string | *name* | |
| svc-enabled[5] | integer | 0 (disable)<br>1 (enable)[3] | 0 |
| svc-ie-proxy-policy | word | none, auto, bypass-local | |
| svc-required[5] | integer | 0 (disable)<br>1 (enable)[3] | 0 |
| timeout (Session-Timeout[1]) | integer (seconds) | 1–1209600 | 43200 |
| urllist-name | string | *name* | |
| user-vpn-group | string | *name* | |
| wins-server-primary | ipaddr | *IP_address* | |
| wins-servers | ipaddr | *IP_address* | |
| wins-server-secondary | ipaddr | *IP_address* | |

1. Standard IETF RADIUS attributes.
2. Any integer other than 0 enables this feature.
3. Any integer other than 0 enables this feature.

4. You can specify either split-include or split-exclude, but you cannot specify both options.
5. You can specify either svc-enable or svc-required, but you cannot specify both options.

## What to Do Next

Proceed to the next section to see information about customizing the URL list configured in Step 10 of the section "Configuring an SSL VPN Policy Group."

# Configuring a URL List for Clientless Remote Access

The steps in this configuration task show how to configure a URL list. The URL list, as the name implies, is a list of HTTP URLs that are displayed on the portal page after a successful login. The URL list is configured in webvpn context configuration and webvpn group policy configuration modes.

## Prerequisites

SSL VPN gateway and context configurations are enabled and operational.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **url-list** *name*
5. **heading** *text-string*
6. **url-text** {*name* **url-value** *url*}
7. **exit**
8. **policy group** *name*
9. **url-list** *name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **url-list** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# url-list ACCESS` | Enters enter webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of an SSL VPN. |
| **Step 5** | **heading** *text-string*<br><br>**Example:**<br>`Router(config-webvpn-url)# heading "Quick Links"` | Configures the heading that is displayed above URLs listed on the portal page of an SSL VPN.<br>• The URL list heading entered as a text string. The heading must be entered inside of quotation marks if it contains spaces. |
| **Step 6** | **url-text** {*name* **url-value** *url*}<br><br>**Example:**<br>`Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com` | Adds an entry to a URL list. |
| **Step 7** | **exit**<br><br>**Example:**<br>`Router(config-webvpn-url)# exit` | Exits webvpn URL list configuration mode, and enters SSL VPN context configuration mode. |
| **Step 8** | **policy group** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# policy group ONE` | Enters webvpn group policy configuration mode to configure a group policy. |
| **Step 9** | **url-list** *name*<br><br>**Example:**<br>`Router(config-webvpn-group)# url-list ACCESS` | Attaches the URL list to the policy group configuration. |

## What to Do Next

Proceed to the next section to see information about configuring clientless remote access to file shares.

# Configuring Microsoft File Shares for Clientless Remote Access

In clientless remote access mode, files and directories created on Microsoft Windows servers can be accessed by the remote client through the HTTPS-enabled browser. When enabled, a list of file server and directory links are displayed on the portal page after login. The administrator can customize permissions on the SSL VPN gateway to provide limited read-only access for a single file or full-write access and network browsing capabilities. The following access capabilities can be configured:

- Network browse (listing of domains)
- Domain browse (listing of servers)
- Server browse (listing of shares)
- Listing files in a share
- Downloading files

- Modifying files
- Creating new directories
- Creating new files
- Deleting files

## Common Internet File System Support

CIFS is the protocol that provides access to Microsoft file shares and support for common operations that allow shared files to be accessed or modified.

## NetBIOS Name Service Resolution

Windows Internet Name Service (WINS) uses NetBIOS name resolution to map and establish connections between Microsoft servers. A single server must be identified by its IP address in this configuration. Up to three servers can be added to the configuration. If multiple servers are added, one server should be configured as the master browser.

## Samba Support

Microsoft file shares can be accessed through the browser on a Linux system that is configured to run Samba.

## Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- A Microsoft file server is operational and reachable from the SSL VPN gateway over TCP/IP.

## Restrictions

- Only file shares configured on Microsoft Windows 2000 or XP servers are supported.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **nbns-list** *name*
5. **nbns-server** *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]
6. **exit**
7. **policy group** *name*
8. **nbns-list** *name*
9. **functions** {**file-access** | **file-browse** | **file-entry** | **svc-enabled** | **svc-required**}

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **Step 4** | **nbns-list** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# nbns-list SERVER_LIST` | Enters webvpn nbnslist configuration mode to configure an NBNS server list for CIFS name resolution. |
| **Step 5** | **nbns-server** *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]<br><br>**Example:**<br>`Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master`<br>`Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5`<br>`Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5` | Adds a server to an NBNS server list and enters webvpn nbnslist configuration mode.<br>• The server specified with the ip-address argument can be a primary domain controller (PDC) in a Microsoft network.<br>• When multiple NBNS servers are specified, a single server is configured as master browser.<br>• Up to three NBNS server statements can be configured. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Router(config-webvpn-nbnslist)# exit` | Exits webvpn nbnslist configuration mode and enters webvpn context configuration mode. |
| **Step 7** | **policy group** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# policy group ONE` | Enters webvpn group policy configuration mode to configure a group policy. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **nbns-list** *name*<br><br>**Example:**<br>`Router(config-webvpn-group)# nbns-list SERVER_LIST` | Attaches a NBNS server list to a policy group configuration. |
| **Step 9** | **functions** {**file-access** \| **file-browse** \| **file-entry** \| **svc-enabled** \| **svc-required**}<br><br>**Example:**<br>`Router(config-webvpn-group)# functions file-access`<br>`Router(config-webvpn-group)# functions file-browse`<br>`Router(config-webvpn-group)# functions file-entry` | Configures access for Microsoft file shares.<br>• Entering the **file-access** keyword enables network file share access. File servers in the server list are listed on the SSL VPN portal page when this keyword is enabled.<br>• Entering the **file-browse** keyword enables browse permissions for server and file shares. The file-access function must be enabled in order to also use this function.<br>• Entering the **file-entry** keyword enables "modify" permissions for files in the shares listed on the SSL VPN portal page. |

## Examples

### NBNS Server List Example

The following example, starting in global configuration mode, configures a server list for NBNS resolution:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)# exit
```

### File Share Permissions Example

The following example attaches the server list to and enables full file and network access permissions for policy group ONE:

```
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# nbns-list SERVER_LIST
Router(config-webvpn-group)# functions file-access
Router(config-webvpn-group)# functions file-browse
Router(config-webvpn-group)# functions file-entry
Router(config-webvpn-group)# end
```

## What to Do Next

Proceed to the next section to see information about configuring clientless remote access for Citrix-enabled applications.

# Configuring Citrix Application Support for Clientless Remote Access

Clientless Citrix support allows the remote user to run Citrix-enabled applications through the SSL VPN as if the application were locally installed (similar to traditional thin-client computing). Citrix applications run on a MetaFrame XP server (or server farm). The SSL VPN gateway provides access to the remote user. The applications run in real time over the SSL VPN. This task shows how to enable Citrix support for policy group remote users.

## ICA Client

The Independent Computing Architecture (ICA) client carries keystrokes and mouse clicks from the remote user to the MetaFrame XP server. ICA traffic is carried over TCP port number 1494. This port is opened when a Citrix application is accessed. If multiple application are accessed, the traffic is carried over a single TCP session.

## Prerequisites

- A Citrix Metaframe XP server is operational and reachable from the SSL VPN gateway over TCP/IP.
- SSL VPN gateway and context configurations are enabled and operational.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
4. **webvpn context** *name*
5. **policy group** *name*
6. **citrix enabled**
7. **filter citrix** *extended-acl*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **access-list** *access-list-number* {**permit** \| **deny**} *protocol source destination*<br><br>**Example:**<br>`Router (config)# access-list 100 permit ip 192.168.1.0 0.255.255.255 any` | Configures the access list mechanism for filtering frames by protocol type or vendor code. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **Step 5** | **policy group** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# policy group ONE` | Enters webvpn group policy configuration mode to configure a group policy. |
| **Step 6** | **citrix enabled**<br><br>**Example:**<br>`Router(config-webvpn-group)# citrix enabled` | Enables Citrix application support for remote users in a policy group. |
| **Step 7** | **filter citrix** *extended-acl*<br><br>**Example:**<br>`Router(config-webvpn-group)# filter citrix 100` | Configures a Citrix Thin Client filter.<br>• An extended access list is configured to define the Thin Client filter. This filter is used to control remote user access to Citrix applications. |

## Examples

The following example, starting in global configuration mode, enables Citrix application support for remote users with a source IP address in the 192.168.1.0/24 network:

```
Router(config)# access-list 100 permit ip 192.168.1.0 0.255.255.255 any
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# citrix enabled
Router(config-webvpn-group)# filter citrix 100
```

## What to Do Next

Support for standard applications that use well-known port numbers, such as e-mail and Telnet, can be configured using the port forwarding feature. Proceed to the next section to see more information.

# Configuring Application Port Forwarding

Application port forwarding is configured for thin client mode SSL VPN. Port forwarding extends the cryptographic functions of the SSL-protected browser to provide remote access to TCP and UDP-based applications that use well-known port numbers, such as POP3, SMTP, IMAP, Telnet, and SSH.

When port forwarding is enabled, the hosts file on the SSL VPN client is modified to map the application to the port number configured in the forwarding list. The application port mapping is restored to default when the user terminates the SSL VPN session.

## Administrative Privileges on the Remote Client

When enabling port forwarding, the SSL VPN gateway will modify the hosts file on the PC of the remote user. Some software configurations and software security applications will detect this modification and prompt the remote user to select "Yes" to permit. To permit the modification, the remote user must have local administrative privileges.

**Note** There is a known compatibility issue with the encryption type and Java. If the Java port-forwarding applet does not download properly and the configuration line **ssl encryption 3des-sha1 aes-sha1** is present, you should remove the line from the webvpn gateway subconfiguration.

## Prerequisites

SSL VPN gateway and SSL VPN context configurations are enabled and operational.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **port-forward** *name*
5. **local-port** {*number* **remote-server** *name* **remote-port** *number* **description** *text-string*}
6. **exit**
7. **policy group** *name*
8. **port-forward** *name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **port-forward** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# port-forward EMAIL` | Enters webvpn port-forward list configuration mode to configure a port forwarding list. |
| **Step 5** | **local-port** {*number* **remote-server** *name* **remote-port** *number* **description** *text-string*}<br><br>**Example:**<br>`Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com remote-port 110 description POP3` | Remaps (forwards) an application port number in a port forwarding list.<br>• The remote port number is the well-known port to which the application listens. The local port number is the entry configured in the port forwarding list. A local port number can be configured only once in a given port forwarding list. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Router(config-webvpn-port-fwd)# exit` | Exits webvpn port-forward list configuration mode, and enters webvpn context configuration mode. |
| **Step 7** | **policy group** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# policy group ONE` | Enters webvpn group policy configuration mode to configure a group policy. |
| **Step 8** | **port-forward** *name*<br><br>**Example:**<br>`Router(config-webvpn-group)# port-forward EMAIL` | Attaches a port forwarding list to a policy group configuration. |

## Examples

The following example, starting in global configuration mode, configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail1.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail2.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail3.company.com
remote-port 143 description IMAP
Router(config-webvpn-port-fwd)# exit
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# port-forward EMAIL
Router(config-webvpn-group)# end
```

# Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files

The SSL VPN gateway is preconfigured to distribute Cisco Secure Desktop (CSD) and/or Cisco AnyConnect VPN Client software package files to remote users. The files are distributed only when CSD or Cisco AnyConnect VPN Client support is needed. The administrator performs the following tasks to prepare the gateway:

- The current software package is downloaded from www.cisco.com.
- The package file is copied to a local file system.
- The package file is installed for distribution by configuring the **webvpn install** command.

## Remote Client Software Installation Requirements

The remote user must have administrative privileges, and the JRE for Windows version 1.4 or later must be installed before the CSD client package can be installed.

For Cisco AnyConnect VPN Client software installation, the remote user must have either the Java Runtime Environment for Windows (version 1.4 or later), or the browser must support or be configured to permit Active X controls.

### Remote PC System Requirements

The AnyConnect client supports the following operating systems on the remote PC:

- Microsoft Visa
- Microsoft Windows 2000
- Microsoft Windows XP
- MAC Intel
- MAC Power PC
- Linux

The legacy SSL VPN Client (SVC) supports the following operating systems on the remote PC:

- Microsoft Windows 2000
- Microsoft Windows XP

## Software Package Download

The latest versions of the CSD and Cisco AnyConnect VPN Client software client packages should be installed for distribution on the SSL VPN gateway.

The CSD software package can be downloaded at the following URL:

- http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

The Cisco AnyConnect VPN Client software package can be downloaded at the following URL:

- http://www.cisco.com/cgi-bin/tablebuild.pl/SSL VPNclient

**Note** You will be prompted to enter your login name and password to download these files from Cisco.com.

## Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- Software installation packages are copied to a local files system, such as flash memory.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn install** [**csd** *location-name* | **svc** *location-name*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn install** [**csd** *location-name* \| **svc** *location-name*]<br><br>**Example:**<br>`Router(config)# webvpn install svc flash:/webvpn/svc.pkg` | Installs a CSD or Cisco AnyConnect VPN Client package file to an SSL VPN gateway for distribution to remote users.<br>• The CSD and Cisco AnyConnect VPN Client software packages are pushed to remote users as access is needed. |

## Examples

The following example, starting in global configuration mode, installs the Cisco AnyConnect VPN Client package to an SSL VPN gateway:

```
Router(config)# webvpn install svc flash:/webvpn/svc.pkg
SSL VPN Package SSL-VPN-Client : installed successfully
```

The following example, starting in global configuration mode, installs the CSD package to an SSL VPN gateway:

```
Router(config)# webvpn install csd flash:/securedesktop_10_1_0_9.pkg
SSL VPN Package Cisco-Secure-Desktop : installed successfully
```

## What to Do Next

Support for CSD and Cisco AnyConnect VPN Client can be enabled for remote users after the gateway has been prepared to distribute CSD or Cisco AnyConnect VPN Client software.

# Configuring Cisco Secure Desktop Support

CSD provides a session-based interface where sensitive data can be shared for the duration of an SSL VPN session. All session information is encrypted. All traces of the session data are removed from the remote client when the session is terminated, even if the connection is terminated abruptly. CSD support for remote clients is enabled in this task.

## Java Runtime Environment

The remote user (PC or device) must have administrative privileges, and the JRE for Windows version 1.4 or later must be installed before the CSD client packages can be installed.

## Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- The CSD software package is installed for distribution on the SSL VPN gateway.

  See the "Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files" section if you have not already prepared the SSL VPN gateway to distribute CSD software.

## Restrictions

- Only Microsoft Windows 2000 and Windows XP are supported on the remote client.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **csd enable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **Step 4** | **csd enable**<br><br>**Example:**<br>`Router(config-webvpn-context)# csd enable` | Enables CSD support for SSL VPN sessions. |

## What to Do Next

Upon competition of this task, the SSL VPN gateway has been configured to provide clientless and thin client support for remote users. The SSL VPN feature also has the capability to provide full VPN access (similar to IPsec). Proceed to the next section to see more information.

# Configuring Cisco AnyConnect VPN Client Full Tunnel Support

The Cisco AnyConnect VPN Client is an application that allows a remote user to establish a full VPN connection similar to the type of connection that is established with an IPsec VPN. Cisco AnyConnect VPN Client software is pushed (downloaded) and installed automatically on the PC of the remote user. The Cisco AnyConnect VPN Client uses SSL to provide the security of an IPsec VPN without the complexity required to install IPsec in your network and on remote devices. The following tasks are completed in this configuration:

- An access list is applied to the tunnel to restrict VPN access.
- Cisco AnyConnect VPN Client tunnel support is enabled.
- An address pool is configured for assignment to remote clients.
- The default domain is configured.
- DNS is configured for Cisco AnyConnect VPN Client tunnel clients.
- Dead peer timers are configured the SSL VPN gateway and remote users.
- The login home page is configured.
- The Cisco AnyConnect VPN Client software package is configured to remain installed on the remote client.
- Tunnel key refresh parameters are defined.

## Remote Client Software from the SSL VPN Gateway

The Cisco AnyConnect VPN Client software package is pushed from the SSL VPN gateway to remote clients when support is needed. The remote user (PC or device) must have either the Java Runtime Environment for Windows (version 1.4 later), or the browser must support or be configured to permit Active X controls. In either scenario, the remote user must have local administrative privileges.

## The Address Pool

The address pool is first defined with the **ip local pool** command in global configuration mode. The standard configuration assumes that the IP addresses in the pool are reachable from a directly connected network.

### Address Pools for Nondirectly Connected Networks

If you need to configure an address pool for IP addresses from a network that is not directly connected, perform the following steps:

1. Create a local loopback interface and configure it with an IP address and subnet mask from the address pool.
2. Configure the address pool with the **ip local pool** command. The range of addresses must fall under the subnet mask configured in Step 1.
3. Set up the route. If you are using the Routing Information Protocol (RIP), configure the **router rip** command and then the **network** command, as usual, to specify a list of networks for the RIP process. If you are using the Open Shortest Path First (OSPF) protocol, configure the **ip ospf network point-to-point** command in the loopback interface. As a third choice (instead of using the RIP or OSPF protocol), you can set up static routes to the network.
4. Configure the **svc address-pool** command with the name configured in Step 2.

See the examples in this section for a complete configuration example.

## A Manual Entry to the IP Forwarding Table

If the SSL VPN software client is unable to update the IP forwarding table on the PC of the remote user, the following error message will be displayed in the router console or syslog:

```
Error : SSL VPN client was unable to Modify the IP forwarding table ......
```

This error can occur if the remote client does not have a default route. You can work around this error by performing the following steps:

1. Open a command prompt (DOS shell) on the remote client.
2. Enter the **route print** command.
3. If a default route is not displayed in the output, enter the **route** command followed by the **add** and **mask** keywords. Include the default gateway IP address at the end of the route statement. See the following example:

   ```
   C:\>route ADD 0.0.0.0 MASK 0.0.0.0 10.1.1.1
   ```

## Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- The Cisco AnyConnect VPN Client software package is installed for distribution on the SSL VPN gateway.
- The remote client has administrative privileges. Administrative privileges are required to download the SSL VPN software client.

  See the "Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files" section if you have not already prepared the SSL VPN gateway to distribute SSL VPN software.

## Restrictions

- Only Microsoft Windows 2000 and Windows XP are supported on the remote client.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **filter tunnel** *extended-acl*
6. **functions** {**file-access** | **file-browse** | **file-entry** | **svc-enabled** | **svc-required**}
7. **svc address-pool** *name*
8. **svc default-domain** *name*
9. **svc dns-server** {**primary** | **secondary**} *ip-address*
10. **svc dpd-interval** {**client** | **gateway**} *seconds*
11. **svc homepage** *string*
12. **svc keep-client-installed**
13. **svc rekey** {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **Step 4** | **policy group** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# policy group ONE` | Enters webvpn group policy configuration mode to configure a group policy. |
| **Step 5** | **filter tunnel** *extended-acl*<br><br>**Example:**<br>`Router(config-webvpn-group)# filter tunnel 101` | Configures an SSL VPN tunnel access filter.<br>• The tunnel access filter is used control network and application level access. The tunnel filter is also defined in an extended access list. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **functions** {**file-access** \| **file-browse** \| **file-entry** \| **svc-enabled** \| **svc-required**}<br><br>**Example:**<br>`Router(config-webvpn-group)# functions svc-enabled`<br>`Router(config-webvpn-group)# functions svc-required` | Configures Cisco AnyConnect VPN Client tunnel mode support.<br>• Entering the **svc-enabled** keyword enables tunnel support for the remote user. If the Cisco AnyConnect VPN Client software package fails to install, the remote user can continue to use clientless mode or thin-client mode.<br>• Entering the **svc-required** keyword enables only tunnel support for the remote user. If the Cisco AnyConnect VPN Client software package fails to install (on the PC of the remote user), the other access modes cannot be used. |
| **Step 7** | **svc address-pool** *name*<br><br>**Example:**<br>`Router(config-webvpn-group)# svc address-pool ADDRESSES` | Configures configure a pool of IP addresses to assign to remote users in a policy group.<br>• The address pool is first defined with the **ip local pool** command in global configuration mode.<br>• If you are configuring an address pool for a network that is not directly connected, an address from the pool must be configured on a locally loopback interface. See the third example at the end of this section. |
| **Step 8** | **svc default-domain** *name*<br><br>**Example:**<br>`Router(config-webvpn-group)# svc default-domain cisco.com` | Configures the default domain for a policy group. |
| **Step 9** | **svc dns-server** {**primary** \| **secondary**} *ip-address*<br><br>**Example:**<br>`Router(config-webvpn-group)# svc dns-server primary 192.168.3.1`<br>`Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1` | Configures DNS servers for policy group remote users. |
| **Step 10** | **svc dpd-interval** {**client** \| **gateway**} *seconds*<br><br>**Example:**<br>`Router(config-webvpn-group)# svc dpd-interval gateway 30`<br>`Router(config-webvpn-group)# svc dpd-interval client 300` | Configures the dead peer detection (DPD) timer value for the gateway or client.<br>• The DPD timer is reset every time a packet is received over the SSL VPN tunnel from the gateway or remote user. |
| **Step 11** | **svc homepage** *string*<br><br>**Example:**<br>`Router(config-webvpn-group)# svc homepage www.cisco.com` | Configures configure the URL of the web page that is displayed upon successful user login.<br>• The *string* argument is entered as an HTTP URL. The URL can be up to 255 characters in length. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 12** | **svc keep-client-installed**<br><br>**Example:**<br>`Router(config-webvpn-group)# svc keep-client-installed` | Configures the remote user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled. |
| **Step 13** | **svc rekey** {**method** {**new-tunnel** \| **ssl**} \| **time** *seconds*}<br><br>**Example:**<br>`Router(config-webvpn-group)# svc rekey method new-tunnel`<br>`Router(config-webvpn-group)# svc rekey time 3600` | Configures the time and method that a tunnel key is refreshed for policy group remote users.<br>• The tunnel key is refreshed by renegotiating the SSL connection or initiating a new tunnel connection.<br>• The time interval between tunnel refresh cycles is configured in seconds. |

# Examples

### Tunnel Filter Configuration

The following example, starting in global configuration mode, configures a deny access filter for any host from the 172.16.2/24 network:

```
Router(config)# access-list 101 deny ip 172.16.2.0 0.0.0.255 any
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# filter tunnel 101
Router(config-webvpn-group)# end
```

### Address Pool (Directly Connected Network) Configuration

The following example, starting in global configuration mode, configures the 192.168.1/24 network as an address pool:

```
Router(config)# ip local pool ADDRESSES 192.168.1.1 192.168.1.254
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

### Address Pool (Nondirectly Connected Network) Configuration

The following example, starting in global configuration mode, configures the 172.16.1/24 network as an address pool. Because the network is not directly connected, a local loopback interface is configured.

```
Router(config)# interface loopback 0
Router(config-int)# ip address 172.16.1.126 255.255.255.0
Router(config-int)# no shutdown
Router(config-int)# exit
Router(config)# ip local pool ADDRESSES 172.16.1.1 172.16.1.254
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

#### Full Tunnel Configuration

The following example, starting in global configuration mode, configures full Cisco AnyConnect VPN Client tunnel support on an SSL VPN gateway:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# functions svc-required
Router(config-webvpn-group)# svc default-domain cisco.com
Router(config-webvpn-group)# svc dns-server primary 192.168.3.1
Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1
Router(config-webvpn-group)# svc dpd-interval gateway 30
Router(config-webvpn-group)# svc dpd-interval client 300
Router(config-webvpn-group)# svc homepage www.cisco.com
Router(config-webvpn-group)# svc keep-client-installed
Router(config-webvpn-group)# svc rekey method new-tunnel
Router(config-webvpn-group)# svc rekey time 3600
Router(config-webvpn-group)# end
```

### What to Do Next

Proceed to the next section to see advanced Cisco AnyConnect VPN Client tunnel configuration information.

## Configuring Advanced SSL VPN Tunnel Features

This section describes advanced Cisco AnyConnect VPN Client tunnel configurations. The following configuration steps are completed in this task:

- Split tunnel support and split DNS resolution are enabled on the SSL VPN gateway.
- SSL VPN gateway support for Microsoft Internet Explorer proxy settings is configured.
- WINS resolution is configured for Cisco AnyConnect VPN Client tunnel clients.

### Microsoft Internet Explorer Proxy Configuration

The SSL VPN gateway can be configured to pass or bypass Microsoft Internet Explorer (MSIE) proxy settings. Only HTTP proxy settings are supported by the SSL VPN gateway. MSIE proxy settings have no effect on any other supported browser.

### Split Tunneling

Split tunnel support allows you to configure a policy that permits specific traffic to be carried outside of the Cisco AnyConnect VPN Client tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the Internet Service Provider [ISP] or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the same time. Entering the **local-lans** keyword permits the remote user to access resources on a local LAN, such as network printer.

### Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.

- The Cisco AnyConnect VPN Client software package is installed for distribution on the SSL VPN gateway.

## Restrictions

- Only Microsoft Windows 2000 and Windows XP are supported on the remote client.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **svc split exclude** {{*ip-address mask* | **local-lans**} | **include** *ip-address mask*}
6. **svc split dns** *name*
7. **svc msie-proxy** {**exception** *host* | **option** {**auto** | **bypass-local** | **none**}}
8. **svc msie-proxy server** *host*
9. **svc wins-server** {**primary** | **secondary**} *ip-address*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **Step 4** | **policy group** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# policy group ONE` | Enters webvpn group policy configuration mode to configure a group policy. |
| **Step 5** | **svc split exclude** {{*ip-address mask* \| **local-lans**} \| **include** *ip-address mask*}<br><br>**Example:**<br>`Router(config-webvpn-group)# svc split exclude 192.168.1.1 0.0.0.255`<br>`Router(config-webvpn-group)# svc split include 172.16.1.0 255.255.255.0` | Configures split tunneling for policy group remote users.<br>• Split tunneling is configured to include or exclude traffic in the Cisco AnyConnect VPN Client tunnel. Traffic that is included is sent over the SSL VPN tunnel. Traffic is excluded is resolved outside of the tunnel.<br>• Exclude and include statements are configured with IP address/wildcard mask pairs. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **svc split dns** *name*<br><br>**Example:**<br>`Router(config-webvpn-group)# svc split dns www.cisco.com`<br>`Router(config-webvpn-group)# svc split dns my.company.com` | Configures the SSL VPN gateway to resolve the specified fully qualified DNS names through the Cisco AnyConnect VPN Client tunnel.<br>• A default domain was configured in the previous task with the **svc default-domain** command. DNS names configured with the **svc split dns** command are configured in addition.<br>• Up to 10 split DNS statements can be configured. |
| **Step 7** | **svc msie-proxy** {**exception** *host* \| **option** {**auto** \| **bypass-local** \| **none**}}<br><br>**Example:**<br>`Router(config-webvpn-group)# svc msie-proxy option auto`<br>`Router(config-webvpn-group)# svc msie-proxy exception www.cisco.com`<br>`Router(config-webvpn-group)# svc msie-proxy exception 10.20.20.1` | Configures configure MSIE browser proxy settings for policy group remote users.<br>• Entering the **option auto** keywords configures the browser of the remote user to auto-detect proxy settings.<br>• Entering the **option bypass-local** keywords configures local addresses to bypass the proxy.<br>• Entering the **option none** keywords configures the browser on the remote client to not use a proxy. |
| **Step 8** | **svc msie-proxy server** *host*<br><br>**Example:**<br>`Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80` | Specifies an MSIE proxy server for policy group remote users.<br>• The proxy server is specified by entering an IP address or a fully qualified domain name. |
| **Step 9** | **svc wins-server** {**primary** \| **secondary**} *ip-address*<br><br>**Example:**<br>`Router(config-webvpn-group)# svc wins-server primary 172.31.1.1`<br>`Router(config-webvpn-group)# svc wins-server secondary 172.31.2.1` | Configures WINS servers for policy group remote users. |

# Examples

### Split DNS Configuration

The following example, starting in global configuration mode, configures the following DNS names to be resolved in the Cisco AnyConnect VPN Client tunnel:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc split dns www.example.com
Router(config-webvpn-group)# svc split dns my.company.com
```

### Including and Excluding IP Prefixes

The following example configures a list of IP addresses to be resolved over the tunnel (included) and a list to be resolved outside of the tunnel (excluded):

```
Router(config-webvpn-group)# svc split exclude 192.168.1.0 255.255.255.0
Router(config-webvpn-group)# svc split include 172.16.1.0 255.255.255.0
```

#### MSIE Proxy Configuration

The following example configures MSIE proxy settings:

```
Router(config-webvpn-group)# svc msie-proxy option auto
Router(config-webvpn-group)# svc msie-proxy exception www.example.com
Router(config-webvpn-group)# svc msie-proxy exception 10.20.20.1
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
```

#### WINS Server Configuration

The following example configures primary and secondary WINS servers for the policy group:

```
Router(config-webvpn-group)# svc wins-server primary 172.31.1.1
Router(config-webvpn-group)# svc wins-server secondary 172.31.2.1
Router(config-webvpn-group)# svc wins-server secondary 172.31.3.1
Router(config-webvpn-group)# end
```

# Configuring VRF Virtualization

VRF Virtualization allows you to associate a traditional VRF with an SSL VPN context configuration. This feature allows you to apply different configurations and reuse address space for different groups of users in your organization.

## Prerequisites

- A VRF has been configured in global configuration mode.
- SSL VPN gateway and context configurations are enabled and operational.
- A policy group has been configured and associated with the WebVPN context.

## Restrictions

- Only a single VRF can be configured for each SSL VPN context configuration.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **vrf-name** *name*

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router(config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **Step 4** | **vrf-name** *name*<br><br>**Example:**<br>`Router(config-webvpn-context)# vrf-name BLUE` | Associates a VRF with an SSL VPN context. |

## Examples

The following example, starting in global configuration mode, associates the VRF under the SSL VPN context configuration:

```
Router(config)# ip vrf BLUE
Router(config-vrf)# rd 10.100.100.1
Router(config-vrf)# exit
Router(config)# webvpn context BLUE
Router(config-webvpn-context)# policy group BLUE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy BLUE
Router(config-webvpn-context)# vrf-name BLUE
Router(config-webvpn-context)# end
```

# Configuring ACL Rules

To configure ACL rules on the application layer level for an individual user, perform the following tasks.

**Note**

- The ACL rules can be overridden for an individual user when the user logs on to the gateway (using AAA policy attributes).
- If a user session has no ACL attribute configured, all application requests from that user session are permitted by default.

## Prerequisites

Before configuring the ACL rules, you must have first configured the time range using the **time-range** command (this prerequisite is in addition to optionally configuring the time range, in the task table below, as part of the **permit** or **deny** entries).

## Restrictions

There is no limitation on the maximum number of filtering rules that can be configured for each ACL entry, but keeping the number below 50 should have no significant impact on router performance.

### SUMMARY STEPS

#### Required Steps

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **acl** *acl-name*
5. **permit** [**url** [**any** | ***url-string***]] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | ***source-ip source-mask***] [**any** | ***destination-ip destination-mask***] **[time-range** ***time-range-name*****]** [**syslog**]

   or

   **deny** [**url** [**any** | ***url-string***]] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | ***source-ip source-mask***] [**any** | ***destination-ip destination-mask***] [**time-range** ***time-range-name***] [**syslog**]

#### Optional Steps

6. **add** *position acl-entry*
7. **error-url** *access-deny-page-url*
8. **error-msg** *message-string*
9. **list**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Required Steps** | | |
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router (config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **Step 4** | **acl** *acl-name*<br><br>**Example:**<br>`Router (config-webvpn-context)# acl acl1` | Defines the ACL and enters webvpn acl configuration modes. |
| **Step 5** | **permit** [**url** [**any** \| *url-string*]] [**ip** \| **tcp** \| **udp** \| **http** \| **https** \| **cifs**] [**any** \| *source-ip source-mask*] [**any** \| *destination-ip destination-mask*] **time-range** {*time-range-name*} [**syslog**]<br><br>or<br><br>**deny** [**url** [**any** \| *url-string*]] [**ip** \| **tcp** \| **udp** \| **http** \| **https** \| **cifs**] [**any** \| *source-ip source-mask*] [**any** \| *destination-ip destination-mask*] [**time-range** *time-range-name*] [**syslog**]<br><br>**Example:**<br>`Router (config-webvpn-acl)# permit url any` | Sets conditions in a named SSL VPN access list that will permit or deny packets. |
| **Optional Steps** | | |
| **Step 6** | **add** *position acl-entry*<br><br>**Example:**<br>`Router (config-webvpn-acl)# add 3 permit url any` | Adds an ACL entry at a specified position. |
| **Step 7** | **error-url** *access-deny-page-url*<br><br>**Example:**<br>`Router (config-webvpn-acl)# error-url "http://www.example.com"` | Defines a URL as an ACL violation page.<br>• If the **error-url** command is configured, the user is redirected to a predefined URL for every request that is not allowed. If the **error-url** command is not configured, the user gets a standard, gateway-generated error page. |
| **Step 8** | **error-msg** *message-string*<br><br>**Example:**<br>`Router (config-webvpn-acl)# error-msg "If you have any questions, please contact <a href+mailto:employee1@example.com>Employee1</a> ."` | Displays a specific error message when a user logs on and his or her request is denied. |
| **Step 9** | **list**<br><br>**Example:**<br>`Router (config-webvpn-acl)# list` | Lists the currently configured ACL entries sequentially and assigns a position number. |

# Associating an ACL Attribute with a Policy Group

To associate an ACL attribute with a policy group, perform the following steps.

**Note**

- Associating an ACL attribute for an individual user must be performed as part of a AAA operation.
- The ACL rules can be overridden for an individual user when the user logs on to the gateway (using AAA policy attributes).
- If a user session has no ACL attribute configured, all application requests from that user session are permitted by default.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **exit**
6. **acl** *acl-name*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router (config)# webvpn context context1` | Configures the SSL VPN context and enters webvpn context configuration mode. |
| **Step 4** | **policy group** *name*<br><br>**Example:**<br>`Router (config-webvpn-context)# policy group group1` | Defines a policy that can be applied to the user and enters webvpn policy group configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **exit**<br><br>**Example:**<br>`Router (config-webvpn-group)# exit` | Exits webvpn policy group configuration mode. |
| **Step 6** | **acl** *acl-name*<br><br>**Example:**<br>`Router (config-webvpn-context)# acl acl1` | Defines the ACL and enters webvpn acl configuration mode. |

## Monitoring and Maintaining ACLs

To monitor and maintain your ACL configuration, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **debug webvpn acl**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **debug webvpn acl**<br><br>**Example:**<br>`Router# debug webvpn acl` | Displays information about ACLs. |

# Configuring SSO Netegrity Cookie Support for a Virtual Context

To configure SSO Netegrity cookie support, perform the following steps.

## Prerequisites

- A Cisco plug-in must first be installed on a Netegrity server.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **sso-server** *name*

5. **web-agent-url** *url*
6. **secret-key** *key-name*
7. **max-retry-attempts** *number-of-retries*
8. **request-timeout** *number-of-seconds*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router (config)# webvpn context context1` | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **Step 4** | **sso-server** *name*<br><br>**Example:**<br>`Router (config-webvpn-context)# sso-server "test-sso-server"` | Creates a SSO server name under an SSL VPN context and enters webvpn sso server configuration mode |
| **Step 5** | **web-agent-url** *url*<br><br>**Example:**<br>`Router (config-webvpn-sso-server)# web-agent-url http://www.example.comwebvpn/` | Configures the Netegrity agent URL to which SSO authentication requests will be dispatched. |
| **Step 6** | **secret-key** *key-name*<br><br>**Example:**<br>`Router (config-webvpn-sso-server)# secret-key "12345"` | Configures the policy server secret key that is used to secure authentication requests. |
| **Step 7** | **max-retry-attempts** *number-of-retries*<br><br>**Example:**<br>`Router (config-webvpn-sso-server)# max-retry-attempts 3` | Sets the maximum number of retries before SSO authentication fails. |
| **Step 8** | **request-timeout** *number-of-seconds*<br><br>**Example:**<br>`Router (config-webvpn-sso-server)# request-timeout 15` | Sets the number of seconds before an authentication request times out. |

# Associating an SSO Server with a Policy Group

To associate an SSO server with a policy group, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **sso-server** *name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router (config)# webvpn context context1` | Configures the SSL VPN context and enters webvpn context configuration mode. |
| **Step 4** | **policy group** *name*<br><br>**Example:**<br>`Router (config-webvpn-context)# policy group ONE` | Configures a group policy and enters webvpn group policy configuration mode. |
| **Step 5** | **sso-server** *name*<br><br>**Example:**<br>`Router (config-group-webvpn)# sso-server "test-sso-server"` | Attaches an SSO server to a policy group. |

# Configuring URL Obfuscation (Masking)

To configure URL obfuscation, masking, for a policy group, perform the following steps.

### SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **mask-urls**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router (config)# webvpn context context1` | Configures the SSL VPN context and enters webvpn context configuration mode. |
| **Step 4** | **policy group** *name*<br><br>**Example:**<br>`Router (config-webvpn-context)# policy group ONE` | Configures a group policy and enters group policy configuration mode. |
| **Step 5** | **mask-urls**<br><br>**Example:**<br>`Router (config-webvpn-group)# mask-urls` | Obfuscates, or masks, sensitive portions of an enterprise URL, such as IP addresses, hostnames, or port numbers. |

# Adding a CIFS Server URL List to an SSL VPN Context and Attaching It to a Policy Group

To add a CIFS server URL list to an SSL VPN context and attach it to a policy group, perform the following steps.

## Prerequisites

Before adding a CIFS server URL list to an SSL VPN context, you must have already set up the Web VPN context using the **webvpn context** command, and you must be in webvpn context configuration mode.

### SUMMARY STEPS

1. **cifs-url-list** *name*

2. **heading** *text-string*
3. **url-text** *name*
4. **end**
5. **policy group** *name*
6. **cifs-url-list** *name*
7. **end**
8. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cifs-url-list** *name*<br><br>**Example:**<br>`Router (config-webvpn-context) cifs-url-list c1` | Enters webvpn URL list configuration mode to configure a list of CIFS server URLs to which a user has access on the portal page of an SSL VPN. |
| **Step 2** | **heading** *text-string*<br><br>**Example:**<br>`Router (config-webvpn-url) heading "cifs-url"` | Configures the heading that is displayed above URLs listed on the portal page of an SSL VPN. |
| **Step 3** | **url-text** *name*<br><br>**Example:**<br>`Router (config-webvpn-url)# url-text "SSLVPN-SERVER2" url-value "\\SLVPN-SERVER2"` | Adds an entry to a URL list.<br>• More than one entry can be added by reentering the **url-text** command for each subsequent entry. |
| **Step 4** | **end**<br><br>**Example:**<br>`Router (config-webvpn-url)# end` | Exits webvpn URL list configuration mode. |
| **Step 5** | **policy group** *name*<br><br>**Example:**<br>`Router (config)# policy group ONE` | Enters webvpn group policy configuration mode to configure a group policy. |
| **Step 6** | **cifs-url-list** *name*<br><br>**Example:**<br>`Router (config-webvpn-group)# cifs-url-list "c1"` | Attaches a URL list to a policy group. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **end**<br><br>**Example:**<br>`Router (config-webvpn-group)# end` | Exits webvpn group policy configuration mode. |
| **Step 8** | **end**<br><br>**Example:**<br>`Router (config)# end` | Exits global configuration mode. |

# Configuring User-Level Bookmarks

To configure user-level bookmarks, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **user-profile location flash:***directory*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **webvpn context** *name*<br><br>**Example:**<br>`Router (config)# webvpn context context1` | Configures the SSL VPN context and enters webvpn context configuration mode. |
| **Step 4** | **user-profile location flash:***directory*<br><br>**Example:**<br>`Router (config-webvpn-context)# user-profile location flash:webvpn/sslvpn/vpn_context/` | Stores bookmarks on a directory. |

# Configuring FVRF

To configure FVRF so that the SSL VPN gateway is fully integrated into an MPLS network, perform the following steps.

## Prerequisites

As the following configuration task shows, IP VRF must be configured before the FVRF can be associated with the SSL VPN gateway. For more information about configuring IP VRF, see the subsection "Configuring IP VRF (**ip vrf** command)" in the "Related Documents" section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **end**
5. **webvpn gateway** *name*
6. **vrfname** *name*
7. **end**
8. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip vrf** *vrf-name*<br><br>**Example:**<br>`Router (config)# ip vrf vrf_1` | Defines a VPN VRF instance and enters VRF configuration mode.<br>**Note** The *vrf-name* argument specified here must be the same as the name arguement in Step 6. |
| **Step 4** | **end**<br><br>**Example:**<br>`Router (config-vrf)# end` | Exits VRF configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **webvpn gateway** *name*<br><br>**Example:**<br>`Router (config)# webvpn gateway mygateway` | Enters webvpn gateway configuration mode to configure an SSL VPN gateway. |
| **Step 6** | **vrfname** *name*<br><br>**Example:**<br>`Router (config-webvpn-gateway)# vrfname vrf_1` | Associates a VPN FVRF with an SSL VPN gateway.<br>**Note** The *name* argument here must the same as the *vrf-name* argument in Step 3. |
| **Step 7** | **end**<br><br>**Example:**<br>`Router (config-webvpn-gateway)# end` | Exits webvpn gateway configuration mode. |
| **Step 8** | **end**<br><br>**Example:**<br>`Router (config)# end` | Exits global configuration mode. |

# Using SSL VPN Clear Commands

This section describes **clear** commands that are used to perform the following tasks:

- Clear NBNS cache information
- Clear remote user sessions
- Clear (or reset) SSL VPN application and access counters

### SUMMARY STEPS

1. **enable**
2. **clear webvpn nbns** [**context** {*name* | **all**}]
3. **clear webvpn session** [**user** *name*] **context** {*name* | **all**}
4. **clear webvpn stats** [[**cifs** | **citrix** | **mangle** | **port-forward** | **sso** | **tunnel**] [**context** {*name* | **all**}]]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **clear webvpn nbns** [**context** {*name* \| **all**}]<br><br>**Example:**<br>`Router# clear webvpn nbns context all` | Clears the NBNS cache on an SSL VPN gateway. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **clear webvpn session** [**user** *name*] **context** {*name* \| **all**}<br><br>**Example:**<br>`Router# clear webvpn session context all` | Clears SSL VPN remote user sessions. |
| **Step 4** | **clear webvpn stats** [[**cifs** \| **citrix** \| **mangle** \| **port-forward** \| **sso** \| **tunnel**] [**context** {*name* \| **all**}]]<br><br>**Example:**<br>`Router# clear webvpn stats` | Clears SSL VPN application and access counters. |

# Verifying SSL VPN Configurations

This section describes show commands that are used to verify the following:

- SSL VPN gateway configuration
- SSL VPN context configuration
- CSD and Cisco AnyConnect VPN Client installation status
- NetBIOS name services information
- SSL VPN group policy configuration
- SSL VPN user session information
- SSL VPN application statistics

## SUMMARY STEPS

1. **enable**
2. **show webvpn context** [*name*]
3. **show webvpn gateway** [*name*]
4. **show webvpn install** {**file** *name* | **package** {**csd** | **svc**} | **status** {**csd** | **svc**}}
5. **show webvpn nbns** {**context** {**all** | *name*}}
6. **show webvpn policy group** *name* **context** {**all** | *name*}
7. **show webvpn session** {[**user** *name*] **context** {**all** | *name*}}
8. **show webvpn stats** [**cifs** | **citrix** | **mangle** | **port-forward** | **sso** | **tunnel**] [**detail**] [**context** {**all** | *name*}]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show webvpn context** [*name*]<br><br>**Example:**<br>`Router# show webvpn context` | Displays the operational status and configuration parameters for SSL VPN context configurations. |
| **Step 3** | **show webvpn gateway** [*name*]<br><br>**Example:**<br>`Router# show webvpn gateway` | Displays the status of the SSL VPN gateway. |
| **Step 4** | **show webvpn install** {**file** *name* \| **package** {**csd** \| **svc**} \| **status** {**csd** \| **svc**}}<br><br>**Example:**<br>`Router# show webvpn install status csd` | Displays the installation status of Cisco AnyConnect VPN Client or CSD client software packages. |
| **Step 5** | **show webvpn nbns** {**context** {**all** \| *name*}}<br><br>**Example:**<br>`Router# show webvpn nbns context all` | Displays information in the NetBIOS Name Service (NBNS) cache. |
| **Step 6** | **show webvpn policy group** *name* **context** {**all** \| *name*}<br><br>**Example:**<br>`Router# show webvpn policy group ONE context all` | Displays the context configuration associated with a policy group. |
| **Step 7** | **show webvpn session** {[**user** *name*] **context** {**all** \| *name*}}<br><br>**Example:**<br>`Router# show webvpn session context all` | Displays SSL VPN user session information. |
| **Step 8** | **show webvpn stats** [**cifs** \| **citrix** \| **mangle** \| **port-forward** \| **sso** \| **tunnel**] [**detail**] [**context** {**all** \| *name*}]<br><br>**Example:**<br>`Router# show webvpn stats tunnel detail context all` | Displays SSL VPN application and network statistics. |

# Using SSL VPN Debug Commands

To monitor and manage your SSL VPN configurations, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **debug webvpn** [**verbose**] [**aaa** | **acl** | **cifs** | **citrix** [**verbose**] | **cookie** [**verbose**] | **count** | **csd** | **data** | **dns** | **emweb** [**state**] | **entry** *context-name* [**source** *ip* [*network-mask*] | **user** *username*] | **http** [**authentication** | **trace** | **verbose**] | **package** | **sdps** [**level** *number*] | **sock** [**flow**] | **sso** | **timer** | **trie** | **tunnel** [**traffic** *acl-number* | **verbose**] | **url-disp** | **webservice** [**verbose**]]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **debug webvpn** [**verbose**] [**aaa** \| **acl** \| **cifs** \| **citrix** [**verbose**] \| **cookie** [**verbose**] \| **count** \| **csd** \| **data** \| **dns** \| **emweb** [**state**] \| **entry** *context-name* [**source** *ip* [*network-mask*] \| **user** *username*] \| **http** [**authentication** \| **trace** \| **verbose**] \| **package** \| **sdps** [**level** *number*] \| **sock** [**flow**] \| **sso** \| **timer** \| **trie** \| **tunnel** [**traffic** *acl-number* \| **verbose**] \| **url-disp** \| **webservice** [**verbose**]]<br><br>**Example:**<br>`Router# debug webvpn` | Enables the display of debug information for SSL VPN applications and network activity. |

# Remote User Guide

For information specifically for the remote user, see the document *SSL VPN Remote User Guide*.

# Configuration Examples for SSL VPN

This section includes the following configuration examples:

# Configuring a Generic SSL VPN Gateway: Example

The following output example shows that a generic SSL VPN gateway has been configured in privileged EXEC mode:

```
Router# show running-config

webvpn gateway SSL_gateway2
 ip address 10.1.1.1. port 442
 ssl trustpoint TP_self_signed _4138349635
 inservice
!
webvpn context SSL_gateway2
 ssl authenticate verify all
!
!
policy group default
default-group-policy default
 gateway SSL_gateway2
inservice
```

# Configuring an ACL: Example

The following output example shows the ACL is “acl1.” It has been associated with policy group “default.”

```
Router# show running-config

webvpn context context1
 ssl authenticate verify all
 !
 acl "acl1"
   error-msg "warning!!!..."
   permit url "http://www.example1.com"
   deny url "http://www.example2.com"
   permit http any any
 !
 nbns-list l1
   nbns-server 10.1.1.20
 !
 cifs-url-list "c1"
   heading "cifs-url"
   url-text "SSL VPN-SERVER2" url-value "\\SSL VPN-SERVER2"
   url-text "SSL-SERVER2" url-value "\\SSL-SERVER2"
 !
 policy group default
   acl "acl1"
   cifs-url-list "c1"
   nbns-list "l1"
   functions file-access
   functions file-browse
   functions file-entry
 default-group-policy default
 gateway public
 inservice
!
```

# Configuring HTTP Proxy: Example

The following output example shows that HTTP proxy has been configured and that the portal (home) page from URL “http://www.example.com” will automatically download the home page of the user:

```
Router# show running-config

webvpn context myContext
 ssl authenticate verify all
 !
 !
 port-forward "email"
   local-port 20016 remote-server "ssl-server1.SSL VPN-ios.com" remote-port 110
description "POP-ssl-server1"
 !
 policy group myPolicy
   port-forward "email" auto-download http-proxy proxy-url "http://www.example.com"
 inservice
```

# RADIUS Accounting for SSL VPN Sessions: Example

The following output example shows that RADIUS accounting has been configured for SSL VPN user sessions:

```
Router# show running-config

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
aaa new-model
!
!
aaa accounting network SSL VPNaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.16.2.133
ip name-server 172.16.11.48
!

line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
webvpn gateway GW1
 ip address 172.19.216.141 port 443
 inservice
 !
webvpn gateway SSL VPN
 no inservice
```

```
 !
webvpn install svc flash:/webvpn/svc.pkg
webvpn aaa accounting-list SSL VPNaaa
 !
webvpn context Default_context
 ssl encryption
 ssl authenticate verify all
 !
 no inservice
!
!
```

# URL Obfuscation (Masking): Example

The following output example shows that URL obfuscation (masking) has been configured for policy group "gp_urlobf."

```
Router: show running-config

!
!
policy group gp_urlobf
   mask-urls
 default-group-policy gp_urlobf
 gateway gw domain dom
 inservice
!
!
```

# Adding a CIFS Server URL List and Attaching It to a Policy List: Example

The following output example shows that the CIFS server URLs "SSLVPN-SERVER2" and "SSL-SERVER2" have been added as portal page URLs to which a user has access. The output also shows that the two servers have been attached to a policy group.

```
webvpn context context_1
 ssl authenticate verify all
 !
 acl "acl1"
   error-msg "warning!!!..."
   permit url "http://www.example1.com"
   deny url "http://www.example2.com"
   permit http any any
 !
 nbns-list l1
   nbns-server 10.1.1.20
 !
 cifs-url-list "c1"
   heading "cifs-url"
   url-text "SSLVPN-SERVER2" url-value "\\SSLVPN-SERVER2"
   url-text "SSL-SERVER2" url-value "\\SSL-SERVER2"
 !
 policy group default
   acl "acl1"
   cifs-url-list "c1"
   nbns-list "l1"
   functions file-access
   functions file-browse
   functions file-entry
```

```
 default-group-policy default
 gateway public
 inservice
!
```

# Typical SSL VPN Configuration: Example

The following output is an example of an SSL VPN configuration that includes most of the features that are available using SSL VPN:

```
Router# show running-config

hostname sslvpn
!
!
aaa new-model
!
!
aaa authentication login default local group radius
!
!
crypto pki trustpoint Gateway
 enrollment selfsigned
 ip-address 192.168.22.13
 revocation-check crl
 rsakeypair keys 1024 1024
!
!
crypto pki certificate chain Gateway
 certificate self-signed 02
!
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.0
!
!
interface GigabitEthernet0/1
 ip address 192.168.22.14 255.255.255.0 secondary
 ip address 192.168.22.13 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
!
ip local pool svc-pool 10.10.10.100 10.10.10.110
!
!
ip radius source-interface FastEthernet1/1
!
!
webvpn gateway ssl-vpn
 ip address 192.168.22.13 port 443
 http-redirect port 80
 ssl trustpoint Gateway
 inservice
 !
! The following line is required for SSLVPN Client.
webvpn install svc flash:/webvpn/svc.pkg
!
! The following line is required for Cisco Secure Desktop.
webvpn install csd flash:/webvpn/sdesktop.pkg
```

```
!
webvpn context ssl-vpn
 ssl authenticate verify all
!
 url-list "sslvpn-dt"
   url-text "sslvpn-dt" url-value "http://10.1.1.40"
   url-text "Exchange Server" url-value "http://10.1.1.40/exchange"
!
 sso-server "netegrity"
   web-agent-url "http://10.1.1.37/vpnauth/"
   secret-key "sslvpn1"
   retries 3
   timeout 15
!
 nbns-list cifs
   nbns-server 10.1.1.40
!
 port-forward "mail_test"
   local-port 30016 remote-server "mail.sslvpn-dt.com" remote-port 143 description
"IMAP-test"
   local-port 30017 remote-server "mail.sslvpn-dt.com" remote-port 110 description
"POP3-test"
   local-port 30018 remote-server "mail.sslvpn-dt.com" remote-port 25 description
"SMTP-test"
 !
 policy group default
! The following line applies the URL list.
   url-list "sslvpn-dt"
! The following line applies TCP port forwarding.
   port-forward "mail_test"
! The following line applies CIFS.
   nbns-list "cifs"
! The following line enables CIFS functionality.
   functions file-access
! The following line enables CIFS functionality.
   functions file-browse
! The following line enables CIFS functionality.
   functions file-entry
! The following line enables SSLVPN Client.
   functions svc-enabled
! The following line enables clientless Citrix.
   citrix enabled
 default-group-policy default
! The following line maps this context to the virtual gateway and defines the domain to
use.
 gateway ssl-vpn domain sslvpn
! The following line enables Cisco Secure Desktop.
 csd enable
 inservice
!
!
end
```

# debug Command Output: Examples

## Configuring SSO: Example

The following output example displays ticket creation, session setup, and response handling information for an SSO configuration:

```
Router# debug webvpn sso

*Jun 12 20:37:01.052: WV-SSO: Redirect to SSO web agent URL -
http://example.examplecompany.com/vpnauth/
*Jun 12 20:37:01.052: WV_SSO: Set session cookie with SSO redirect
*Jun 12 20:37:01.056: WV-SSO: Set SSO auth flag
*Jun 12 20:37:01.056: WV-SSO: Attach credentials - building auth ticket
*Jun 12 20:37:01.060: WV-SSO: user: [user11], secret: [secret123], version: [1.0], login
time: [BCEFC86D], session key: [C077F97A], SHA1 hash :
[B07D0A924DB33988D423AE9F937C1C5A66404819]
*Jun 12 20:37:01.060: WV-SSO: auth_ticket :
user11:1.0@C077F97A@BCEFC86D@B07D0A924DB33988D423AE9F937C1C5A66404819
*Jun 12 20:37:01.060: WV-SSO: Base64 credentials for the auth_ticket:
dXNlcjExOjEuMEBDMDc3Rjk3QUBCQ0VGQzg2REBCMDdEMEE5MjREQjMzOTg4RDQyM0FFOUY5MzdDMUM1QTY2NDA0OD
E5
*Jun 12 20:37:01.060: WV-SSO: Decoded credentials =
user11:1.0@C077F97A@BCEFC86D@B07D0A924DB33988D423AE9F937C1C5A66404819
*Jun 12 20:37:01.060: WV-SSO: Starting SSO request timer for 15-second

*Jun 12 20:37:01.572: WV-SSO: SSO auth response rcvd - status[200]
*Jun 12 20:37:01.572: WV-SSO: Parsed non-SM cookie: SMCHALLENGE
*Jun 12 20:37:01.576: WV-SSO: Parsed SMSESSION cookie
*Jun 12 20:37:01.576: WV-SSO: Sending logon page after SSO auth success
```

# show Command Output: Examples

The following examples display information about various SSL VPN features and scenarios:



### show webvpn context Example

The following is sample output from the **show webvpn context** command:

```
Router# show webvpn context

Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host
```

```
Context Name        Gateway  Domain/VHost      VRF      AS    OS
------------        -------  ------------      -------  ----  --------
Default_context     n/a      n/a               n/a      down  down
con-1               gw-1     one               -        up    up
con-2               -        -                 -        down  down
```

#### show webvpn context name Example

The following is sample output from the **show webvpn context** command, entered with the name of a specific SSL VPN context:

```
Router# show webvpn context context1

Admin Status: up
Operation Status: up
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List not configured
AAA Authentication Domain not configured
Default Group Policy: PG_1
Associated WebVPN Gateway: GW_ONE
Domain Name: DOMAIN_ONE
Maximum Users Allowed: 10000 (default)
NAT Address not configured
VRF Name not configured
```

#### show webvpn gateway Example

The following is sample output from the **show webvpn gateway** command:

```
Router# show webvpn gateway

Gateway Name                        Admin  Operation
------------                        -----  ---------
GW_1                                up     up
GW_2                                down   down
```

#### show webvpn gateway name Example

The following is sample output from the **show webvpn gateway** command, entered with a specific SSL VPN gateway name:

```
Router# show webvpn gateway GW_1

Admin Status: up
Operation Status: up
IP: 10.1.1.1, port: 443
SSL Trustpoint: TP-self-signed-26793562
```

#### show webvpn install file Example

The following is sample output from the **show webvpn install** command, entered with the **file** keyword:

```
Router# show webvpn install file \webvpn\stc\version.txt

SSL VPN File \webvpn\stc\version.txt installed:
CISCO STC win2k+ 1.0.0
1,1,0,116
Fri 06/03/2005 03:02:46.43
```

#### show webvpn install package svc Example

The following is sample output from the **show webvpn install** command, entered with the **package svc** keywords:

```
Router# show webvpn install package svc

SSL VPN Package SSL-VPN-Client installed:
File: \webvpn\stc\1\binaries\detectvm.class, size: 555
File: \webvpn\stc\1\binaries\java.htm, size: 309
File: \webvpn\stc\1\binaries\main.js, size: 8049
File: \webvpn\stc\1\binaries\ocx.htm, size: 244
File: \webvpn\stc\1\binaries\setup.cab, size: 176132
File: \webvpn\stc\1\binaries\stc.exe, size: 94696
File: \webvpn\stc\1\binaries\stcjava.cab, size: 7166
File: \webvpn\stc\1\binaries\stcjava.jar, size: 4846
File: \webvpn\stc\1\binaries\stcweb.cab, size: 13678
File: \webvpn\stc\1\binaries\update.txt, size: 11
File: \webvpn\stc\1\empty.html, size: 153
File: \webvpn\stc\1\images\alert.gif, size: 2042
File: \webvpn\stc\1\images\buttons.gif, size: 1842
File: \webvpn\stc\1\images\loading.gif, size: 313
File: \webvpn\stc\1\images\title.gif, size: 2739
File: \webvpn\stc\1\index.html, size: 4725
File: \webvpn\stc\2\index.html, size: 325
File: \webvpn\stc\version.txt, size: 63
Total files: 18
```

### show webvpn install status svc Example

The following is sample output from the **show webvpn install** command, entered with the **status svc** keywords:

```
Router# show webvpn install status svc

SSL VPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,0,2,127
Fri 07/22/2005 12:14:45.43
```

### show webvpn nbns context all Example

The following sample output from the **show webvpn nbns** command, entered with the **context all** keywords:

```
Router# show webvpn nbns context all

NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
```

### show webvpn policy Example

The following is sample output from the **show webvpn policy** command:

```
Router# show webvpn policy group ONE context all

WEBVPN: group policy = ONE ; context = SSL VPN
      idle timeout = 2100 sec
      session timeout = 43200 sec
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep SSL VPN client installed = disabled
```

```
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
WEBVPN: group policy = ONE ; context = SSL VPN_TWO
      idle timeout = 2100 sec
      session timeout = 43200 sec
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep SSL VPN client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
```

### show webvpn policy Example (with NTLM disabled)

The following is sample output from the **show webvpn policy** command. NTLM authentication has been disabled.

```
Router# show webvpn policy group ntlm context ntlm

WEBVPN: group policy = ntlm; context = ntlm
      url list name = "ntlm-server"
      idle timeout = 2100 sec
      session timeout = 43200 sec
      functions =
                httpauth-disabled
                file-access
                svc-enabled

      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep SSL VPN client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
```

### show webvpn session Example

The following is sample output from the **show webvpn session** command. The output is filtered to display user session information for only the specified context.

```
Router# show webvpn session context SSL VPN

WebVPN context name: SSL VPN
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              10.2.1.220                2         04:47:16  00:01:26
user2              10.2.1.221                2         04:48:36  00:01:56
```

### show webvpn session user Example

The following is sample output from the **show webvpn session** command. The output is filtered to display session information for a specific user.

```
Router# show webvpn session user user1 context all

WebVPN user name = user1 ; IP address = 10.2.1.220; context = SSL VPN
    No of connections: 0
    Created 00:00:19, Last-used 00:00:18
    CSD enabled
    CSD Session Policy
       CSD Web Browsing Allowed
       CSD Port Forwarding Allowed
       CSD Full Tunneling Disabled
```

```
       CSD FILE Access Allowed
    User Policy Parameters
      Group name = ONE
    Group Policy Parameters
      url list name = "Cisco"
      idle timeout = 2100 sec
      session timeout = 43200 sec
      port forward name = "EMAIL"
      tunnel mode = disabled
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep stc installed = disabled
      rekey interval = 3600 sec
      rekey method = ssl
      lease duration = 3600 sec
```

### show webvpn stats Example

The following is sample output from the **show webvpn stats** command entered with the **detail** and **context** keywords:

```
Router# show webvpn stats detail context SSL VPN

WebVPN context name : SSL VPN
User session statistics:
    Active user sessions     : 0          AAA pending reqs         : 0
    Peak user sessions       : 0          Peak time                : never
    Active user TCP conns    : 0          Terminated user sessions : 0
    Session alloc failures   : 0          Authentication failures  : 0
    VPN session timeout      : 0          VPN idle timeout         : 0
    User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
    CEF switched packets - client: 0         , server: 0
    CEF punted packets - client: 0         , server: 0

Mangling statistics:
    Relative urls            : 0          Absolute urls            : 0
    Non-http(s) absolute urls: 0          Non-standard path urls   : 0
    Interesting tags         : 0          Uninteresting tags       : 0
    Interesting attributes   : 0          Uninteresting attributes : 0
    Embedded script statement: 0          Embedded style statement : 0
    Inline scripts           : 0          Inline styles            : 0
    HTML comments            : 0          HTTP/1.0 requests        : 0
    HTTP/1.1 requests        : 0          Unknown HTTP version     : 0
    GET requests             : 0          POST requests            : 0
    CONNECT requests         : 0          Other request methods    : 0
    Through requests         : 0          Gateway requests         : 0
    Pipelined requests       : 0          Req with header size >1K : 0
    Processed req hdr bytes  : 0          Processed req body bytes : 0
    HTTP/1.0 responses       : 0          HTTP/1.1 responses       : 0
    HTML responses           : 0          CSS responses            : 0
    XML responses            : 0          JS responses             : 0
    Other content type resp  : 0          Chunked encoding resp    : 0
    Resp with encoded content: 0          Resp with content length : 0
    Close after response     : 0          Resp with header size >1K: 0
    Processed resp hdr size  : 0          Processed resp body bytes: 0
    Backend https response   : 0          Chunked encoding requests: 0

CIFS statistics:
  SMB related Per Context:
    TCP VC's                 : 0          UDP VC's                 : 0
    Active VC's              : 0          Active Contexts          : 0
    Aborted Conns            : 0
  NetBIOS related Per Context:
```

```
    Name Queries              : 0          Name Replies              : 0
    NB DGM Requests           : 0          NB DGM Replies            : 0
    NB TCP Connect Fails      : 0          NB Name Resolution Fails  : 0
  HTTP related Per Context:
    Requests                  : 0          Request Bytes RX          : 0
    Request Packets RX        : 0          Response Bytes TX         : 0
    Response Packets TX       : 0          Active Connections        : 0
    Active CIFS context       : 0          Requests Dropped          : 0

Socket statistics:
    Sockets in use            : 0          Sock Usr Blocks in use    : 0
    Sock Data Buffers in use  : 0          Sock Buf desc in use      : 0
    Select timers in use      : 0          Sock Select Timeouts      : 0
    Sock Tx Blocked           : 0          Sock Tx Unblocked         : 0
    Sock Rx Blocked           : 0          Sock Rx Unblocked         : 0
    Sock UDP Connects         : 0          Sock UDP Disconnects      : 0
    Sock Premature Close      : 0          Sock Pipe Errors          : 0
    Sock Select Timeout Errs  : 0

Port Forward statistics:
    Connections serviced      : 0          Server Aborts (idle)      : 0
  Client                                  Server
    in pkts                   : 0          out pkts                  : 0
    in bytes                  : 0          out bytes                 : 0
    out pkts                  : 0          in pkts                   : 0
    out bytes                 : 0          in bytes                  : 0

WEBVPN Citrix statistics:
Connections serviced : 0

                Server                    Client
  Packets in  : 0                          0
  Packets out : 0                          0
  Bytes in    : 0                          0
  Bytes out   : 0                          0

Tunnel Statistics:
    Active connections        : 0
    Peak connections          : 0          Peak time                 : never
    Connect succeed           : 0          Connect failed            : 0
    Reconnect succeed         : 0          Reconnect failed          : 0
    SVCIP install IOS succeed: 0           SVCIP install IOS failed  : 0
    SVCIP clear IOS succeed   : 0          SVCIP clear IOS failed    : 0
    SVCIP install TCP succeed: 0           SVCIP install TCP failed  : 0
    DPD timeout               : 0
  Client                                  Server
    in  CSTP frames           : 0          out IP pkts               : 0
    in  CSTP data             : 0          out stitched pkts         : 0
    in  CSTP control          : 0          out copied pkts           : 0
    in  CSTP Addr Reqs        : 0          out bad pkts              : 0
    in  CSTP DPD Reqs         : 0          out filtered pkts         : 0
    in  CSTP DPD Resps        : 0          out non fwded pkts        : 0
    in  CSTP Msg Reqs         : 0          out forwarded pkts        : 0
    in  CSTP bytes            : 0          out IP bytes              : 0
    out CSTP frames           : 0          in  IP pkts               : 0
    out CSTP data             : 0          in  invalid pkts          : 0
    out CSTP control          : 0          in  congested pkts        : 0
    out CSTP Addr Resps       : 0          in  bad pkts              : 0
    out CSTP DPD Reqs         : 0          in  nonfwded pkts         : 0
    out CSTP DPD Resps        : 0          in  forwarded pkts        : 0
    out CSTP Msg Reqs         : 0
    out CSTP bytes            : 0          in  IP bytes              : 0
```

### show webvpn stats sso Examples

The following output example displays statistics for an SSO server:

```
webvpn# show webvpn stats sso

Single Sign On statistics:
   Auth Requests           : 4         Pending Auth Requests    :0
   Successful Requests     : 1         Failed Requests          :3
   Retranmissions          : 0         DNS Errors               :0
   Connection Errors       : 0         Request Timeouts         :0
   Unknown Responses       :
```

The following output example displays extra information about SSO servers that are configured for the SSL VPN context:

```
Router# show webvpn context test_sso

  Context SSO server: sso-server
      Web agent URL :  "http://example1.examplecompany.com/vpnauth/"
      Policy Server Secret : "Secret123"
      Request Re-tries : 5, Request timeout: 15-second
```

The following output example displays extra information about a SSO server that is configured for the policy group of the SSL VPN context:

```
Router# show webvpn policy group sso context test_sso

WV: group policy = sso ; context = test_sso
      idle timeout = 2100 sec
      session timeout = 43200 sec
      sso server name = "server1"
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep SSL VPN client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
```

### F VRF show Command Output Example

The following output example shows that FVRF has been configured:

```
Router# show webvpn gateway mygateway

Admin Status: down
Operation Status: down
Error and Event Logging: Disabled
GW IP address not configured
SSL Trustpoint: TP-self-signed-788737041
FVRF Name: vrf_1
```

# Additional References

The following sections provide references related to SSL VPN.

## Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco AnyConnect VPN Client | • Cisco SSL VPN Client Home Page<br>http://www.cisco.com/en/US/partner/products/ps6496/tsd_products_support_series_home.html<br>• *Cisco AnyConnect VPN Client Administrator Guide, Version 2.0*<br>• *Release Notes for Cisco AnyConnect VPN Client, Version 2.0* |
| Cisco Secure Desktop | Cisco Secure Desktop Home Page<br>http://www.cisco.com/en/US/partner/products/ps6742/tsd_products_support_series_home.html |
| Configuring IP VRF (**ip vrf** command) | *Cisco IOS IP Application Services Command Reference* |
| IANA Application Port Numbers | *Port Numbers*<br>http://www.iana.org/assignments/port-numbers |
| RADIUS accounting | "Configuring RADIUS" chapter of the *Cisco IOS Security Configuration Guide*, Release 12.4 |
| Security configurations | *Cisco IOS Security Configuration Guide*, Release 12.4<br>http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_book09186a008043360a.html |
| Security commands | *Cisco IOS Security Command Reference*, Release 12.4T<br>http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_book09186a0080497056.html |
| SSL VPN licensing | *Cisco IOS SSL VPN Licensing Information* |
| SSL VPN platforms | *Cisco IOS SSL VPN* ("Feature Availability" section) |
| SSL VPN remote users guide | *SSL VPN Remote User Guide* |

## Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

# MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

# RFCs

| RFCs | Title |
|---|---|
| No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature. | — |

# Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/techsupport |

# Command Reference

This section documents new and modified commands only.

- nbns-list (policy group)
- nbns-server
- permit (webvpn acl)
- policy group
- port-forward
- port-forward (policy group)
- request-timeout
- secondary-color
- secondary-text-color
- secret-key
- show webvpn context
- show webvpn gateway
- show webvpn nbns
- show webvpn policy
- show webvpn session
- show webvpn stats
- ssl encryption
- ssl trustpoint
- sso-server
- svc address-pool
- svc default-domain
- svc dns-server
- svc dpd-interval
- svc homepage
- svc keep-client-installed
- svc msie-proxy
- svc rekey
- svc split
- svc split dns
- svc wins-server
- text-color
- timeout (policy group)
- time-range
- title
- title-color
- url-list
- url-text
- user-profile location

- vrf-name
- vrf-name
- web-agent-url
- webvpn context
- webvpn enable (Privileged EXEC)
- webvpn gateway
- webvpn install

# aaa accounting-list

To enable authentication, authorization, and accounting (AAA) accounting when you are using RADIUS for Secure Socket Layer Virtual Private Network (SSL VPN) sessions, use the **aaa accounting-list** command in global configuration mode. To disable the AAA accounting, use the **no** form of this command.

**aaa accounting-list** *aaa-list*

**no aaa accounting-list** *aaa-list*

## Syntax Description

| | |
|---|---|
| *aaa-list* | Name of the AAA accounting list that has been configured under global configuration. |

## Defaults

AAA accounting is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Before configuring this command, ensure that the AAA accounting list has already been configured under global configuration.

## Examples

The following example shows that AAA accounting has been configured for an SSL VPN session:

```
Router (config)# aaa accounting-list aaalist1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting network SSLVPN start-stop group radius** | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+. |

# aaa authentication (WebVPN)

To configure authentication, authorization, and accounting (AAA) authentication for SSL VPN sessions, use the **aaa authentication** command in webvpn context configuration mode. To remove the AAA configuration from the SSL VPN context configuration, use the **no** form of this command.

**aaa authentication** {**domain** *name* | **list** *name*}

**no aaa authentication** {**domain** | **list**}

## Syntax Description

| | |
|---|---|
| **domain** *name* | Configures authentication using the specified domain name. |
| **list** *name* | Configures authentication using the specified list name. |

## Command Default

If this command is not configured or if the **no** form of this command is entered, the SSL VPN gateway will use global AAA parameters (if configured).

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The **aaa authentication** command is entered to specify an authentication list or server group under a SSL VPN context configuration. If this command is not configured and AAA is configured globally on the router, global authentication will be applied to the context configuration.

The database that is configured for remote-user authentication on the SSL VPN gateway can be a local database, or the database can be accessed through any RADIUS or TACACS+ AAA server.

We recommend that you use a separate AAA server, such as a Cisco Access Control Server (ACS). A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions.

## Examples

### Local AAA Example (Default to Global Configuration)

The following example configures local AAA for remote-user connections. Notice that the **aaa authentication** command is not configured in a context configuration.

```
Router (config)# aaa new-model
Router (config)# username USER1 secret 0 PsW2143
Router (config)# aaa authentication login default local
```

### AAA Access Control Server Example

The following example configures a RADIUS server group and associates the AAA configuration under the SSL VPN context configuration.

```
Router (config)# aaa new-model
Router (config)# aaa group server radius myServer
Router (config-sg-radius)# server 10.1.1.20 auth-port 1645 acct-port 1646
Router (config-sg-radius)# exit
Router (config)# aaa authentication login default local group myServer
Router (config)# radius-server host 10.1.1.0 auth-port 1645 acct-port 1646
Router (config)# webvpn context context1
Router (config-webvpn-context)# aaa authentication list myServer
Router (config-webvpn-context)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# acl (WebVPN)

To define an access control list (ACL) using a Secure Socket Layer Virtual Private Network (SSL VPN) gateway at the Application Layer level and to associate an ACL with a policy group, use the **acl** command in webvpn context configuration and webvpn group policy configuration modes. To remove the ACL definition, use the **no** form of this command.

**acl** *acl-name*

**no acl** *acl-name*

## Syntax Description

| | |
|---|---|
| *acl-name* | Name of the ACL. |

## Command Default

If a user session has no ACL attributes configured, all application requests are permitted.

## Command Modes

Web context configuration
Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

The ACL can be defined for an individual user or for a policy group.

A defined ACL can be overridden by an individual user when the user logs on to the gateway (using AAA policy attributes).

## Examples

The following example shows that “acl1” has been defined as the ACL and that it has been associated with policy group “default.”

```
webvpn context context1
 acl acl1
  permit url "http://www.example.com"
 policy group default
  acl acl1
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Configures a policy group and enters group policy configuration mode. |
| **webvpn context** | Configures the SSL VPN context and enters webvpn context configuration mode. |

# add (WebVPN)

To add an ACL entry at a specified position, use the **add** command in webvpn acl configuration mode. To remove an entry from the position specified, use the **no** form of this command.

**add** *position acl-entry*

**no add** *position acl-entry*

## Syntax Description

| | |
|---|---|
| *position* | Position in the entry list to which the ACL rule is to be added. |
| *acl-entry* | Permit or deny command string. |

## Command Default

The ACL entry is appended to the end of the entry list.

## Command Modes

Webvpn acl configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Examples

The following example shows that the ACL rule should be added to the third position of the ACL list:

```
webvpn context context1
 acl acl1
  add 3 permit url any
```

## Related Commands

| Command | Description |
|---|---|
| **acl** | Defines an ACL using a SSL VPN gateway at the Application Layer level. |
| **wevpn context** | Configures the SSL VPN context and enters webvpn context configuration mode. |

# banner (WebVPN)

To configure a banner to be displayed after a successful login, use the **banner** command in webvpn group policy configuration mode. To remove the banner from the policy group configuration, use the **no** form of this command.

**banner** *string*

**no banner**

## Syntax Description

| | |
|---|---|
| *string* | Text string that contains 7-bit ASCII values and HTML tags and escape sequences. The text banner must be in quotation marks if it contains spaces. |

## Command Default

A banner is not displayed after a successful login.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Examples

The following example configures “Login Successful” to be displayed after login:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# banner “Login Successful”
Router(config-webvpn-group)#
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# cifs-url-list

To enter webvpn URL list configuration mode to configure a list of Common Internet File System (CIFS) server URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSL VPN) and to attach the URL list to a policy group, use the **cifs-url-list** command in webvpn context configuration and webvpn group policy configuration mode, respectively. To remove the CIFS server URL list from the SSL VPN context configuration and from the policy group, use the **no** form of this command.

**cifs-url-list** *name*

**no cifs-url-list** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the URL list. The list name can up to 64 characters in length. |

## Command Default

Webvpn URL list configuration mode is not entered, and a list of URLs to which a user has access on the portal page of an SSL VPN website is not configured. If the command is not used to attach a CIFS server URL list to a policy group, then a URL list is not attached to a group policy.

## Command Modes

Webvpn context configuration (config-webvpn-context)
Webvpn group policy configuration (config-webvpn-group)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |

## Usage Guidelines

Entering this command places the router in webvpn URL list configuration mode. In this mode, the list of CIFS server URLs is configured. A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual CIFS server URL list configurations must have unique names.

## Examples

The following example shows that CIFS URL lists have been added under the webvpn context and for a policy group:

```
webvpn context context1
 ssl authenticate verify all
 !
 acl "acl1"
   error-msg "warning!!!..."
   permit url "http://www.exampleurl1.com"
   deny url "http://www.exampleurl2.com"
   permit http any any
 !
 nbns-list l1
   nbns-server 10.1.1.20
 !
 cifs-url-list "c1"
```

```
  heading "cifs-url"
  url-text "SSLVPN-SERVER2" url-value "\\SSLVPN-SERVER2"
  url-text "SSL-SERVER2" url-value "\\SSL-SERVER2"
!
policy group default
  acl "acl1"
  cifs-url-list "c1"
  nbns-list "l1"
  functions file-access
  functions file-browse
  functions file-entry
default-group-policy default
gateway public
inservice
```

## Related Commands

| Command | Description |
|---|---|
| **heading** | Configures the heading that is displayed above URLs listed on the portal page of a SSL VPN website. |
| **policy group** | Attaches a URL list to policy group configuration. |
| **url-text** | Adds an entry to a URL list. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# citrix enabled

To enable Citrix application support for end users in a policy group, use the **citrix enabled** command in webvpn group policy configuration mode. To remove Citrix support from the policy group configuration, use the **no** form of this command.

**citrix enabled**

**no citrix enabled**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Citrix application support is not enabled.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Citrix support allows a citrix client to use applications running on a remote server as if they were running locally. Entering the **citrix-enabled** command configures Citrix support for the policy group.

## Examples

The following example configures Citrix support under the policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# citrix enabled
Router(config-webvpn-group)#
```

## Related Commands

| Command | Description |
|---|---|
| **filter citrix** | Configures a Citrix application access filter. |
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# clear webvpn nbns

To clear the NetBIOS name service (NBNS) cache on a SSL VPN gateway, use the **clear webvpn nbns** command in privileged EXEC mode.

**clear webvpn nbns** [**context** {*name* | **all**}]

## Syntax Description

| | |
|---|---|
| **context** | (Optional) Clears NBNS statistics for a specific context or all contexts. |
| *name* | Clears NBNS statistics for a specific context. |
| **all** | Clears NBNS statistics for all contexts. |

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Entering this command without any keywords or arguments clears all NBNS counters on the network device.

## Examples

The following example clears all NBNS counters:

```
Router# clear webvpn nbns
```

## Related Commands

| Command | Description |
|---|---|
| **clear webvpn session** | Clears remote users sessions on a SSL VPN gateway. |
| **clear webvpn stats** | Clears application and access counters on a SSL VPN gateway. |

# clear webvpn session

To clear SSL VPN remote user sessions, use the **clear webvpn session** command in privileged EXEC mode.

**clear webvpn session** [**user** *name*] **context** {*name* | **all**}

## Syntax Description

| | |
|---|---|
| **user** *name* | (Optional) Clears session information for a specific user. |
| **context** {*name* \| **all**} | Clears session information for a specific context or all contexts. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

This command is used to clear the session for either the specified remote user or all remote users in the specified context.

## Examples

The following example clears all session information:

```
Router# clear webvpn session context all
```

## Related Commands

| Command | Description |
|---|---|
| **clear webvpn nbns** | Clears the NBNS cache on a SSL VPN gateway. |
| **clear webvpn stats** | Clears application and access counters on a SSL VPN gateway. |

# clear webvpn stats

To clear (or reset) SSL VPN application and access counters, use the **clear webvpn stats** command in privileged EXEC mode.

**clear webvpn stats** [[**cifs** | **citrix** | **mangle** | **port-forward** | **sso** | **tunnel**] [**context** {*name* | **all**}]]

## Syntax Description

| | |
|---|---|
| **cifs** | (Optional) Clears Windows file share (CIFS) statistics. |
| **citrix** | (Optional) Clears Citrix application statistics. |
| **mangle** | (Optional) Clears URL mangling statistics. |
| **port-forward** | (Optional) Clears port forwarding statistics. |
| **sso** | (Optional) Clears statistics for Single SignOn (SSO) activities. |
| **tunnel** | (Optional) Clears Cisco AnyConnect VPN Client tunnel statistics. |
| **context** {*name* \| **all**} | (Optional) Clears information for either a specific context or all contexts. |

## Command Default

If no keywords are entered, all SSL VPN application and access counters are cleared.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(11)T | The **sso** keyword was added. |

## Usage Guidelines

This command is used to clear counters for Windows file shares, Citrix applications, URL mangling, application port forwarding, SSO, and Cisco AnyConnect VPN Client tunnels. The counters are cleared for either the specified context or all contexts on the SSL VPN gateway.

## Examples

The following example clears all statistics counters for all SSL VPN processes:

```
Router# clear webvpn stats
```

The following example clears statistics for SSO activities:

```
Router# clear webvpn stats sso
```

## Related Commands

| Command | Description |
|---|---|
| **clear webvpn nbns** | Clears the NBNS cache on a SSL VPN gateway. |
| **clear webvpn session** | Clears remote users sessions on a SSL VPN gateway. |

# csd enable

To enable Cisco Secure Desktop (CSD) support for SSL VPN sessions, use the **csd enable** command in webvpn context configuration mode. To remove CSD support from the SSL VPN context configuration, use the **no** form of this command.

**csd enable**

**no csd enable**

## Syntax Description

This command has no keywords or arguments.

## Command Default

CSD support is not enabled.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The CSD software installation package must be present in a local file system, such as flash memory, and it must be cached for distribution to end users (remote PC or networking device). The **webvpn install** command is used to install the software installation package to the distribution cache.

## Examples

The following example enables CSD support for SSL VPN sessions:

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg
SSLVPN Package Cisco-Secure-Desktop : installed successfully
Router(config)# webvpn context context1
Router(config-webvpn-context)# csd enable
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **webvpn install** | Installs a CSD or SSL VPN client package file to a SSL VPN gateway for distribution to end users. |

# debug webvpn

To enable the display of debug information for SSL VPN applications and network activity, use the **debug webvpn** command in privileged EXEC mode. To stop debugging messages from being processed and displayed, use the **no** form of this command.

**debug webvpn** [**verbose**] [**aaa** | **acl** | **cifs** | **citrix** [**verbose**] | **cookie** [**verbose**] | **count** | **csd** | **data** | **dns** | **emweb** [**state**] | **entry** *context-name* [**source** *ip* [*network-mask*] | **user** *username*] | **http** [**authentication** | **trace** | **verbose**] | **package** | **sdps** [**level** *number*] | **sock** [**flow**] | **sso** | **timer** | **trie** | **tunnel** [**traffic** *acl-number* | **verbose**] | **url-disp** | **webservice** [**verbose**]]

**no debug webvpn** [**verbose**] [**aaa** | **acl** | **cifs** | **citrix** [**verbose**] | **cookie** [**verbose**] | **count** | **csd** | **data** | **dns** | **emweb** [**state**] | **entry** *context-name* [**source** *ip* [*network-mask*] | **user** *username*] | **http** [**authentication** | **trace** | **verbose**] | **package** | **sdps** [**level** *number*] | **sock** [**flow**] | **sso** | **timer** | **trie** | **tunnel** [**traffic** *acl-number* | **verbose**] | **url-disp** | **webservice** [**verbose**]]

## Syntax Description

| | |
|---|---|
| **verbose** | (Optional) Detailed information about SSL VPN applications and network activity is displayed in addition to the nondetailed information. |
| **aaa** | (Optional) Displays authentication, authorization, and accounting (AAA) event and error messages. |
| **acl** | (Optional) Displays information about the Application Layer access control list (ACL). |
| **cifs** | (Optional) Displays Microsoft Windows file share access event and error messages. |
| **citrix** [**verbose**] | (Optional) Displays Citrix application event and error messages.<br>• **verbose** (Optional)—All detailed and nondetailed citrix messages are displayed. If the **verbose** keyword is not used, only the nondetailed messages are displayed. |
| **cookie** [**verbose**] | (Optional) Displays event and error messages that relate to the cookie that is pushed to the browser of the end user.<br>• **verbose** (Optional)—All detailed and nondetailed cookie messages are displayed. If the **verbose** keyword is not used, only the nondetailed messages are displayed. |
| **count** | (Optional) Displays reference count information for a context. |
| **csd** | (Optional) Displays Cisco Secure Desktop (CSD) event and error messages. |
| **data** | (Optional) Displays data debug messages. |
| **dns** | (Optional) Displays domain name system (DNS) event and error messages. |
| **emweb** [**state**] | (Optional) Displays emweb state debug messages. |

| | |
|---|---|
| **entry** *context-name* [**source** *ip* [*network-mask*] \| **user** *username*] | (Optional) Displays information for a specific user or group.<br>• *context-name*—SSL VPN context name.<br>• **source** *ip* (Optional)—IP address of the user or group. The *network-mask* argument is optional. If not specified, 255.255.255.255 is used.<br>• **user** *username* (Optional)— Username of the user.<br>**Note** The **entry** keyword can be used with other **debug** commands to single out the debug messages for a particular user or group. If the **debug webvpn** entry is not defined, the debug messages of the feature or function that are turned on are printed for every user. |
| **http** [**authentication** \| **trace** \| **verbose**] | (Optional) Displays HTTP debug messages.<br>• **authentication** (Optional)—Displays information for HTTP authentication, such as NT LAN Manager (NTLM).<br>• **trace** (Optional)—Displays HTTP information that involves EmWeb processing.<br>• **verbose** (Optional)—All detailed and nondetailed HTTP messages are displayed. If the **verbose** keyword is not used, only the nondetailed messages are displayed. |
| **package** | (Optional) Deploys event and error messages for the software packages that are pushed to the end user. |
| **sdps** [**level** *number*] | (Optional) Displays SDPS debug messages. The level is entered as a number from 1 to 5. |
| **sock** [**flow**] | (Optional) Displays socket debug messages. |
| **sso** | (Optional) Displays information about Single SignOn (SSO) ticket creation, session setup, and response handling. |
| **timer** | (Optional) Displays timer debug messages. |
| **trie** | (Optional) Displays trie debug messages. |
| **tunnel** [**traffic** *acl-number* \| **verbose**] | (Optional) Displays tunnel debug messages.<br>• **traffic** *acl-number* (Optional)—Access control list number of the traffic to be displayed.<br>• **verbose** (Optional)—All detailed and nondetailed tunnel messages are displayed. If the **verbose** keyword is not used, only the nondetailed messages are displayed. |
| **url-disp** | (Optional) Displays URL debug messages. |
| **webservice** [**verbose**] | (Optional) Displays web service event and error messages.<br>• **verbose** (Optional)—All detailed and nondetailed web service messages are displayed. If the **verbose** keyword is not used, only the nondetailed messages are displayed. |

**Command Default** None.

**Command Modes** Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(6)T | Support for the SSL VPN enhancements feature was added. |
| 12.4(11)T | The following keywords were deleted effective with Cisco IOS Release 12.4(11)T:<br>• **port-forward**<br>• **detail** keyword option for the **tunnel** keyword<br>The following keywords and arguments were added effective with Cisco IOS Release 12.4(11)T:<br>• **verbose**<br>• **acl**<br>• **entry** *context-name* [**source** *ip* [*network-mask*] \| **user** *username*]<br>• **authentication**, **trace**, and **verbose** keyword options for the **http** keyword<br>• **sso**<br>• **verbose** keyword option for the **citrix**, **cookie**, **tunnel**, and **webservice** keywords |

## Usage Guidelines

This command should be used with caution on a production router or networking device. It is recommended that debugging is enabled only for individual components as necessary. This restriction is intended to prevent the console session from be overwhelmed by large numbers of messages.

The **no** form of this command turns off feature debugging. It does not matter if the **verbose** keyword has been used or not.

If the **no** form of this command is used with the **verbose** keyword option for any keyword, all keyword and argument fields must be an exact match.

## Examples

### debug webvpn Command Output for Various SSL VPN Sessions

The following example displays **debug webvpn** output for various SSL VPN sessions:

```
Router# debug webvpn

*Dec 23 07:47:41.368: WV: Entering APPL with Context: 0x64C5F270,
      Data buffer(buffer: 0x64C877D0, data: 0x4F27B638, len: 272,
      offset: 0, domain: 0)
*Dec 23 07:47:41.368: WV: http request: /sslvpn with domain cookie
*Dec 23 07:47:41.368: WV: Client side Chunk data written..
 buffer=0x64C877B0 total_len=189 bytes=189 tcb=0x6442FCE0
*Dec 23 07:47:41.368: WV: sslvpn process rcvd context queue event
*Dec 23 07:47:41.372: WV: sslvpn process rcvd context queue event
*Dec 23 07:47:41.372: WV: Entering APPL with Context: 0x64C5F270,
      Data buffer(buffer: 0x64C877D0, data: 0x4F26D018, len: 277,
      offset: 0, domain: 0)
*Dec 23 07:47:41.372: WV: http request: /webvpn.html with domain cookie
*Dec 23 07:47:41.372: WV: [Q]Client side Chunk data written..
 buffer=0x64C877B0 total_len=2033 bytes=2033 tcb=0x6442FCE0
*Dec 23 07:47:41.372: WV: Client side Chunk data written..
 buffer=0x64C87710 total_len=1117 bytes=1117 tcb=0x6442FCE0
```

### debug webvpn Command Output for a Specific User

The following example displays information for a specific user (user1 under the context "mycontext") and for a feature or function:

```
Router# debug webvpn entry mycontext_user_user1

! The above line turns debugging on for user1.
! The following line turns on debugging for a feature (or features) or function (or
functions)—in this case; for authentication, authorization, and accounting (AAA).
Router# debug webvpn aaa
```

The actual output is as follows:

```
*Dec 23 07:56:41.351: WV-AAA: AAA authentication request sent for user: "user1"
*Dec 23 07:56:41.351: WV-AAA: AAA Authentication Passed!
*Dec 23 07:56:41.351: WV-AAA: User "user1" has logged in from "10.107.163.147" to gateway
"sslvpn" context "mycontext"
*Dec 23 07:59:01.535: WV-AAA: User "user1" has logged out from gateway "sslvpn" context
"mycontext"
```

### debug webvpn Command Cookie and HTTP Output for a Group of Users

The following example displays cookie and HTTP information for a group of users under the context "mycontext" having a source IP range from 192.168.1.1. to 192.168.1.255:

```
Router# debug webvpn entry mycontext source 192.168.1.0 255.255.255.0

! The above command line sets up debugging for the group.
!The following command lines turn on debugging for cookie and HTTP information.
Router# debug webvpn cookie
Router# debug webvpn http
```

The actual output is as follows:

```
*Dec 23 08:10:11.191: WV-HTTP: Original client request
GET /webvpn.html HTTP/1.1

*Dec 23 08:10:11.191: WV-HTTP: HTTP Header parsing complete
*Dec 23 08:10:11.191: WV-HTTP: * HTTP request complete
*Dec 23 08:10:11.191: WV-COOKIE: Enter VW context cookie check with Context:0x64C5F470,
          buffer: 0x64C87710, buffer->data: 0x4F26D018, buffer->len: 277,
          cookie: 0x4F26D10A, length: 33
*Dec 23 08:10:11.191: WV-COOKIE: webvpn context cookie received is
webvpncontext=00@mycontext
*Dec 23 08:10:11.191: WV-COOKIE: context portion in context cookie is: mycontext
*Dec 23 08:10:11.327: WV-HTTP: Original client request
GET /paramdef.js HTTP/1.1

*Dec 23 08:10:11.327: WV-HTTP: HTTP Header parsing complete
*Dec 23 08:10:11.327: WV-HTTP: * HTTP request complete
```

### debug webvpn Command SSO Output

The following output example displays information about SSO ticket creation, session setup, and response handling:

```
Router# debug webvpn sso

*Jun 12 20:37:01.052: WV-SSO: Redirect to SSO web agent URL -
http://example.examplecompany.com/vpnauth/
*Jun 12 20:37:01.052: WV_SSO: Set session cookie with SSO redirect
*Jun 12 20:37:01.056: WV-SSO: Set SSO auth flag
*Jun 12 20:37:01.056: WV-SSO: Attach credentials - building auth ticket
```

```
*Jun 12 20:37:01.060: WV-SSO: user: [user11], secret: [example123], version: [1.0], login
time: [BCEFC86D], session key: [C077F97A], SHA1 hash :
[B07D0A924DB33988D423AE9F937C1C5A66404819]
*Jun 12 20:37:01.060: WV-SSO: auth_ticket :
user11:1.0@C077F97A@BCEFC86D@B07D0A924DB33988D423AE9F937C1C5A66404819
*Jun 12 20:37:01.060: WV-SSO: Base64 credentials for the auth_ticket:
dXNlcjExOjEuMEBDMDc3Rjk3QUBCQ0VGQzg2REBCMDdEMEE5MjREQjMzOTg4RDQyM0FFOUY5MzdDMUM1QTY2NDA0OD
E5
*Jun 12 20:37:01.060: WV-SSO: Decoded credentials =
user11:1.0@C077F97A@BCEFC86D@B07D0A924DB33988D423AE9F937C1C5A66404819
*Jun 12 20:37:01.060: WV-SSO: Starting SSO request timer for 15-second

*Jun 12 20:37:01.572: WV-SSO: SSO auth response rcvd - status[200]
*Jun 12 20:37:01.572: WV-SSO: Parsed non-SM cookie: SMCHALLENGE
*Jun 12 20:37:01.576: WV-SSO: Parsed SMSESSION cookie
*Jun 12 20:37:01.576: WV-SSO: Sending logon page after SSO auth success
```

# default-group-policy

To associate a policy group with a SSL VPN context configuration, use the **default-group-policy** command in webvpn context configuration mode. To remove the policy group from the webvpn context configuration, use the **no** form of this command.

**default-group-policy** *name*

**no default-group-policy**

## Syntax Description

| | |
|---|---|
| *name* | Name of the policy configured with the **policy group** command. |

## Command Default

A policy group is not associated with a SSL VPN context configuration.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The **policy group** command is first configured to define policy group configuration parameters. This command is configured to attach the policy group to the SSL VPN context when multiple policy groups are defined under the context. This policy will be used as the default unless an authentication, authorization, and accounting (AAA) server pushes an attribute that specifically requests another group policy.

## Examples

The following example configures policy group ONE as the default policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy-group ONE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# policy-group TWO
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy ONE
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# deny (WebVPN)

To set conditions in a named Secure Sockets Layer Virtual Private Network (SSL VPN) access list that will deny packets, use the **deny** command in webvpn acl configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

**deny** [**url** [**any** | *url-string*]] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | *source-ip source-mask*] [**any** | *destination-ip destination-mask*] **time-range** {*time-range-name*} [**syslog**]

**no deny url** [**any** | *url-string*] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | *source-ip source-mask*] [**any** | *destination-ip destination-mask*] **time-range** {*time-range-name*} [**syslog**]

## Syntax Description

| | |
|---|---|
| **url** | (Optional) Filtering rules are applied to the URL.<br>• Use the **any** keyword as an abbreviation for any URL. |
| *url-string* | (Optional) URL string defined as follows: **scheme://host[:port][/path]**<br>• **scheme**—Can be HTTP, Secure HTTPS (HTTPS), or Common Internet File System (CIFS). This field is required in the URL string.<br>• **host**—Can be a hostname or a host IP (host mask). The host can have one wildcard (*).<br>• **port**—Can be any valid port number (1–65535). It is possible to have multiple port numbers separated by a comma (,). The port range is expressed using a dash (-).<br>• **path**—Can be any valid path string. In the path string, the $user is translated to the current user name. |
| **ip** | (Optional) Denies only IP packets. When you enter the **ip** keyword, you must use the specific command syntax shown for the IP form of the deny command. |
| **tcp** | (Optional) Denies only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the deny command. |
| **udp** | (Optional) Denies only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the deny command. |
| **http** | (Optional) Denies only HTTP packets. When you enter the **http** keyword, you must use the specific command syntax shown for the HTTP form of the deny command. |
| **https** | (Optional) Denies only HTTPS packets. When you enter the **https** keyword, you must use the specific command syntax shown for the HTTPS form of the deny command. |
| **cifs** | (Optional) Denies only CIFS packets. When you enter the **cifs** keyword, you must use the specific command syntax shown for the CIFS form of the deny command. |
| *source-ip source-mask* | (Optional) Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:<br>• Use a 32-bit quantity in four-part dotted-decimal format.<br>• Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255.<br>• Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0. |

| | |
|---|---|
| *destination-ip destination-mask* | (Optional) Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:<br>• Use a 32-bit quantity in four-part dotted-decimal format.<br>• Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255.<br>• Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0. |
| **time-range** *time-range-name* | Name of the time range that applies to this **deny** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively. |
| **syslog** | (Optional) System logging messages are generated. |

## Command Default

There are no specific conditions under which a packet is denied passing the named access list.

## Command Modes

Webvpn acl configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Use this command following the **acl** command to specify conditions under which a packet cannot pass the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this deny statement is in effect.

## Examples

The following example shows that all packets from the URL "https://10.168.2.228:34,80-90,100-/public" will be denied:

```
webvpn context context1
 acl acl1
  deny url "https://10.168.2.228:34,80-90,100-/public"
```

## Related Commands

| Command | Description |
|---|---|
| **absolute** | Specifies an absolute time for a time range. |
| **periodic** | Specifies a recurring (weekly) time range for functions that support the time-range feature. |
| **permit (webvpn acl)** | To set conditions to allow a packet to pass a named SSL VPN access list. |
| **time-range** | Enables time-range configuration mode and defines time ranges for functions (such as extended access lists). |

# error-msg

To display a specific error message when a user logs on to a Secure Sockets Layer Virtual Private Network (SSL VPN) gateway, use the **error-msg** command in webvpn acl configuration mode. To remove the error message, use the **no** form of this command.

**error-msg** *message-string*

**no error-msg** *message-string*

## Syntax Description

| | |
|---|---|
| *message-string* | Error message to be displayed. |

## Command Default

No special error message is displayed.

## Command Modes

Webvpn acl configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

If the **error-url** command is configured, the user is redirected to the error URL for every request that is not allowed. If the **error-url** command is not configured, the user gets a standard, gateway-generated information page showing the message that was configured using the **error-msg** command.

## Examples

This example shows that the following error message will be displayed when the user logs on to the SSL VPN gateway:

```
webvpn context context1
 acl acl1
  error-msg "If you have any questions, please contact <a
  href+mailto:employee1@example.com>Employee1</a>."
```

## Related Commands

| Command | Description |
|---|---|
| **acl** | Defines an ACL using a SSL VPN gateway at the Application Layer level and enters webvpn acl configuration mode. |
| **error-url** | Defines a URL as an ACL violation page using a SSL VPN gateway. |
| **webvpn context** | Configures a SSL VPN context and enters webvpn context configuration mode. |

# error-url

To define a URL as an access control list (ACL) violation page using a Secure Socket Layer Virtual Private Network (SSL VPN) gateway, use the **error-url** command in webvpn acl configuration mode. To remove the ACL violation page, use the **no** form of this command.

**error-url** *access-deny-page-url*

**no error-url** *access-deny-page-url*

## Syntax Description

| | |
|---|---|
| *access-deny-page-url* | URL to which a user is directed for an ACL violation. |

## Command Default

If this command is not configured, the gateway redirects the ACL violation page to a predefined URL.

## Command Modes

Webvpn acl configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

If the **error-url** command is configured, the user is redirected to a predefined URL for every request that is not allowed. If the **error-url** command is not configured, the user gets a standard, gateway-generated error page.

## Examples

The following example shows that the URL “http://www.example.com” has been defined as the ACL violation page:

```
webvpn context context1
 acl acl1
  error-url “http://www.example.com”
```

## Related Commands

| Command | Description |
|---|---|
| **acl** | Defines an ACL using a SSL VPN gateway at the Application Layer level. |
| **error-msg** | Displays a specific error message when a user logs on to a SSL VPN gateway. |
| **webvpn context** | Configures the SSL VPN context and enters webvpn context configuration mode. |

# filter citrix

To configure a Citrix application access filter, use the **filter citrix** command in webvpn group policy configuration mode. To remove the access filter from the policy group configuration, use the **no** form of this command.

**filter citrix** *extended-acl*

**no filter citrix** *extended-acl*

## Syntax Description

| | |
|---|---|
| *extended-acl* | Defines the filter on the basis of an extended access list (ACL). A named, numbered, or expanded access list is entered. |

## Command Default

A Citrix application access filter is not configured.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Citrix application support is enabled under the policy group by configuring the **citrix enabled** command. User access to Citrix applications is configured with the **filter citrix** command. An extended access list is configured to define the filter.

## Examples

The following example configures Citrix support for end users that have a source address in the 192.168.1.0/24 network:

```
Router(config)# access-list 100 permit ip 192.168.1.0 0.255.255.255 any
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# citrix enabled
Router(config-webvpn-group)# filter citrix 100
Router(config-webvpn-group)#
```

## Related Commands

| Command | Description |
|---|---|
| **citrix enabled** | Enables Citrix support under a policy group. |
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# filter tunnel

To configure a SSL VPN tunnel access filter, use the **filter tunnel** command in webvpn group policy configuration mode. To remove the tunnel access filter, use the **no** form of this command.

**filter tunnel** *extended-acl*

**no filter tunnel** *extended-acl*

## Syntax Description

| | |
|---|---|
| *extended-acl* | Defines the filter on the basis of an extended access list (ACL). A named, numbered, or expanded access list is entered. |

## Command Default

A SSL VPN tunnel access filter is not configured.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The tunnel access filter is used to control network- and application-level access.

## Examples

The following example configures a deny access filter for any host from the 172.16.2/24 network:

```
Router(config)# access-list 101 deny ip 172.16.2.0 0.0.0.255 any
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# filter tunnel 101
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# functions

To enable a file access function or tunnel mode support in a group policy configuration, use the **functions** command in webvpn group policy configuration mode. To remove file access or tunnel support from the group policy configuration, use the **no** form of this command.

**functions** {**file-access** | **file-browse** | **file-entry** | **svc-enabled** | **svc-required**}

**no functions** {**file-access** | **file-browse** | **file-entry** | **svc-enabled** | **svc-required**}

## Syntax Description

| | |
|---|---|
| **file-access** | Enables network file-share access. File servers in the server list are listed on the SSL VPN home page if this keyword is enabled. |
| **file-browse** | Enables browse permissions for server and file shares. The file-access function must be enabled to also use this function. |
| **file-entry** | Enables "modify" permissions for files in the shares listed on the SSL VPN home page. |
| **svc-enabled** | Enables tunnel support for the user. Allows the user of the group to use tunnel mode. If the Cisco AnyConnect VPN Client software package fails to install on the PC of the end user, the end user can continue to use clientless mode or thin-client mode. |
| **svc-required** | Enables only tunnel support for the user. If the Cisco AnyConnect VPN Client software package fails to install on the PC of the end user, the other access modes cannot be used. |

## Command Default

File access function or tunnel mode support is not enabled.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The end user must have administrative privileges, and the Java Runtime Environment (JRE) for Windows version 1.4 or later must be installed before Cisco Secure Desktop (CSD) or Cisco AnyConnect VPN Client packages can be installed.

## Examples

The following example enables file share access with server-browse and file-modify permission:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# functions file-access
Router(config-webvpn-group)# functions file-browse
Router(config-webvpn-group)# functions file-entry
```

**Related Commands**

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a group policy. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# gateway (WebVPN)

To associate a SSL VPN gateway with a SSL VPN context, use the **gateway** command in webvpn context configuration mode. To remove the gateway from the SSL VPN context configuration, use the **no** form of this command.

**gateway** *name* [**domain** *name* | **virtual-host** *name*]

**no gateway** *name*

## Syntax Description

| | |
|---|---|
| **domain** *name* | (Optional) Maps SSL VPN sessions to the specified domain name (for example, “https://gw-address/domain”). |
| **virtual-host** *name* | (Optional) Maps SSL VPN sessions to the specified virtual host. |

## Command Default

A SSL VPN gateway is not associated with a SSL VPN context.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

This command is used to attach a SSL VPN gateway to a SSL VPN context configuration.

A virtual host name is specified when multiple virtual hosts are mapped to the same IP address on the SSL VPN gateway (similar to a canonical domain name). The virtual host name differentiates the host request on the gateway. The host header in the HTTP message is modified to direct traffic to the virtual host.

## Examples

The following example configures the gateway and then attaches the SSL VPN context:

```
Router(config)# webvpn gateway GW_1
Router(config-webvpn-gateway)# ip address 10.1.1.1
Router(config-webvpn-gateway)# inservice
Router(config-webvpn-gateway)# exit
Router(config)# webvpn context context1
Router(config-webvpn-context)# gateway GW_1 domain cisco.com
Router(config-webvpn-context)# inservice
```

**Related Commands**

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |
| **webvpn gateway** | Enters webvpn gateway configuration mode to configure a SSL VPN gateway. |

# heading

To configure the heading that is displayed above URLs listed on the portal page of a SSL VPN, use the **heading** command in webvpn URL list configuration mode. To remove the heading, use the **no** form of this command.

**heading** *text-string*

**no heading**

## Syntax Description

| | |
|---|---|
| *text-string* | The URL list heading entered as a text string. The heading must be in quotation marks if it contains spaces. |

## Command Default

A heading is not configured.

## Command Modes

Webvpn URL list configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)#
```

## Related Commands

| Command | Description |
|---|---|
| **url-list** | Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN. |

# hide-url-bar

To prevent the URL bar from being displayed on the SSL VPN portal page, use the **hide-url-bar** command in webvpn group policy configuration mode. To display the URL bar on the portal page, use the **no** form of this command.

**hide-url-bar**

**no hide-url-bar**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The URL bar is displayed on the SSL VPN portal page.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The configuration of this command applies only to clientless mode access.

## Examples

The following example hides the URL bar on the SSL VPN portal page:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# hide-url-bar
Router(config-webvpn-group)#
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# hostname (WebVPN)

To configure the hostname for a SSL VPN gateway, use the **hostname** command in webvpn gateway configuration mode. To remove the hostname from the SSL VPN gateway configuration, use the **no** form of this command.

**hostname** *name*

**no hostname**

## Syntax Description

| | |
|---|---|
| *name* | Specifies the hostname. |

## Command Default

The hostname is not configured.

## Command Modes

Webvpn gateway configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

A hostname is configured for use in the URL and cookie-mangling process. In configurations where traffic is balanced among multiple SSL VPN gateways, the hostname configured with this command maps to the gateway IP address configured on the load-balancing device(s).

## Examples

The following example configures a hostname for a SSL VPN gateway:

```
Router(config)# webvpn gateway GW_1
Router(config-webvpn-gateway)# hostname VPN_Server
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn gateway** | Defines a SSL VPN gateway and enters webvpn gateway configuration mode. |

# http-redirect

To configure HTTP traffic to be carried over secure HTTP (HTTPS), use the **http-redirect** command in webvpn gateway configuration mode. To remove the HTTPS configuration from the SSL VPN gateway, use the **no** form of this command.

**http-redirect** [**port** *number*]

**no http-redirect**

## Syntax Description

| | |
|---|---|
| **port** *number* | (Optional) Specifies a port number. The value for this argument is a number from 1 to 65535. |

## Command Default

The following default value is used if this command is configured without entering the **port** keyword:

**port** *number* : 80

## Command Modes

Webvpn gateway configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

When this command is enabled, the HTTP port is opened and the SSL VPN gateway listens for HTTP connections. HTTP connections are redirected to use HTTPS. Entering the **port** keyword and *number* argument configures the gateway to listen for HTTP traffic on the specified port. Entering the **no** form, disables HTTP traffic redirection. HTTP traffic is handled by the HTTP server if one is running.

## Examples

The following example, starting in global configuration mode, redirects HTTP traffic (on TCP port 80) over to HTTPS (on TCP port 443):

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# http-redirect
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn gateway** | Defines a SSL VPN gateway and enters webvpn gateway configuration mode. |

# inservice (WebVPN)

To enable a SSL VPN gateway or context process, use the **inservice** command in webvpn gateway configuration or webvpn context configuration mode. To disable a SSL VPN gateway or context process without removing the configuration from the router configuration file, use the **no** form of this command.

**inservice**

**no inservice**

## Syntax Description

This command has no arguments or keywords.

## Command Default

A SSL VPN gateway or context process is not enabled.

## Command Modes

Webvpn gateway configuration
Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The enable form of this command initializes required system data structures, initializes TCP sockets, and performs other start-up tasks related to the SSL VPN gateway or context process. The gateway and context processes must both be “inservice” to enable SSL VPN.

## Examples

The following example enables the SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# inservice
```

The following example configures and activates the SSL VPN context configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# inservice
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn configuration mode to configure the SSL VPN context. |
| **webvpn gateway** | Defines a SSL VPN gateway and enters webvpn gateway configuration mode. |

# ip address (WebVPN)

To configure a proxy IP address on a SSL VPN gateway, use the **ip address** command in webvpn gateway configuration mode. To remove the proxy IP address from the SSL VPN gateway, use the **no** form of this command.

**ip address** *number* [**port** *number*] [**secondary**]

**no ip address**

## Syntax Description

| | |
|---|---|
| *number* | IPv4 address. |
| **port** *number* | (Optional) Specifies the port number for proxy traffic. A number from 1 to 65535 can be entered for this argument. |
| **secondary** | (Optional) Configures the gateway using a secondary IP address. |

## Command Default

The following default value is used if this command is configured without entering the **port** keyword:

**port** *number* : 443

## Command Modes

Webvpn gateway configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The **ip address** command is used to configure a proxy IP address for a SSL VPN gateway. The IP address is the termination point for all SSL VPN client connections. This IP address can be any routable IP address assigned to a valid interface.

A secondary IP address is configured if an external device performs load-balancing functions.

A secondary address must be configured if the proxy IP address is not on a directly connected network.

**Note** A secondary IP address will not respond to Area Response Protocol (ARP) or Internet Control Message Protocol (ICMP) requests.

## Examples

The following example configures 192.168.1.1 as a proxy address on a SSL VPN gateway. Proxy traffic is directed over port 443.

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ip address 192.168.1.1 port 443
```

**Related Commands**

| Command | Description |
|---|---|
| **webvpn gateway** | Defines a SSL VPN gateway and enters webvpn gateway configuration mode. |

# list (WebVPN)

To list the currently configured access control list (ACL) entries sequentially, use the **list** command in webvpn acl configuration mode. This command has no **no** form.

**list**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Currently configured ACL entries are not listed.

## Command Modes

Webvpn acl configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Before using this command, you must have configured the web context and the **acl** command.

## Examples

The following example shows that currently configured ACL entries are to be listed:

```
webvpn context context1
 acl acl1
  list
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Configures the WebVPN context and enters SSL VPN configuration mode. |
| **acl** | Defines an ACL using a SSL VPN gateway at the Application Layer level. |

# local-port (WebVPN)

To remap (forward) an application port number in a port forwarding list, use the **local-port** command in webvpn port-forward list configuration mode. To remove the application port mapping from the forwarding list, use the **no** form of this command.

**local-port** {*number* **remote-server** *name* **remote-port** *number* **description** *text-string*}

**no local-port** {*number*}

## Syntax Description

| | |
|---|---|
| *number* | Configures the port number to which the local application is mapped. A number from 1 through 65535 is entered. |
| **remote-server** *name* | Identifies the remote server. An IPv4 address or fully qualified domain name is entered. |
| **remote-port** *number* | Specifies the well-known port number of the application, for which port-forwarding is to be configured. A number from 1 through 65535 is entered. |
| **description** *text-string* | Configures a description for this entry in the port-forwarding list. The text string is displayed on the end-user applet window. A text string up to 64 characters in length is entered. |

## Command Default

An application port number is not remapped.

## Command Modes

Webvpn port-forward list configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The **local-port** command is configured to add an entry to the port-forwarding list. The forward list is created with the **port-forward** command in webvpn context configuration mode. The remote port number is the well-known port to which the application listens. The local port number is the entry configured in the port forwarding list. A local port number can be configured only once in a given port-forwarding list.

## Examples

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com
remote-port 143 description IMAP
```

**Related Commands**

| Command | Description |
|---|---|
| **port-forward** | Enters webvpn port-forward list configuration mode to configure a port-forwarding list. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# login-message

To configure a login message for the text box on the user login page, use the **login-message** command in webvpn context configuration mode. To reconfigure the SSL VPN context configuration to display the default message, use the **no** form of this command.

**login-message** [*message-string*]

**no login-message** [*message-string*]

## Syntax Description

| | |
|---|---|
| *message-string* | (Optional) Login message string up to 255 characters in length. The string value may contain 7-bit ASCII values, HTML tags, and escape sequences. |

## Defaults

The following message is displayed if this command is not configured or if the **no** form is entered:

"Please enter your username and password"

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

The optional form of this command is used to change or enter a login message. A text string up to 255 characters in length can be entered. The **no** form of this command is entered to configure the default message to be displayed. When the **login-message** command is entered without the optional text string, no login message is displayed.

## Examples

The following example changes the default login message to "Please enter your login credentials":

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# login-message "Please enter your login credentials"
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# login-photo

To set the photo parameters on a Secure Socket Layer Virtual Private Network (SSL VPN) login page, use the **login-photo** command in web vpn context configuration mode. To display the login page with no photo but with a message that spans the message and the photo columns, use the **no** form of this command.

**login-photo** [**file** *file-name* | **none**]

**no login-photo**

## Syntax Description

| | |
|---|---|
| **file** *file-name* | Points to a file to be displayed on the login page. The *file-name* argument can be **jpeg**, **bitmap**, or **gif**. However, gif files are recommended. |
| **none** | No photo appears on the login page. |

## Command Default

No photo appears, and the message spans the two columns (message and photo columns).

## Command Modes

Webvpn context configuration (config-webvpn-context)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |

## Usage Guidelines

To display no photo, use the **login-photo none** option. To display no photo and have the message span both columns (message column and photo column), use the **no login-photo** option.

The best resolution for login photos is 179 x 152 pixels.

## Examples

The following example shows that no photo is displayed:

```
Router (config)# webvpn context
Router (config-webvpn-context)# login-photo none
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# logo

To configure a custom logo to be displayed on the login and portal pages of an SSL VPN, use the **logo** command in SSLVPN configuration mode. To configure the Cisco logo to be displayed, use the **no** form of this command.

**logo** [**file** *filename* | **none**]

**no logo** [**file** *filename* | **none**]

## Syntax Description

| | |
|---|---|
| **file** *filename* | (Optional) Specifies the location of an image file. A gif, jpg, or png file can be specified. The file can be up to 100 KB in size. The name of the file can be up 255 characters in length. |
| **none** | (Optional) No logo is displayed. |

## Defaults

The Cisco logo is displayed if the **no** form of this command is not configured or if the **no** form is entered.

## Command Modes

SSLVPN configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

The source image file for the logo is a gif, jpg, or png file that is up to 255 characters in length (filename) and up to 100 kilobytes (KB) in size. The file is referenced from a local file system, such as flash memory. An error message will be displayed if the file is not referenced from a local file system. No logo will be displayed if the image file is removed from the local file system.

## Examples

The following example references mylogo.gif (from flash memory) to use as the SSL VPN logo:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# logo file flash:/mylogo.gif
Router(config-webvpn-context)#
```

In the following example, no logo is to be displayed on the login or portal pages:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# logo none
Router(config-webvpn-context)#
```

The following example configures the SSL VPN to display the default logo (Cisco) on the login and portal pages:

```
Router(config)# webvpn context SSLVPN
Router(config-webvpn-context)# logo none
Router(config-webvpn-context)#
```

**Related Commands**

| Command | Description |
|---|---|
| **webvpn context** | Enters SSLVPN configuration mode to configure the WebVPN context. |

# mask-urls

To obfuscate, or mask, sensitive portions of an enterprise URL, such as IP addresses, hostnames, or port numbers, use the **mask-urls** command in webvpn group policy configuration mode. To remove the masking, use the **no** form of this command.

**mask-urls**

**no mask-urls**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Sensitive portions of an enterprise URL are not masked.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

This command is configured in group configuration only.

## Examples

The following example shows that URL obfuscation (masking) has been configured for policy group "GP":

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group GP
Router(config-webvpn-group)# mask-urls
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# max-retry-attempts

To set the maximum number of retries before Single SignOn (SSO) authentication fails, use the **max-retry-attempts** command in webvpn sso server configuration mode. To remove the number of retries that were set, use the **no** form of this command.

**max-retry-attempts** *number-of-retries*

**no max-retry-attempts** *number-of-retries*

## Syntax Description

| | |
|---|---|
| *number-of-retries* | Number of retries. Value = 1 through 5. Default = 3. |

## Command Default

A maximum number of retries is not set. If this command is not configured, the default is 3 retries.

## Command Modes

Webvpn sso server configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

This command is useful for networks that are congested and tend to have losses. Corporate networks are generally not affected by congestion or losses.

## Examples

The following example shows that the maximum number of retries is 3:

```
webvpn context context1
 sso-server test-sso-server
  max-retry-attempts 3
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# max-users (WebVPN)

To limit the number of connections to an SSL VPN that will be permitted, use the **max-users** command in webvpn context configuration mode. To remove the connection limit from the SSL VPN context configuration, use the **no** form of this command.

**max-users** *number*

**no max-users**

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of SSL VPN user connections. A number from 1 to 1000 can be entered for this argument. |

## Command Default

The following is the default if this command is not configured or if the **no** form is entered:

*number* : 1000

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Examples

The following example configures a limit of 500 user connections that will be accepted by the SSL VPN:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# max-users 500
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# nbns-list

To enter the webvpn NBNS list configuration mode to configure a NetBIOS Name Service (NBNS) server list for Common Internet File System (CIFS) name resolution, use the **nbns-list** command in webvpn context configuration mode. To remove the NBNS server list from the SSL VPN context configuration, use the **no** form of this command.

**nbns-list** *name*

**no nbns-list** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the NBNS list. The name can be up to 64 characters in length. This argument is case sensitive. |

## Command Default

Webvpn NBNS list configuration mode is not entered, and a NBNS server list cannot be configured.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The NBNS server list is used to configure a list of Windows Internet Name Service (WINS) to resolve Microsoft file-directory shares. Entering the **nbns-list** command places the router in webvpn NBNS list configuration mode. You can specify up to three NetBIOS name servers. A single server is configured as the master browser if multiple servers are specified in the server list.

**Note** NBNS and CIFS resolution is supported only on Microsoft Windows 2000 or Linux Samba servers.

## Examples

The following example configures an NBNS server list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)#
```

**Related Commands**

| Command | Description |
|---|---|
| **nbns-server** | Adds a server to an NBNS server list. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# nbns-list (policy group)

To attach a NetBIOS name service (NBNS) server list to a policy group configuration, use the **nbns-list** command in webvpn group policy configuration mode. To remove the NBNS server list from the policy group configuration, use the **no** form of this command.

**nbns-list** *name*

**no nbns-list**

## Syntax Description

| | |
|---|---|
| *name* | Name of the NBNS server list that was configured in webvpn context configuration mode. |

## Command Default

An NBNS server list is not attached to a policy group configuration.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The configuration of this command applies to only clientless mode configuration.

## Examples

The following example applies the NBNS server list to the policy group configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)# exit
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# nbns-list SERVER_LIST
Router(config-webvpn-group)#
```

## Related Commands

| Command | Description |
|---|---|
| **nbns-list** | Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution. |
| **nbns-server** | Adds a server to an NBNS server list. |
| **policy group** | Enters webvpn group policy configuration mode to configure a group policy. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# nbns-server

To add a server to a NetBIOS name service (NBNS) server list, use the **nbns-server** command in webvpn NBNS list configuration mode. To remove the server entry from the NBNS server list, use the **no** form of this command.

**nbns-server** *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]

**no nbns-server** *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]

## Syntax Description

| | |
|---|---|
| *ip-address* | The IPv4 address of the NetBIOS server. |
| **master** | (Optional) Configures a single NetBIOS server as the master browser. |
| **timeout** *seconds* | (Optional) Configures the length of time, in seconds, that the networking device will wait for a query reply before sending a query to another NetBIOS server. A number from 1 through 30 can be configured for this argument. |
| **retries** *number* | (Optional) Number of times that the specified NetBIOS server will be queried. A number from 0 through 10 can be configured for this argument. Entering the number 0 configures the networking device not to resend a query. |

## Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

**timeout** 2
**retries** 2

## Command Modes

Webvpn NBNS list configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The server specified with the *ip-address* argument can be a primary domain controller (PDC) in a Microsoft network. A Windows Internet Naming Service (WINS) server cannot and should not be specified. When multiple NBNS servers are specified, a single server is configured as master browser.

## Examples

The following example adds three servers to an NBNS server list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
```

**Related Commands**

| Command | Description |
|---|---|
| **nbns-list** | Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# permit (webvpn acl)

To set conditions to allow packets to pass a named Secure Sockets Layer Virtual Private Network (SSL VPN) access list, use the **permit** command in webvpn acl configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

**permit** [**url** [**any** | *url-string*]] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | *source-ip source-mask*] [**any** | *destination-ip destination-mask*] **time-range** *time-range-name* [**syslog**]

**no permit url** [**any** | *url-string*] [**ip** | **tcp** | **udp** | **http** | **https** | **cifs**] [**any** | *source-ip source-mask*] [**any** | *destination-ip destination-mask*] **time-range** *time-range-name* [**syslog**]

## Syntax Description

| | |
|---|---|
| **url** | (Optional) Filtering rules are applied to a URL.<br>• Use the **any** keyword as an abbreviation for any URL. |
| *url-string* | (Optional) URL string defined as follows: **scheme://host[:port][/path]**<br>• **scheme**—Can be HTTP, Secure HTTPS (HTTPS), or Common Internet File System (CIFS). This field is required in the URL string.<br>• **host**—Can be a hostname or a host IP (host mask). The host can have one wildcard (*).<br>• **port**—Can be any valid port number (1–65535). It is possible to have multiple port numbers separated by a comma (,). The port range is expressed using a dash (-).<br>• **path**—Can be any valid path string. In the path string, the $user is translated to the current user name. |
| **ip** | (Optional) Permits only IP packets. When you enter the **ip** keyword, you must use the specific command syntax shown for the IP form of the **permit** command. |
| **tcp** | (Optional) Permits only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the **permit** command. |
| **udp** | (Optional) Permitss only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the **permit** command. |
| **http** | (Optional) Permits only HTTP packets. When you enter the **http** keyword, you must use the specific command syntax shown for the HTTP form of the **permit** command. |
| **https** | (Optional) Permits only HTTPS packets. When you enter the **https** keyword, you must use the specific command syntax shown for the HTTPS form of the **permit** command. |
| **cifs** | (Optional) Permits only CIFS packets. When you enter the **cifs** keyword, you must use the specific command syntax shown for the CIFS form of the **permit** command. |

| | |
|---|---|
| *source-ip source-mask* | (Optional) Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:<br>• Use a 32-bit quantity in four-part dotted-decimal format.<br>• Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255.<br>• Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0. |
| *destination-ip destination-mask* | (Optional) Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:<br>• Use a 32-bit quantity in four-part dotted-decimal format.<br>• Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255.<br>• Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0. |
| **time-range** *time-range-name* | Name of the time range that applies to this **permit** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively. |
| **syslog** | (Optional) System logging messages are generated. |

## Command Default

All packets are permitted.

## Command Modes

Webvpn acl configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Use this command following the **acl** command (in webvpn context configuration mode) to specify conditions under which a packet can pass the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this permit statement is in effect.

## Examples

The following example shows that all packets from the URL "https://10.168.2.228:34,80-90,100-/public" are permitted to pass ACL "acl1":

```
webvpn context context1
 acl acl1
  permit url "https://10.168.2.228:34,80-90,100-/public"
```

**Related Commands**

| Command | Description |
|---|---|
| **absolute** | Specifies an absolute time for a time range. |
| **deny (webvpn acl)** | Sets conditions in a named SSL VPN access list that will deny packets. |
| **periodic** | Specifies a recurring (weekly) time range for functions that support the time-range feature. |
| **time-range** | Enables time-range configuration mode and defines time ranges for extended access lists. |

# policy group

To enter webvpn group policy configuration mode to configure a group policy, use the **policy group** command in webvpn context configuration mode. To remove the policy group from the router configuration file, use the **no** form of this command.

**policy group** *name*

**no policy group** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the policy group. |

## Command Default

Webvpn group policy configuration mode is not entered, and a policy group is not configured.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of end users. Entering the **policy group** command places the router in webvpn group policy configuration mode. After the group policy is configured, the policy group is attached to the SSL VPN context configuration by configuring the **default-group-policy** command.

## Examples

The following example configures a policy group named ONE:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy ONE
```

## Related Commands

| Command | Description |
|---|---|
| **banner** | Configures a banner to be displayed after a successful login. |
| **citrix enabled** | Enables Citrix application support for end users in a policy group. |
| **default-group-policy** | Configures a default group policy for SSL VPN sessions. |
| **filter citrix** | Configures a Citrix application access filter. |
| **filter tunnel** | Configures a SSL VPN tunnel access filter. |
| **functions** | Enables a file access function or tunnel mode support in a group policy configuration. |
| **hide-url-bar** | Prevents the URL bar from being displayed on the SSL VPN portal page. |

| Command | Description |
|---|---|
| **nbns-list (policy group)** | Attaches a NBNS server list to a policy group configuration. |
| **port-forward (policy group)** | Attaches a port-forwarding list to a policy group configuration. |
| **svc address-pool** | Configures a pool of IP addresses to assign to end users in a policy group. |
| **svc default-domain** | Configures the domain for a policy group. |
| **svc dns-server** | Configures DNS servers for policy group end users. |
| **svc dpd-interval** | Configures the DPD timer value for the gateway or client. |
| **svc homepage** | Configures the URL of the web page that is displayed upon successful user login. |
| **svc keep-client-installed** | Configures the end user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled. |
| **svc msie-proxy** | Configures MSIE browser proxy settings for policy group end users. |
| **svc msie-proxy server** | Specifies a Microsoft Internet Explorer proxy server for policy group end users. |
| **svc rekey** | Configures the time and method that a tunnel key is refreshed for policy group end users. |
| **svc split** | Configures split tunneling for policy group end users. |
| **svc wins-server** | Configures configure WINS servers for policy group end users. |
| **timeout** | Configures the length of time that an end user session can remain idle or the total length of time that the session can remain connected. |
| **url-list (policy group)** | Attaches a URL list to policy group configuration. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# port-forward

To enter webvpn port-forward list configuration mode to configure a port-forwarding list, use the **port-forward** command in webvpn context configuration mode. To remove the port-forwarding list from the SSL VPN context configuration, use the **no** form of this command.

**port-forward** *name*

**no port-forward** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the port-forwarding list. |

## Command Default

Webvpn port-forward list configuration mode is not entered, and a port-forwarding list is not configured.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

The **port-forward** command is used to create the port-forwarding list. Application port number mapping (port forwarding) is configured with the **local-port** command in webvpn port-forward configuration mode.

A port-forwarding list is configured for thin client mode SSL VPN. Port forwarding extends the cryptographic functions of the SSL-protected browser to provide remote access to TCP-based applications that use well-known port numbers, such as POP3, SMTP, IMAP, Telnet, and SSH.

When port forwarding is enabled, the hosts file on the SSL VPN client is modified to map the application to the port number configured in the forwarding list. The application port mapping is restored to default when the user terminates the SSL VPN session.

## Examples

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com
remote-port 143 description IMAP
```

**Related Commands**

| Command | Description |
|---|---|
| **local-port (WebVPN)** | Remaps an application port number in a port-forwarding list. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# port-forward (policy group)

To attach a port-forwarding list to a policy group configuration, use the **port-forward** command in webvpn group policy configuration mode. To remove the port-forwarding list from the policy group configuration, use the **no** form of this command.

**port-forward** *name* **[auto-download]** | [**http-proxy [proxy-url {***homepage-url***}]]**

**no port-forward** *name* **[auto-download]** | [**http-proxy [proxy-url {***homepage-url***}]]**

## Syntax Description

| | |
|---|---|
| *name* | Name of the port-forwarding list that was configured in webvpn context configuration mode. |
| **auto-download** | (Optional) Allows for automatic download of the port-forwarding Java applet on the portal page of a website. |
| **http-proxy** | (Optional) Allows the Java applet to act as a proxy for the browser of the user. |
| **proxy-url** *homepage-url* | (Optional) Page at this URL address opens as the portal page of the user. |

## Command Default

A port-forwarding list is not attached to a policy group configuration.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(9)T | The **auto-download** keyword was added. |

## Usage Guidelines

The configuration of this command applies to only clientless mode configuration.

## Examples

The following example applies the port-forwarding list to the policy group configuration:

```
webvpn context context1
 port-forward EMAIL
  local-port 30016 remote-server mail.company.com remote-port 110 description POP3
  local-port 30017 remote-server mail.company.com remote-port 25 description SMTP
  local-port 30018 remote-server mail.company.com remote-port 143 description IMAP
  exit
 policy group ONE
 port-forward EMAIL auto-download
```

The following example shows that HTTP proxy has been configured. The page at URL “http://www.example.com” will automatically download as the home page of the user.

```
webvpn context myContext
 ssl authenticate verify all
```

```
 !
 !
 port-forward "email"
   local-port 20016 remote-server "ssl-server1.sslvpn-ios.com" remote-port 110 description
"POP-ssl-server1"
 !
 policy group myPolicy
   port-forward "email" auto-download http-proxy proxy-url "http://www.example.com"
 inservice
```

## Related Commands

| Command | Description |
|---|---|
| **local-port (WebVPN)** | Remaps an application port number in a port-forwarding list. |
| **policy group** | Enters webvpn group policy configuration mode to configure a group policy. |
| **port-forward** | Enters webvpn port-forward list configuration mode to configure a port-forwarding list. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# request-timeout

To set the number of seconds before an authentication request times out, use the **request-timeout** command in webvpn sso server configuration mode.

**request-timeout** *number-of-seconds*

**no request-timeout** *number-of-seconds*

## Syntax Description

| | |
|---|---|
| *number-of-seconds* | Number of seconds. Value = 10 through 30. Default = 15. |

## Command Default

None

## Command Modes

Webvpn sso server configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

This command is useful for networks that are congested and tend to have losses. Corporate networks are generally not affected by congestion or losses.

## Examples

The following example shows that the number of seconds before an authentication request times out is 25:

```
webvpn context context1
 sso-server test-sso-server
  request-timeout 25
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# secondary-color

To configure the color of the secondary title bars on the login and portal pages of a SSL VPN website, use the **secondary-color** command in webvpn context configuration mode. To remove the color from the WebVPN context configuration, use the **no** form of this command.

**secondary-color** *color*

**no secondary-color** *color*

## Syntax Description

| | |
|---|---|
| *color* | The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a"#"), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):<br>• \#/x{6}<br>• \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255)<br>• \w+<br>The default color is purple. |

## Defaults

The color purple is used if this command is not configured or if the **no** form is entered.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

Configuring a new color overrides the color of the preexisting color.

## Examples

The following examples show the three forms in which the secondary color is configured:

```
Router(config-webvpn-context)# secondary-color darkseagreen
Router(config-webvpn-context)# secondary-color #8FBC8F
Router(config-webvpn-context)# secondary-color 143,188,143
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# secondary-text-color

To configure the color of the text on the secondary bars of an SSL VPN website, use the **secondary-text-color** command in webvpn context configuration mode. To revert to the default color, use the **no** form of this command.

**secondary-text-color** [**black** | **white**]

**no secondary-text-color** [**black** | **white**]

## Syntax Description

| | |
|---|---|
| **black** | (Optional) Color of the text is black. This is the default value. |
| **white** | (Optional) Color of the text is white. |

## Defaults

The color of the text on secondary bars is black if this command is not configured or if the **no** form is entered.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

The color of the text on the secondary bars must be aligned with the color of the text on the title bar.

## Examples

The following example sets the secondary text color to white:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# secondary-text-color white
Router(config-webvpn-context)#
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# secret-key

To configure the policy server secret key that is used to secure authentication requests, use the **secret-key** command in webvpn sso server configuration mode. To remove the secret key, use the **no** form of this command.

**secret-key** *key-name*

**no secret-key** *key-name*

## Syntax Description

| | |
|---|---|
| *key-name* | Name of secret key. |

## Command Default

A policy server secret key is not configured.

## Command Modes

Webvpn sso server configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

**Note**

- A web agent URL and policy server secret key are required for a Single SignOn (SSO) server configuration. If the web agent URL and policy server secret key are not configured, a warning message is displayed. (See the Warning Message section in the Examples section below.)
- This is the same secret key that should be configured on the Cisco SiteMinder plug-in.

## Examples

The following example shows the policy server secret key is “example.123”:

```
webvpn context context1
 sso-server test-sso-server
  secret-key example.123
```

### Warning Message

If a web agent URL and policy server secret key are not configured, a message similar to the following is received:

```
Warning: must configure web agent URL for sso-server “example”
Warning: must configure SSO policy server secret key for sso-server “example”
Warning: invalid configuration. SSO for “example” being disabled
```

**Related Commands**

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# show webvpn context

To display the operational status and configuration parameters for SSL VPN context configurations, use the **show webvpn context** command in privileged EXEC mode.

**show webvpn context** [*name*]

## Syntax Description

| | |
|---|---|
| *name* | (Optional) Filters the output to display more detailed information about the named context. |

## Command Default

Entering this command without specifying a context name displays general information about the operational status of all SSL VPN contexts.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(11)T | An output example was added for Single SignOn (SSO) servers. |

## Usage Guidelines

Entering a context name displays more detailed information, such as the operational status and specific configuration information for the named context.

## Examples

The following is sample output from the **show webvpn context** command:

```
Router# show webvpn context context1

Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host

Context Name        Gateway  Domain/VHost      VRF      AS    OS
------------        -------  ------------      -------  ----  --------
Default_context     n/a      n/a               n/a      down  down
con-1               gw-1     one               -        up    up
con-2               -        -                 -        down  down
```

Table 6 describes the significant fields shown in the display.

***Table 6 show webvpn context Field Descriptions***

| Field | Description |
|---|---|
| Context Name | Displays the name of the context. |
| Gateway | Displays the name of the associated gateway. n/a is displayed if no gateway is associated. |

*Table 6 show webvpn context Field Descriptions (continued)*

| Field | Description |
|---|---|
| Domain/VHost | Displays the SSL VPN domain or virtual hostname. |
| VRF | Displays the Virtual Private Network (VPN) routing and forwarding (VRF) —if configured—that is associated with the context configuration. |
| AS | Displays the administrative status of the SSL VPN context. The status is displayed as “up” or “down.” |
| OS | Displays the operational status of the SSL VPN context. The status is displayed as “up” or “down.” |

The following is sample output from the **show webvpn context** command, entered with the name of a specific SSL VPN context:

```
Router# show webvpn context context1

Admin Status: up
Operation Status: up
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List not configured
AAA Authentication Domain not configured
Default Group Policy: PG_1
Associated WebVPN Gateway: GW_1
Domain Name: DOMAIN_ONE
Maximum Users Allowed: 10000 (default)
NAT Address not configured
VRF Name not configured
```

Table 7 describes the significant fields shown in the display.

*Table 7 show webvpn context (Specific WebVPN Context) Field Descriptions*

| Field | Description |
|---|---|
| Admin Status | Administrative status of the context. The status is displayed as “up” or “down.” The **inservice** command is used to configure this configuration parameter. |
| Operation Status | Displays the operational status of the SSL VPN. The status is displayed as “up” or “down.” The context and the associated gateway must both be in an enabled state for the operational status to be “up.” |
| CSD Status | Displays the status of Cisco Secure Desktop (CSD). The status is displayed as “Enabled” or “Disabled.” |
| Certificate authentication type | Displays the CA type. |
| AAA Authentication List... | Displays the authentication list if configured. |
| AAA Authentication Domain... | Displays the AAA domain if configured. |
| Default Group Policy | Name of the group policy configured under the named context. |
| Domain Name | Domain name or virtual hostname configured under the named context. |

*Table 7 show webvpn context (Specific WebVPN Context) Field Descriptions (continued)*

| Field | Description |
|---|---|
| Maximum Users Allowed | Displays the maximum number of user sessions that can be configured. |
| NAT Address... | Displays the Network Address Translation (NAT) address if configured. |
| VRF | Displays the Virtual Private Network (VPN) routing and forwarding (VRF)—if configured—that is associated with the context configuration. |

The following output is an example of additional information that can be displayed for SSO servers configured for the SSL VPN context:

```
Router# show webvpn context context1

   Web agent URL :  "http://example.examplecompany.com/vpnauth/"
   Policy Server Secret : "Example123"
   Request Re-tries : 5, Request timeout: 15-second
```

Table 8 describes the significant fields shown in the display.

*Table 8 show webvpn context (SSO) Field Descriptions*

| Field | Description |
|---|---|
| Web agent URL | URL of a web server in which the Cisco SiteMinder web agent is running. |
| Policy Server Secret | Shared secret key for user-session authentication on an SSO server. |
| Request Re-tries | Number of retries of the SSO sign-on request. |
| Request timeout | Timeout value of a request. |

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# show webvpn gateway

To display the status of a SSL VPN gateway, use the **show webvpn gateway** command in privileged EXEC mode.

**show webvpn gateway** [*name*]

## Syntax Description

| | |
|---|---|
| *name* | (Optional) Filters the output to display more detailed information about the named gateway. |

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Entering this command without specifying a gateway name, displays general the operational status of all SSL VPN gateways. Entering a gateway name displays the IP address and CA trustpoint.

## Examples

The following is sample output from the **show webvpn gateway** command:

```
Router# show webvpn gateway

Gateway Name                    Admin  Operation
------------                    -----  ---------
GW_1                            up     up
GW_2                            down   down
```

Table 9 describes the significant fields shown in the display.

***Table 9 show webvpn gateway Field Descriptions***

| Field | Description |
|---|---|
| Gateway Name | Name of the gateway. |
| Admin | The administrative status of the gateway, displayed as “up” or “down.” Administrative status is configured with the **inservice** command. |
| Operation | The operational status of the gateway, displayed as “up” or “down.” The gateway must be “inservice” and configured with a valid IP address to be in an “up” state. |

The following is sample output from the **show webvpn gateway** command, entered with a specific SSL VPN gateway name:

```
Router# show webvpn gateway GW_1

Admin Status: up
Operation Status: up
IP: 10.1.1.1, port: 443
SSL Trustpoint: TP-self-signed-26793562
```

Table 10 describes the significant fields shown in the display.

***Table 10 show webvpn gateway name Field Descriptions***

| Field | Description |
|---|---|
| Admin Status | The administrative status of the gateway, displayed as “up” or “down.” Administrative status is configured with the **inservice** command. |
| Operation Status | The operational status of the gateway, displayed as “up” or “down.” The gateway must be “inservice” and configured with a valid IP address to be in an “up” state. |
| IP: ... port: ... | The configured IP address and port number of the WebVPN gateway. The default port number 443. |
| SSL Trustpoint: | Configures the CA certificate trust point. |

## Related Commands

| Command | Description |
|---|---|
| **webvpn gateway** | Enters webvpn gateway configuration mode to configure a SSL VPN gateway. |

# show webvpn nbns

To display information in the NetBIOS Name Service (NBNS) cache, use the **show webvpn nbns** command in privileged EXEC mode.

**show webvpn nbns** {**context** {**all** | *name*}}

## Syntax Description

| | |
|---|---|
| **context** *name* | Filters the output to display NBNS information for the named context. |
| **context all** | Displays NBNS information for all contexts. |

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

This command is used to display information about NBNS cache entries. The NetBIOS name, IP address of the Windows Internet Name Service (WINS) server, and associated time stamps.

## Examples

The following is sample output from the **show webvpn nbns** command, entered with the **context** and **all** keywords:

```
Router# show webvpn nbns context all

NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
NetBIOS name        IP Address       Timestamp

0 total entries
```

Table 1 describes the significant fields shown in the display.

***Table 11 show webvpn nbns context all Field Descriptions***

| Field | Description |
|---|---|
| NetBIOS name | NetBIOS name. |
| IP Address | The IP address of the WINs server. |

*Table 11 show webvpn nbns context all Field Descriptions (continued)*

| Field | Description |
|---|---|
| Timestamp | Time stamp for the last entry. |
| ... total entries | Total number of NetBIOS cache entries. |

## Related Commands

| Command | Description |
|---|---|
| **nbns-list** | Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution. |
| **webvpn install** | Installs a CSD or Cisco AnyConnect VPN Client package file to a SSL VPN gateway for distribution to end users. |

# show webvpn policy

To display the context configuration associated with a policy group, use the **show webvpn policy** command in privileged EXEC mode.

**show webvpn policy group** *name* **context** {**all** | *name*}

## Syntax Description

| | |
|---|---|
| **group** *name* | Displays information for the named policy group. |
| **context all** | Displays information for all context configurations with which the policy group is associated. |
| **context** *name* | Displays information for the named context configuration. |

## Command Default

None.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(11)T | An output example was added for Single SignOn (SSO) server information. |

## Usage Guidelines

This command is used to display configuration settings that apply only to the policy group. This command can also be used to display all contexts for which the policy group is configured.

## Examples

The following is sample output from the **show webvpn policy** command:

```
Router# show webvpn policy group ONE context all

WEBVPN: group policy = ONE ; context = SSLVPN
      idle timeout = 2100 sec
      session timeout = 43200 sec
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
WEBVPN: group policy = ONE ; context = SSLVPN_TWO
      idle timeout = 2100 sec
      session timeout = 43200 sec
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep sslvpn client installed = disabled
      rekey interval = 3600 sec
```

```
      rekey method =
      lease duration = 43200 sec
```

The following output example displays information about a SSO server configured for a policy group of the SSL VPN context:

```
Router# show webvpn policy group ONE context all

WV: group policy = sso ; context = test_sso
  idle timeout = 2100 sec
  session timeout = 43200 sec
  sso server name = "server2
  citrix disabled
  dpd client timeout = 300 sec
  dpd gateway timeout = 300 sec
  keep sslvpn client installed = disabled
  rekey interval = 3600 sec
  rekey method =
  lease duration = 43200 sec
```

Table 12 describes the significant fields shown in the displays.

***Table 12 show webvpn policy Field Descriptions***

| Field | Description |
|---|---|
| group policy | Name of the policy group. |
| context | Name of the SSL VPN context. |
| idle timeout | Length of time that an remote-user session can remain idle. |
| session timeout | Length of time that a remote-user session can remain active. |
| citrix | Support for Citrix applications, shown as “disabled” or “enabled.” |
| dpd client timeout | Length of time that a session will be maintained with a nonresponsive end user (remote client). |
| dpd gateway timeout | Length of the time that a session will be maintained with a nonresponsive SSL VPN gateway. |
| keep sslvpn client installed | Cisco AnyConnect VPN Client software installation policy on the end user (remote PC). “enabled” indicates that Cisco AnyConnect VPN Client software remains installed after the SSL VPN session is terminated. “disabled” indicates that Cisco AnyConnect VPN Client software is pushed to the end user each time a connection is established. |
| rekey interval | Length of time between tunnel key refresh cycles. |
| rekey method | Tunnel key authentication method. |
| lease duration | Tunnel key lifetime. |
| sso server name | Name of the SSO server. |

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters SSL VPN group policy configuration mode to configure a group policy. |

# show webvpn session

To display Secure Sockets Layer Virtual Private Network (SSL VPN) user session information, use the **show webvpn session** command in privileged EXEC mode.

**show webvpn session** {[**user** *name*] **context** {**all** | *name*}}

## Syntax Description

| | |
|---|---|
| **user** *name* | (Optional) Displays detailed information about the named user session. |
| **context all** | Displays a list of active users sessions for all locally configured contexts. |
| **context** *name* | Displays a list of active users for only the named context. |

## Command Default

Session information is not displayed.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

This command is used to list active SSL VPN connections or to display context configuration policies that apply to the specified end user.

## Examples

The following is sample output from the **show webvpn session** command. The output is filtered to display user session information for only the specified context.

```
Router# show webvpn session context context1

WebVPN context name: context1
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              10.2.1.220                 2         04:47:16  00:01:26
user2              10.2.1.221                 2         04:48:36  00:01:56
```

Table 1 describes the significant fields shown in the display.

***Table 13 show webvpn session Field Descriptions***

| Field | Description |
|---|---|
| WebVPN context name | Name of the context. |
| Client_Login_Name | Login name for the end user (remote PC or device). |
| Client_IP_Address | IP address of the remote user. |
| No_of_Connections | Number of times the remote user has connected. |

*Table 13 show webvpn session Field Descriptions (continued)*

| Field | Description |
|---|---|
| Created | Time, in hh:mm:ss, when the remote connection was established. |
| Last_Used | Time, in hh:mm:ss, that the user connection last generated network activity. |

The following is sample output from the **show webvpn session** command. The output is filtered to display session information for a specific user.

```
Router# show webvpn session user user1 context all

WebVPN user name = user1 ; IP address = 10.2.1.220; context = SSLVPN
    No of connections: 0
    Created 00:00:19, Last-used 00:00:18
    CSD enabled
    CSD Session Policy
       CSD Web Browsing Allowed
       CSD Port Forwarding Allowed
       CSD Full Tunneling Disabled
       CSD FILE Access Allowed
    User Policy Parameters
      Group name = ONE
    Group Policy Parameters
      url list name = "Cisco"
      idle timeout = 2100 sec
      session timeout = 43200 sec
      port forward name = "EMAIL"
      tunnel mode = disabled
      citrix disabled
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keep stc installed = disabled
      rekey interval = 3600 sec
      rekey method = ssl
      lease duration = 3600 sec
```

Table 2 describes the significant fields shown in the display.

*Table 14 show webvpn session Field Descriptions*

| Field | Description |
|---|---|
| WebVPN user name | Name of the end user. |
| IP address | IP address of the end user. |
| context | Name of the context to which user policies apply. |
| No of connections | Number of times the remote user has connected. |
| Created | Time, in hh:mm:ss, when the remote connection was established. |
| Last-used | Time, in hh:mm:ss, that the user connection last generated network activity. |
| CSD enabled | Status of Cisco Secure Desktop (CSD). |

*Table 14 show webvpn session Field Descriptions (continued)*

| Field | Description |
|---|---|
| CSD Session Policy | CSD policy configuration parameters. The parameters are each displayed as “Allowed” or “Disabled.” |
| CSD Web Browsing | Status of Web Internet access through the SSL VPN. |
| CSD Port Forwarding | Status of application port forwarding. |
| CSD Full Tunneling | Status of CSD full-tunnel support. |
| CSD FILE Access | Status of CSD network share and file access. |
| User Policy Parameters | User policy configuration parameters. |
| Group name | Name of the policy group to which the user belongs. |
| Group Policy Parameters | Policy group configuration parameters. The parameters are displayed as default and administrator-defined values. |
| url list name | Name of the URL list configured with the **url-list** command. |
| idle timeout | Length of time that a remote-user session can remain idle. |
| session timeout | Length of time that a remote-user session can remain active. |
| port forward name | Name of the port-forwarding list configured with the **port-forward (policy group)** command. |
| tunnel mode | Tunnel mode of the remote-user session. |
| citrix... | Citrix support for the remote user. |
| dpd client timeout | Length of time that a session will be maintained with a nonresponsive end user (remote client). |
| dpd gateway timeout | Length of the time that a session will be maintained with a nonresponsive SSL VPN gateway. |
| keep stc installed | Cisco AnyConnect VPN Client software installation policy on the end user (remote PC). “enabled” indicates that Cisco AnyConnect VPN Client software remains installed after the SSL VPN session is terminated. “disabled” indicates that Cisco AnyConnect VPN Client software is pushed to the end user each time a connection is established. |
| rekey interval | Length of time between tunnel key refresh cycles. |
| rekey method | Tunnel key authentication method. |
| lease duration | Tunnel key lifetime. |

# show webvpn stats

To display Secure Socket Layer Virtual Private Network (SSL VPN) application and network statistics, use the **show webvpn stats** command in privileged EXEC mode.

**show webvpn stats** [**cifs | citrix | mangle | port-forward | sso | tunnel**] [**detail**] [**context** {**all** | *name*}]

## Syntax Description

| | |
|---|---|
| **cifs** | (Optional) Displays Windows file share (Common Internet File System[CIFS]) statistics. |
| **citrix** | (Optional) Displays Citrix application statistics. |
| **mangle** | (Optional) Displays URL mangling statistics. |
| **port-forward** | (Optional) Displays port forwarding statistics. |
| **sso** | (Optional) Displays statistics for the Single SignOn (SSO) server. |
| **tunnel** | (Optional) Displays VPN tunnel statistics. |
| **detail** | (Optional) Displays detailed information. |
| **context** {**all** \| *name*} | (Optional) Displays information for a specific context or all contexts. |

## Command Default

None

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.4(11)T | The **sso** keyword was added for Cisco 6500 Catalyst switches. |
| 12.4(15)T | Output information was added for Cisco Express Forwarding (CEF). |

## Usage Guidelines

This command is used to display SSL VPN application, authentication, and network statistics and counters.

## Examples

The following is sample output from the **show webvpn stats** command entered with the **detail** and **context** keywords:

```
Router# show webvpn stats detail context context1

WebVPN context name : context1
User session statistics:
    Active user sessions     : 0          AAA pending reqs         : 0
    Peak user sessions       : 0          Peak time                : never
    Active user TCP conns    : 0          Terminated user sessions : 0
    Session alloc failures   : 0          Authentication failures  : 0
    VPN session timeout      : 0          VPN idle timeout         : 0
    User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
```

```
    CEF switched packets - client: 0          , server: 0
    CEF punted packets - client: 0          , server: 0

Mangling statistics:
    Relative urls             : 0          Absolute urls             : 0
    Non-http(s) absolute urls: 0           Non-standard path urls    : 0
    Interesting tags          : 0          Uninteresting tags        : 0
    Interesting attributes    : 0          Uninteresting attributes : 0
    Embedded script statement: 0           Embedded style statement  : 0
    Inline scripts            : 0          Inline styles             : 0
    HTML comments             : 0          HTTP/1.0 requests         : 0
    HTTP/1.1 requests         : 0          Unknown HTTP version      : 0
    GET requests              : 0          POST requests             : 0
    CONNECT requests          : 0          Other request methods     : 0
    Through requests          : 0          Gateway requests          : 0
    Pipelined requests        : 0          Req with header size >1K  : 0
    Processed req hdr bytes   : 0          Processed req body bytes  : 0
    HTTP/1.0 responses        : 0          HTTP/1.1 responses        : 0
    HTML responses            : 0          CSS responses             : 0
    XML responses             : 0          JS responses              : 0
    Other content type resp   : 0          Chunked encoding resp     : 0
    Resp with encoded content: 0           Resp with content length  : 0
    Close after response      : 0          Resp with header size >1K: 0
    Processed resp hdr size   : 0          Processed resp body bytes: 0
    Backend https response    : 0          Chunked encoding requests: 0

CIFS statistics:
  SMB related Per Context:
    TCP VC's                  : 0          UDP VC's                  : 0
    Active VC's               : 0          Active Contexts           : 0
    Aborted Conns             : 0
  NetBIOS related Per Context:
    Name Queries              : 0          Name Replies              : 0
    NB DGM Requests           : 0          NB DGM Replies            : 0
    NB TCP Connect Fails      : 0          NB Name Resolution Fails  : 0
  HTTP related Per Context:
    Requests                  : 0          Request Bytes RX          : 0
    Request Packets RX        : 0          Response Bytes TX         : 0
    Response Packets TX       : 0          Active Connections        : 0
    Active CIFS context       : 0          Requests Dropped          : 0

Socket statistics:
    Sockets in use            : 0          Sock Usr Blocks in use    : 0
    Sock Data Buffers in use  : 0          Sock Buf desc in use      : 0
    Select timers in use      : 0          Sock Select Timeouts      : 0
    Sock Tx Blocked           : 0          Sock Tx Unblocked         : 0
    Sock Rx Blocked           : 0          Sock Rx Unblocked         : 0
    Sock UDP Connects         : 0          Sock UDP Disconnects      : 0
    Sock Premature Close      : 0          Sock Pipe Errors          : 0
    Sock Select Timeout Errs  : 0

Port Forward statistics:
    Connections serviced      : 0            Server Aborts (idle)      : 0
  Client                                   Server
    in pkts                   : 0            out pkts                  : 0
    in bytes                  : 0            out bytes                 : 0
    out pkts                  : 0            in pkts                   : 0
    out bytes                 : 0            in bytes                  : 0

WEBVPN Citrix statistics:
Connections serviced : 0

                Server                    Client
  Packets in  : 0                          0
```

```
  Packets out : 0                         0
  Bytes in    : 0                         0
  Bytes out   : 0                         0

Tunnel Statistics:
    Active connections       : 0
    Peak connections         : 0          Peak time                : never
    Connect succeed          : 0          Connect failed           : 0
    Reconnect succeed        : 0          Reconnect failed         : 0
    SVCIP install IOS succeed: 0          SVCIP install IOS failed : 0
    SVCIP clear IOS succeed  : 0          SVCIP clear IOS failed   : 0
    SVCIP install TCP succeed: 0          SVCIP install TCP failed : 0
    DPD timeout              : 0
  Client                                 Server
    in  CSTP frames          : 0          out IP pkts              : 0
    in  CSTP data            : 0          out stitched pkts        : 0
    in  CSTP control         : 0          out copied pkts          : 0
    in  CSTP Addr Reqs       : 0          out bad pkts             : 0
    in  CSTP DPD Reqs        : 0          out filtered pkts        : 0
    in  CSTP DPD Resps       : 0          out non fwded pkts       : 0
    in  CSTP Msg Reqs        : 0          out forwarded pkts       : 0
    in  CSTP bytes           : 0          out IP bytes             : 0
    out CSTP frames          : 0          in  IP pkts              : 0
    out CSTP data            : 0          in  invalid pkts         : 0
    out CSTP control         : 0          in  congested pkts       : 0
    out CSTP Addr Resps      : 0          in  bad pkts             : 0
    out CSTP DPD Reqs        : 0          in  nonfwded pkts        : 0
    out CSTP DPD Resps       : 0          in  forwarded pkts       : 0
    out CSTP Msg Reqs        : 0
    out CSTP bytes           : 0          in  IP bytes             : 0
```

The following example displays SSO statistics:

```
Router# show webvpn stats sso

   Auth Requests            : 4          Pending Auth Requests      : 0
   Successful Requests      : 1          Failed Requests            : 3
   Retranmissions           : 0          DNS Errors                 : 0
   Connection Errors        : 0          Request Timeouts           : 0
   Unknown Responses        : 0
```

The following example displays information about CEF:

```
Router# show webvpn stats

User session statistics:
   Active user sessions     : 1          AAA pending reqs         : 0
   Peak user sessions       : 1          Peak time                : 00:12:01
   Active user TCP conns    : 1          Terminated user sessions : 1
   Session alloc failures   : 0          Authentication failures  : 0
   VPN session timeout      : 0          VPN idle timeout         : 0
   User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
   Exceeded total user limit: 0
   Client process rcvd pkts : 37         Server process rcvd pkts : 0
   Client process sent pkts : 1052       Server process sent pkts : 0
   Client CEF received pkts : 69         Server CEF received pkts : 0
   Client CEF rcv punt pkts : 1          Server CEF rcv punt pkts : 0
   Client CEF sent pkts     : 1102       Server CEF sent pkts     : 0
   Client CEF sent punt pkts: 448        Server CEF sent punt pkts: 0

   SSLVPN appl bufs inuse   : 0          SSLVPN eng  bufs inuse   : 0
  Active server TCP conns   : 0
```

The descriptions in the displays are self-explanatory.

**Related Commands**

| Command | Description |
|---|---|
| **clear webvpn stats** | Clears application and access counters on a SSL VPN gateway. |

# ssl encryption

To specify the encryption algorithm that the Secure Sockets Layer (SSL) protocol uses for SSL Virtual Private Network (SSL VPN) connections, use the **ssl encryption** command in webvpn gateway configuration mode. To remove an algorithm from the SSL VPN gateway, use the **no** form of this command.

**ssl encryption** [**3des-sha1**] [**aes-sha1**] [**rc4-md5**]

**no ssl encryption**

## Syntax Description

| | |
|---|---|
| **3des-sha1** | (Optional) Configures the 3 DES-SHA1 encryption algorithm. |
| **aes-sha1** | (Optional) Configures the AES-SHA1 encryption algorithm. |
| **rc4-md5** | (Optional) Configures the RC4-MD5 encryption algorithm. |

## Defaults

All algorithms are available in the order shown above.

## Command Modes

Webvpn gateway configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

The SSL VPN provides remote-access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption. Configuring this command allows you to restrict the encryption algorithms that SSL uses in Cisco IOS software. The ordering of the algorithms specifies the preference. If you specify this command after you have specified an algorithm, the previous setting is overridden.

## Examples

The following example configures the gateway to use, in order, the 3DES-SHA1, AES-SHA1, or RC4-MD5 encryption algorithms for SSL connections:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ssl encryption rc4-md5
Router(config-webvpn-gateway)#
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn gateway** | Defines a SSL VPN gateway and enters webvpn gateway configuration mode. |

# ssl trustpoint

To configure the certificate trustpoint on a SSL VPN gateway, use the **ssl trustpoint** command in webvpn gateway configuration mode. To remove the trustpoint association, use the **no** form of this command.

**ssl trustpoint** *name*

**no ssl trustpoint**

## Syntax Description

| | |
|---|---|
| *name* | Name of the trust point. |

## Defaults

This command has no default behavior or values.

## Command Modes

SSLVPN gateway configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

You can configure a persistent self-signed certificate or an external CA server to generate a valid trustpoint.

## Examples

The following example configures a trustpoint named CA_CERT:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ssl trustpoint CA_CERT
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn gateway** | Defines a SSL VPN gateway and enters webvpn gateway configuration mode. |

# sso-server

To create a Single SignOn (SSO) server name under a Secure Sockets Layer Virtual Private Network (SSL VPN) context and to enter webvpn sso server configuration mode—and to attach an SSO server to a policy group—use the **sso-server** command in webvpn sso server configuration and group policy configuration modes, respectively. To remove an SSO server name, use the **no** form of this command.

**sso-server** *name*

**no sso-server** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the SSO server. |

## Command Default

A SSO server is not created or attached to a policy group.

## Command Modes

Webvpn sso server configuration
Group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

The SSO server name is configured under the SSL VPN context in webvpn context configuration mode. All SSO server-related parameters, such as web agent URL and policy server secret key, are configured under the SSO server name. The SSO server name is attached to the policy group in webvpn group policy configuration mode.

## Examples

The following example shows that the SSO server "test-sso-server" is created under the SSL VPN context and attached to a policy group named "ONE":

```
webvpn context context1
 sso-server "test-sso-server"
  web-agent-url "http://webagent.example.com"
  secret-key "12345"
  retries 3
  timeout 15
 policy group ONE
  sso-server "test-sso-server"
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# svc address-pool

To configure a pool of IP addresses to assign to end users in a policy group, use the **svc address-pool** command in webvpn group policy configuration mode. To remove the address pool from the policy group configuration, use the **no** form of this command.

**svc address-pool** *name*

**no svc address-pool**

## Syntax Description

| | |
|---|---|
| *name* | Name of the address pool that is configured using the **ip local pool** command. |

## Command Default

A pool of IP addresses are not assigned to end users.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The address pool is first defined with the **ip local pool** command in global configuration mode. The standard configuration assumes that the IP addresses in the pool are reachable from a directly connected network.

### Configuring Address Pools for Nondirectly Connected Networks

If you need to configure an address pool for IP addresses from a network that is not directly connected, perform the following steps:

1. Create a local loopback interface and configure it with an IP address and subnet mask from the address pool.
2. Configure the address pool with the **ip local pool** command. The range of addresses must fall under the subnet mask configured in Step 1.
3. Configure the **svc address-pool** command with name configured in Step 2.

See the second example on this command reference page for a complete configuration example.

**Note** SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

### Directly Connected Network Example

The following example configures the 192.168.1/24 network as an address pool:

```
Router(config)# ip local pool ADDRESSES 192.168.1.1 192.168.1.254
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

### Nondirectly Connected Network Example

The following example configures the 172.16.1/24 network as an address pool. Because the network is not directly connected, a local loopback is configured.

```
Router(config)# interface loopback 0
Router(config-int)# ip address 172.16.1.128 255.255.255.0
Router(config-int)# no shutdown
Router(config-int)# exit
Router(config)# ip local pool ADDRESSES 172.16.1.1 172.16.1.254
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
```

## Related Commands

| Command | Description |
|---|---|
| **ip local pool** | Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface. |
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# svc default-domain

To configure the Cisco AnyConnect VPN Client domain for a policy group, use the **svc default-domain** command in webvpn group policy configuration mode. To remove the domain from the policy group configuration, use the **no** form of this command.

**svc default-domain** *name*

**no svc default-domain**

## Syntax Description

| | |
|---|---|
| *name* | Name of the domain. |

## Command Default

Cisco AnyConnect VPN Client domain is not configured.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

**Note** SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example configures cisco.com as the default domain:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc default-domain cisco.com
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# svc dns-server

To configure Domain Name System (DNS) servers for policy group end users, use the **svc dns-server** command in webvpn group policy configuration mode. To remove a DNS server from the policy group configuration, use the **no** form of this command.

**svc dns-server** {**primary** | **secondary**} *ip-address*

**no svc dns-server** {**primary** | **secondary**}

## Syntax Description

| | |
|---|---|
| **primary** \| **secondary** | Configures the primary or secondary DNS server. |
| *ip-address* | An IPv4 address is entered to identify the server. |

## Command Default

DNS servers are not configured.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

**Note** SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dns-server primary 192.168.3.1
Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# svc dpd-interval

To configure the dead peer detection (DPD) timer value for the gateway or client, use the **svc dpd-interval** command in webvpn group policy configuration mode. To remove a DPD timer value from the policy group configuration, use the **no** form of this command.

**svc dpd-interval** {**client** | **gateway**} *seconds*

**no svc dpd-interval** {**client** | **gateway**}

## Syntax Description

| | |
|---|---|
| **client** \| **gateway** | Specifies the client or gateway. |
| *seconds* | Sets the time interval, in seconds, for the DPD timer. A number from 0 through 3600 is entered. |

## Command Default

The DPD timer is reset every time a packet is received over the Secure Sockets Layer Virtual Private Network (SSL VPN) tunnel from the gateway or end user.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

**Note** SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example sets the DPD timer to 30 seconds for a SSL VPN gateway and to 5 minutes for end users (remote PC or device):

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dpd-interval gateway 30
Router(config-webvpn-group)# svc dpd-interval client 300
Router(config-webvpn-group)#
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# svc homepage

To configure the URL of the web page that is displayed upon successful user login, use the **svc homepage** command in webvpn group policy configuration mode. To remove the URL from the policy group configuration, use the **no** form of this command.

**svc homepage** *string*

**no svc homepage**

## Syntax Description

| | |
|---|---|
| *string* | The *string* argument is entered as an HTTP URL. The URL can be up to 255 characters in length. |

## Command Default

URL of the home page is not configured.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

**Note** SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example configures www.cisco.com as the Cisco AnyConnect VPN Client home page:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc homepage www.cisco.com
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# svc keep-client-installed

To configure the end user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled, use the **svc keep-client-installed** command in webvpn group policy configuration mode. To remove the software installation requirement from the policy group configuration, use the **no** form of this command.

**svc keep-client-installed**

**no svc keep-client-installed**

## Syntax Description

This command has no keywords or arguments.

## Command Default

No default behavior or values.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The configuration of this command removes the overhead of pushing the Cisco AnyConnect VPN Client software to the end user on each connection attempt.

**Note** SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example configures end users to keep Cisco AnyConnect VPN Client software installed:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc keep-client-installed
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# svc msie-proxy

To configure Microsoft Internet Explorer (MSIE) browser proxy settings for policy group end users, use the **svc msie-proxy** command in webvpn group policy configuration mode. To remove a MSIE proxy setting from the policy group configuration, use the **no** form of this command.

**svc msie-proxy** {**server** *host* | **exception** *host* | **option** {**auto** | **bypass-local** | **none**}}

**no svc msie-proxy** {**server** *host* | **exception** *host* | **option** {**auto** | **bypass-local** | **none**}}

## Syntax Description

| | |
|---|---|
| **server** *host* | Specifies a MSIE proxy server for policy group end users. The *host* argument specifies the location of the MSIE server. The *host* argument is configured as an IPv4 address or fully qualified domain name, followed by a colon and port number. |
| **exception** *host* | Configures the browser not to send traffic for a single Domain Name System (DNS) hostname or IP address through the proxy. |
| **option auto** | Configures the browser to automatically detect proxy settings. |
| **option bypass-local** | Configures the browser to bypass proxy settings that are configured on the remote user. |
| **option none** | Configures the browser to use no proxy settings. |

## Command Default

MSIE browser proxy settings are not configured for policy group end users.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The configuration of this command is applied to end users that use a MSIE browser. The configuration of this command has no effect on any other browser type.

**Note** SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example configures automatic detection of MSIE proxy settings and configures proxy exceptions for traffic from www.example.com and the 10.20.20.1 host:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy option auto
Router(config-webvpn-group)# svc msie-proxy exception www.example.com
Router(config-webvpn-group)# svc msie-proxy exception 10.20.20.1
```

The following example configures a connection to an MSIE proxy server through a fully qualified domain name (FQDN) and a port number:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server www.example.com:80
```

The following example configures a connection to an MSIE proxy server through an IP address and port number:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# svc rekey

To configure the time and method that a tunnel key is refreshed for policy group end users, use the **svc rekey** command in webvpn group policy configuration mode. To remove the tunnel key configuration from the policy group configuration, use the **no** form of this command.

**svc rekey** {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}

**no svc rekey** {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}

## Syntax Description

| | |
|---|---|
| **method new-tunnel** | Refreshes the tunnel key by creating a new tunnel connection to the end user. |
| **method ssl** | Refreshes the tunnel key by renegotiating the Secure Sockets Layer (SSL) session. |
| **time** *seconds* | Configures the time interval, in seconds, at which the tunnel key is refreshed. A number from 0 through 43200 seconds is entered. |

## Command Default

Time and method are not configured.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

**Note** SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example configures the tunnel key to be refreshed by initiating a new tunnel connection once an hour:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc rekey method new-tunnel
Router(config-webvpn-group)# svc rekey time 3600
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn configuration mode to configure the SSL VPN context. |

# svc split

To enable split tunneling for Cisco AnyConnect VPN Client tunnel clients, use the **svc split** command in webvpn group policy configuration mode. To remove the split tunneling configuration from the policy group configuration, use the **no** form of this command.

**svc split** {**exclude** {*ip-address mask* | **local-lans**} | **include** *ip-address mask*}

**no svc split** {**exclude** {*ip-address mask* | **local-lans**} | **include** *ip-address mask*}

## Syntax Description

| | |
|---|---|
| **exclude** *ip-address mask* | The arguments are entered as a destination prefix. Traffic from the specified IP address and mask is not resolved through the Cisco AnyConnect VPN Client tunnel. |
| **exclude local-lans** | Permits remote users to access their local LANs. |
| **include** *ip-address mask* | The arguments are entered as a destination prefix. Traffic from the specified IP address and mask is resolved through the Cisco AnyConnect VPN Client tunnel. |

## Command Default

Split tunneling is not enabled for Cisco AnyConnect VPN Client tunnel clients.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Split tunnel support allows you to configure a policy that permits specific traffic to be carried outside the Cisco AnyConnect VPN Client tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the Internet service provider [ISP] or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the sametime. Entering the **local-lans** keyword permits the remote user to access resources on a local LAN, such as network printer.

**Note** SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example configures a list of IP addresses to be resolved over the tunnel (included) and a list to be resolved outside of the tunnel (excluded):

```
Router(config-webvpn-group)# svc split exclude 192.168.1.0 255.255.255.0
Router(config-webvpn-group)# svc split include 172.16.1.0 255.255.255.0
```

**Related Commands**

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn configuration mode to configure the SSL VPN context. |

# svc split dns

To configure the Secure Sockets Layers Virtual Private Network (SSL VPN) gateway to resolve the specified fully qualified Domain Name System (DNS) names through the Cisco AnyConnect VPN Client tunnel, use the **svc split dns** command in webvpn group policy configuration mode. To remove the split DNS statement from the policy group configuration, use the **no** form of this command.

**svc split dns** *name*

**no svc split dns** *name*

## Syntax Description

| | |
|---|---|
| **dns** *name* | The *name* argument is entered as a fully qualified DNS name. |

## Command Default

The SSL VPN gateway is not configured to resolve the specified fully qualified DNS names through the Cisco AnyConnect VPN Client tunnel.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Entering this command configures the SSL VPN gateway to resolve the specified DNS suffixes (domains) through the tunnel. The gateway automatically incudes the default domain into the list of domains that are resolved through the tunnel. Up to 10 DNS statements can be configured.

**Note** SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc split dns cisco.com
Router(config-webvpn-group)# svc split dns my.company.net
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# svc wins-server

To configure Windows Internet Name Service (WINS) servers for policy group end users, use the **svc wins-server** command in webvpn group policy configuration mode. To remove a WINS server from the policy group configuration, use the **no** form of this command.

**svc wins-server** {**primary** | **secondary**} *ip-address*

**no svc dns-server** {**primary** | **secondary**}

## Syntax Description

| | |
|---|---|
| **primary** \| **secondary** | Configures the primary or secondary WINS server. |
| *ip-address* | An IPv4 address is entered to identify the server. |

## Command Default

WINS servers are not configured for policy group end users.

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

**Note** SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example configures primary and secondary WINS servers for the policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc wins-server primary 172.31.1.1
Router(config-webvpn-group)# svc wins-server secondary 172.31.2.1
```

## Related Commands

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# text-color

**Note** Effective with Cisco IOS Release 12.4(6)T, the **text-color** command is not available in Cisco IOS software.

To set the color of the text on the title bars of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **text-color** command in Web VPN configuration mode. To revert to the default color, use the **no** form of this command.

**text-color** [**black** | **white**]

**no text-color** [**black** | **white**]

## Syntax Description

| | |
|---|---|
| **black** | (Optional) Color of the text is black. |
| **white** | (Optional) Color of the text is white. This is the default value. |

## Defaults

Color of the text is white.

## Command Modes

Web VPN configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(6)T | This command was removed. |

## Usage Guidelines

This command is limited to only two values to limit the number of icons that are on the toolbar.

## Examples

The following example shows that the text color will be black:

```
text-color black
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn** | Enters Web VPN configuration mode. |

# timeout (policy group)

To configure the length of time that an end user session can remain idle or the total length of time that the session can remain connected, use the **timeout** command in webvpn group policy configuration mode. To configure timeout timers to default values, use the **no** form of this command.

**timeout** {**idle** *seconds* | **session** *seconds*}

**no timeout** {**idle** | **session**}

## Syntax Description

| | |
|---|---|
| **idle** *seconds* | Configures the length time that an end user connection can remain idle. |
| **session** *seconds* | Configures the total length of time that an end user can maintain a single connection. |

## Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

**idle** 2100
**session** 43200

## Command Modes

Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

This command is used to configure the idle or session timer value. The idle timer sets the length of time that a session will remain connected when the end user generates no activity. The session timer sets the total length of time that a session will remain connected, with or without activity. Upon expiration of either timer, the end user connection is closed. The user must login or reauthenticate to access the Secure Sockets Layer Virtual Private Network (SSL VPN).

**Note** The idle timer is not the same as the dead peer timer. The dead peer timer is reset when any packet type is received over the Cisco AnyConnect VPN Client tunnel. The idle timer is reset only when the end user generates activity.

## Examples

The following example sets the idle timer to 30 minutes and session timer to 10 hours:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# timeout idle 1800
Router(config-webvpn-group)# timeout session 36000
```

**Related Commands**

| Command | Description |
|---|---|
| **policy group** | Enters webvpn group policy configuration mode to configure a policy group. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# time-range

To enable time-range configuration mode and define time ranges for functions (such as extended access lists), use the **time-range** command in global configuration or webvpn context configuration mode. To remove the time limitation, use the **no** form of this command.

**time-range** *time-range-name*

**no time-range** *time-range-name*

## Syntax Description

| | |
|---|---|
| *time-range-name* | Desired name for the time range. The name cannot contain either a space or quotation mark, and it must begin with a letter. |

## Command Default

None

## Command Modes

Global configuration
Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(1)T | This command was introduced. |
| 12.2(17a)SX | Support for this command was implemented on the Cisco 7600 series routers. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(11)T | This command was available in webvpn context configuration mode. |

## Usage Guidelines

The **time-range** entries are identified by a name, which is referred to by one or more other configuration commands. Multiple time ranges can occur in a single access list or other feature.

**Note** In Cisco IOS 12.2SX releases, IP and IPX-extended access lists are the only types of access lists that can use time ranges.

After the **time-range** command, use the **periodic** time-range configuration command, the **absolute** time-range configuration command, or some combination of them to define when the feature is in effect. Multiple **periodic** commands are allowed in a time range; only one **absolute** command is allowed.

**Tip** To avoid confusion, use different names for time ranges and named access lists.

## Examples

The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m. The example allows UDP traffic on Saturday and Sunday from noon to midnight only.

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
time-range udp-yes
 periodic weekend 12:00 to 24:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
 permit udp any any time-range udp-yes
!
interface ethernet 0
 ip access-group strict in
```

## Related Commands

| Command | Description |
|---|---|
| **absolute** | Specifies an absolute start and end time for a time range. |
| **ip access-list** | Defines an IP access list by name. |
| **periodic** | Specifies a recurring (weekly) start and end time for a time range. |
| **permit (IP)** | Sets conditions under which a packet passes a named IP access list. |

# title

To configure the HTML title string that is shown in the browser title and on the title bar of a Secure Sockets Layer Virtual Private Network (SSL VPN), use the **title** command in webvpn context configuration mode. To revert to the default text string, use the **no** form of this command.

**title** [*title-string*]

**no title** [*title-string*]

## Syntax Description

| | |
|---|---|
| *title-string* | (Optional) Title string, up to 255 characters in length, that is displayed in the browser of the user. The string value may contain 7-bit ASCII characters, HTML tags, and escape sequences. |

## Defaults

If this command is not configured or if the **no** form is entered, the following text is displayed:

"WebVPN Service"

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

The optional form of the **title** command is entered to configure a custom text string. If this command is issued without entering a text string, a title will not be displayed in the browser window. If the **no** form of this command is used, the default title string "WebVPN Service" is displayed.

## Examples

The following example configures "Secure Access: Unauthorized users prohibited" as the title string:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# title "Secure Access: Unauthorized users prohibited"
Router(config-webvpn-context)#
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# title-color

To specify the color of the title bars on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSL VPN), use the **title-color** command in webvpn context configuration mode. To remove the color, use the **no** form of this command.

**title-color** *color*

**no title-color** *color*

## Syntax Description

| | |
|---|---|
| *color* | The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a"#"), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation):<br>• \#/x{6}<br>• \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255)<br>• \w+<br>The default is purple. |

## Defaults

The color purple is used if this command is not configured or if the **no** form is entered.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |
| 12.4(6)T | Support for the SSL VPN enhancements feature was added. |

## Usage Guidelines

Configuring a new color overrides the color the preexisting color.

## Examples

The following examples show the three command forms that can be used to configure the title color:

```
Router(config-webvpn-context)# title-color darkseagreen
Router(config-webvpn-context)# title-color #8FBC8F
Router(config-webvpn-context)# title-color 143,188,143
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# url-list

To enter webvpn URL list configuration mode to configure a list of URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSL VPN) and to attach the URL list to a policy group, use the **url-list** command in webvpn context configuration and webvpn group policy configuration mode, respectively. To remove the URL list from the SSL VPN context configuration and from the policy group, use the **no** form of this command.

**url-list** *name*

**no url-list** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the URL list. The list name can up to 64 characters in length. |

## Command Default

Webvpn URL list configuration mode is not entered, and a list of URLs to which a user has access on the portal page of a SSL VPN website is not configured. If the command is not used to attach a URL list to a policy group, then a URL list is not attached to a group policy.

## Command Modes

Webvpn context configuration
Webvpn group policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

Entering this command places the router in SSL VPN URL list configuration mode. In this mode, the list of URLs is configured. A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual URL list configurations must have unique names.

## Examples

The following example creates a URL list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
```

The following example attaches a URL list to a policy group configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
Router(config-webvpn-url)# exit
```

```
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# url-list ACCESS
```

## Related Commands

| Command | Description |
|---|---|
| **heading** | Configures the heading that is displayed above URLs listed on the portal page of a SSL VPN website. |
| **policy group** | Attaches a URL list to policy group configuration. |
| **url-list** | Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website. |
| **url-text** | Adds an entry to a URL list. |
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# url-text

To add an entry to a URL list, use the **url-text** command in webvpn URL list configuration mode. To remove the entry from a URL list, use the **no** form of this command.

**url-text** {*name* **url-value** *url*}

**no url-text** {*name* **url-value** *url*}

## Syntax Description

| | |
|---|---|
| *name* | Text label for the URL. The label must be inside quotation marks if it contains spaces. |
| **url-value** *url* | An HTTP URL. |

## Command Default

An entry is not added to a URL list.

## Command Modes

Webvpn URL list configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com
Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
```

## Related Commands

| Command | Description |
|---|---|
| **url-list** | Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website. |

# user-profile location

To store user bookmarks in a directory on a device, use the **user-profile location** command in webvpn context configuration mode. To remove a directory that has been configured, use the **no** form of this command.

**user-profile location device:***directory*

**no user-profile location device:***directory*

## Syntax Description

| | |
|---|---|
| **device:** | Storage location on a device. See Table 1 for a list of acceptable storage locations. |
| *directory* | Name of the directory. |

## Command Default

The default location is flash:/webvpn/<context-name>/.

## Command Modes

Webvpn context configuration (config-webvpn-context)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |

## Usage Guidelines

Table 1 lists accept storage locations.

*Table 15 Type of Storage Location*

| Type of Storage Location | Description |
|---|---|
| **archive** | Archived file system. |
| **Bootflash** | Bootflash memory. |
| **disk0** | On Disk 0. |
| **disk1** | On Disk 1. |
| **Flash** | Flash memory. |
| **FTP** | FTP network server. |
| **HTTP** | HTTP file server. |
| **HTTPS** | HTTP secure server. |
| **null** | Null destination for copies. You can copy a remote file to null to determine its size. |
| **NVRAM** | Storage location is in NVRAM. |
| **PRAM** | Phase-change memory (PRAM)—type of nonvolatile computer memory. |

*Table 15 Type of Storage Location (continued)*

| Type of Storage Location | Description |
|---|---|
| **RCP** | Remote copy protocol network server. |
| **SCP** | Secure Copy—A means of securely transferring computer files between a local and a remote host or between two remote hosts using the Secure Shell (SSH) protocol. |
| **slot0** | On Slot 0. |
| **slot1** | On Slot 1. |
| **system** | System memory, including the running configuration. |
| **tmpsys** | Temporary system in a file system. |

## Examples

The following example shows bookmarks are stored in flash on the directory webvpn/sslvpn_context/.

```
Router# webvpn context context1
Router# user-profile location flash:/webvpn/sslvpn_context/
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Configures the SSL VPN context and enters webvpn context configuration mode. |

# vrfname

To associate a Virtual Private Network (VPN) front-door routing and forwarding instance (FVRF) with a SSL VPN gateway, use the **vrfname** command in webvpn gateway configuration mode. To disassociate the FVRF from the SSL VPN gateway, use the **no** form of this command.

**vrfname** *name*

**no vrfname** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the VRF. |

## Command Default

A VPN FVRF is not associated with a SSL VPN gateway.

## Command Modes

Webvpn gateway (config-webvpn-gateway)

## Command History

| Release | Modification |
|---|---|
| 12.4(15)T | This command was introduced. |

## Usage Guidelines

Only one FVRF can be associated with each SSL VPN context configuration.

## Examples

The following example shows FVRF has been configured:

```
Router (config) ip vrf vrf_1
Router (config-vrf) end
Router (config) webvpn gateway mygateway
Router (config-webvpn-gateway) vrfname vrf_1
Router (cofig-webvpn-gateway) end
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn gateway** | Enters webvpn gateway configuration mode to configure a SSL VPN gateway. |

# vrf-name

To associate a Virtual Private Network (VPN) routing and forwarding instance (VRF) with a SSL VPN context, use the **vrf-name** command in webvpn context configuration mode. To remove the VRF from the WebVPN context configuration, use the **no** form of this command.

**vrf-name** *name*

**no vrf-name**

## Syntax Description

| | |
|---|---|
| *name* | Name of the VRF. |

## Command Default

A VPN VRF is not associated with a SSL VPN context.

## Command Modes

Webvpn context configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The VRF is first defined in global configuration mode. Only one VRF can be associated with each SSL VPN context configuration.

## Examples

The following example associates a VRF with a SSL VPN context:

```
Router (config)# ip vrf BLUE
Router (config-vrf)# rd 10.100.100.1
Router (config-vrf)# webvpn context context1
Router (config-webvpn-context)# vrf-name BLUE
```

## Related Commands

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# web-agent-url

To configure the Netegrity agent URL to which Single SignOn (SSO) authentication requests will be dispatched, use the **web-agent-url** command in webvpn sso server configuration mode. To remove the Netegrity agent URL, use the **no** form of this command.

**web-agent-url** *url*

**no web-agent-url** *url*

## Syntax Description

| | |
|---|---|
| *url* | URL to which SSO authentication requests will be dispatched. |

## Command Default

Authentication requests will not be dispatched to a Netegrity agent URL.

## Command Modes

Webvpn sso server configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

**Note** A web agent URL and policy server secret key are required for a SSO server configuration. If they are not configured, a warning message is displayed. (See the warning message information in the Examples section below.)

## Examples

The following example shows that SSO authentication requests will be dispatched to the URL http://www.example.com/webvpn/:

```
webvpn context context1
 sso-server test-sso-server
  web-agent-url http://www.example.com/webvpn/
```

### Warning Message

If a web agent URL and policy server secret key are not configured, a message similar to the following is received:

```
Warning: must configure web agent URL for sso-server "example"
Warning: must configure SSO policy server secret key for sso-server "example"
Warning: invalid configuration. SSO for "example" being disabled
```

**Related Commands**

| Command | Description |
|---|---|
| **webvpn context** | Enters webvpn context configuration mode to configure the SSL VPN context. |

# webvpn context

To enter webvpn context configuration mode to configure the Secure Sockets Layer Virtual Private Network (SSL VPN) context, use the **webvpn context** command in global configuration mode. To remove the SSL VPN configuration from the router configuration file, use the **no** form of this command.

**webvpn context** *name*

**no webvpn context** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the SSL VPN context configuration. |

## Command Default

Webvpn context configuration mode is not entered, and a SSL VPN context is not configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The SSL VPN context defines the central configuration of the SSL VPN. Entering the **webvpn context** command places the router in webvpn context configuration mode.

**Note** The **ssl authenticate verify all** command is enabled by default when a context configuration is created. The context cannot be removed from the router configuration while a SSL VPN gateway is in an enabled state (in service).

## Examples

The following example configures and activates the SSL VPN context configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# inservice
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication (WebVPN)** | Configures AAA authentication for SSL VPN sessions. |
| **csd enable** | Enables CSD support for SSL VPN sessions. |
| **default-group-policy** | Specifies a default group policy for SSL VPN sessions. |
| **gateway (WebVPN)** | Specifies the gateway for SSL VPN sessions. |
| **inservice** | Enables a SSL VPN gateway or context process. |
| **login-message** | Configures a message for a user login text box on the login page. |

| Command | Description |
|---|---|
| **logo** | Configures a custom logo to be displayed on the login and portal pages of a SSL VPN website. |
| **max-users (WebVPN)** | Limits the number of connections to a SSL VPN that will be permitted |
| **nbns-list** | Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution. |
| **policy group** | Enters a webvpn group policy configuration mode to configure a group policy. |
| **port-forward** | Enters webvpn port-forward list configuration mode to configure a port-forwarding list. |
| **secondary-color** | Configures the color of the secondary title bars on the login and portal pages of a SSL VPN website. |
| **secondary-text-color** | Configures the color of the text on the secondary bars of a SSL VPN website. |
| **title** | Configures the HTML title string that is shown in the browser title and on the title bar of a SSL VPN website. |
| **title-color** | Configures the color of the title bars on the login and portal pages of a SSL VPN website. |
| **url-list** | Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website. |
| **vrf-name** | Associates a VRF with a SSL VPN context. |

# webvpn enable (Privileged EXEC)

To enable a Secure Socket Layer Virtual Private Network ( SSL VPN) gateway, use the **webvpn enable** command in privileged EXEC mode. This command has no **no** form.

**webvpn enable** *name gateway-IP-address* [*SSL-trustpoint-name*]

## Syntax Description

| | |
|---|---|
| *name* | Name of the SSL VPN gateway. |
| *gateway-IP-address* | IP address of the gateway. |
| *SSL-trustpoint-name* | Name of the SSL trustpoint. If not specified, a self-signed certificate is used for the gateway. |

## Command Default

A SSL VPN gateway is not enabled.

## Command Modes

Privileged EXEC mode

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

If you use this command, a generic SSL VPN gateway is generated.

## Examples

The following output is an example of a generic SSL VPN gateway that was enabled using the webvpn gateway command in privileged EXEC mode:

```
webvpn gateway SSL_gateway2
 ip address 10.1.1.1. port 442
 ssl trustpoint TP_self_signed _4138349635
 inservice
!
webvpn context SSL_gateway2
 ssl authenticate verify all
!
!
policy group default
default-group-policy default
 gateway SSL_gateway2
inservice
```

## Related Commands

| Command | Description |
|---|---|
| **tunnel protection** | Associates a tunnel interface with an IPsec profile. |
| **virtual interface** | Sets the zone name for the connected AppleTalk network. |
| **virtual template** | Specifies the destination for a tunnel interface. |

# webvpn gateway

To enter webvpn gateway configuration mode to configure a SSL VPN gateway, use the **webvpn gateway** command in global configuration mode. To remove the SSL VPN gateway from the router configuration file, use the **no** form of this command.

**webvpn gateway** *name*

**no webvpn gateway** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the virtual gateway service. |

## Command Default

Webvpn gateway configuration mode is not entered, and a SSL VPN gateway is not configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Entering the **webvpn gateway** command places the router in webvpn gateway configuration mode. Configuration settings specific to the SSL VPN gateway are entered in this configuration mode.

The SSL VPN gateway acts as a proxy for connections to protected resources. Protected resources are accessed through a secure encrypted connection between the gateway and a web-enabled browser on a remote device, such as a personal computer.

The gateway is configured using an IP address at which SSL VPN remote-user sessions terminate. The gateway is not active until the inservice command has been entered in SSL VPN gateway configuration mode. Only one gateway can be configured in a SSL VPN-enabled network.

## Examples

The following example creates and enables a SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# ip address 10.1.1.1 port 443
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN
Router(config-webvpn-gateway)# http-redirect 80
Router(config-webvpn-gateway)# inservice
```

## Related Commands

| Command | Description |
|---|---|
| **hostname (WebVPN)** | Configures a SSL VPN hostname. |
| **http-redirect** | Configures HTTP traffic to be carried over HTTPS. |
| **inservice** | Enables a SSL VPN gateway or context process. |
| **ip address (WebVPN)** | Configures a proxy IP address on a SSL VPN gateway. |

| Command | Description |
|---|---|
| **ssl encryption** | Configures the specify the encryption algorithms that the SSL protocol will use for an SSL VPN. |
| **ssl trustpoint** | Configures the certificate trust point on a SSL VPN gateway. |

# webvpn install

To install a Cisco Secure Desktop (CSD) or Cisco AnyConnect VPN Client package file to a SSL VPN gateway for distribution to end users, use the **webvpn install** command in global configuration mode. To remove a package file from the SSL VPN gateway, use the **no** form of this command.

**webvpn install** [**csd** *location-name* | **svc** *location-name*]

**no webvpn install** [**csd** *location-name* | **svc** *location-name*]

## Syntax Description

| | |
|---|---|
| **csd** *location-name* | (Optional) Installs the CSD client software package. The filename and path are entered. |
| **svc** *location-name* | (Optional) Installs the Cisco AnyConnect VPN Client software package. The filename and path are entered. |

## Command Default

A CSD or Cisco AnyConnect VPN Client package file is not installed to a WebVPN gateway.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The installation packages must first be copied to a local files system, such as flash memory. The CSD and Cisco AnyConnect VPN Client software packages are pushed to end users as access is needed. The end user must have administrative privileges, and the Java Runtime Environment (JRE) for Windows version 1.4 or later must be installed before a CSD or Cisco AnyConnect VPN Client package can be installed.

**Note** SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client is the predecessor of Cisco AnyConnect VPN Client software.

## Examples

The following example installs the Cisco AnyConnect VPN Client package to a SSL VPN gateway:

```
Router(config)# webvpn install svc flash:/webvpn/svc.pkg
SSLVPN Package SSL-VPN-Client : installed successfully
```

The following example installs the CSD package to a SSL VPN gateway:

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg
SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

# Feature Information for SSL VPN

Table 16 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

**Note** Table 16 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

*Table 16 Feature Information for SSL VPN*

| Feature Name | Release | Feature Information |
|---|---|---|
| SSL VPN | 12.4(6)T | This feature enhances SSL VPN support in Cisco IOS software. This feature provides a comprehensive solution that allows easy access to a broad range of web resources and web-enabled applications using native HTTP over SSL (HTTPS) browser support. SSL VPN introduced three modes of SSL VPN access: clientless, thin-client, and full-tunnel client support.<br>The following command was introduced in Cisco IOS Release 12.4(15)T: **cifs-url-list**. |
| Application ACL Support | 12.4(11)T | This feature provides administrators with the flexibility to fine tune access control on the Application Layer level.<br>The following sections provide information about this feature:<br>• Application ACL Support, page 10<br>• Configuring ACL Rules, page 63<br>• Associating an ACL Attribute with a Policy Group, page 66<br>• Configuring an ACL: Example, page 78<br>The following commands were introduced by this feature: **acl, add, error-msg, error-url**, and **list**. |

*Table 16 Feature Information for SSL VPN (continued)*

| | | |
|---|---|---|
| Auto Applet Download | 12.4(9)T | This feature provides administrators with the option of automatically downloading the port-forwarding applet under the policy group.<br><br>The following section provides information about this feature:<br><br>• Options for Configuring HTTP Proxy and the Portal Page, page 8<br><br>The following command was modified by this feature: **port-forward (policy group)** |
| Cisco AnyConnect VPN Client | 12.4(15)T | This feature is the next-generation SSL VPN Client. The feature provides remote users with secure VPN connections to the router platforms supported by SSL VPN and to the Cisco 5500 Series Adaptive Security Appliances.<br><br>Users having Cisco IOS software releases before Release 12.4(15)T see SSL VPN Client GUI. Users having Release 12.4(15)T and later releases see Cisco AnyConnect VPN Client GUI.<br><br>The task configurations in this document for tunnel mode apply to SVC and AnyConnect VPN Client.<br><br>For more information about the Cisco AnyConnect VPN Client feature, see the documents *Cisco AnyConnect VPN Client Administrator Guide* and *Release Notes for Cisco AnyConnect VPN Client, Version 2.0*.<br><br>**Note** Many of the features listed in the documents *Cisco AnyConnect VPN Client Administrator Guide* and *Release Notes for Cisco AnyConnect VPN Client, Version 2.0* apply only to the Cisco ASA 5500 Series Adaptive Security Appliances. For a list of features that do not currently apply to other Cisco platforms, see the restriction in the "Cisco AnyConnect VPN Client" section on page 3 of this document. |
| Debug Infrastructure | 12.4(11)T | Updates to the **webvpn debug** command provide administrators with the ability to turn debugging on for any one user or group.<br><br>The following keywords were introduced by this feature: **acl**, **entry**, **sso**, and **verbose**.<br><br>The following keyword options were added for the **http** keyword: **authentication**, **trace**, and **verbose**.<br><br>The **verbose** keyword option was added for the **citrix**, **cookie**, **tunnel**, and **webservice** keywords.<br><br>The **port-forward** keyword was deleted effective with this release, and the **detail** keyword option for the **tunnel** keyword was deleted. |

*Table 16 Feature Information for SSL VPN (continued)*

| | | |
|---|---|---|
| Front-Door VRF Support | 12.4(15)T | Coupled with the already supported internal VRF, this feature allows the SSL VPN gateway to be fully integrated into an MPLS network.<br>The following sections provide information about this feature:<br>• Front-Door VRF Support, page 10<br>• Configuring FVRF, page 73 |
| GUI Enhancements | 12.4(15)T | These enhancements provide updated examples and explanation of the Web VPN GUIs.<br>The following section provides information about these updates:<br>• GUI Enhancements, page 11 |
| Netegrity Cookie-Based Single SignOn (SSO) Support | 12.4(11)T | This feature allows administrators to configure a SSO server that sets a SiteMinder cookie in the browser of a user when the user initially logs on. The benefit of this feature is that users are prompted to log on only a single time<br>The following sections provide information about this feature:<br>• Netegrity Cookie-Based Single SignOn Support, page 16<br>• Configuring SSO Netegrity Cookie Support for a Virtual Context, page 67<br>• Associating an SSO Server with a Policy Group, page 69<br>The following commands were modified for this feature: **clear webvpn stats, debug webvpn, show webvpn policy, show webvpn context**, and **show webvpn stats**.<br>The following commands were added for this feature: **max-retry-attempts, request-timeout, secret-key, sso-server**, and **web-agent-url**. |
| NTLM Authentication | 12.4(9)T | This feature provides NT LAN Manager (NTLM) authentication support.<br>The following section provides information about this feature:<br>• NTLM Authentication, page 17<br>The following command was modified by this feature: **functions** |

*Table 16 Feature Information for SSL VPN (continued)*

| | | |
|---|---|---|
| Port-Forward Enhancements | 12.4(11)T | This feature provides administrators with more options for configuring HTTP proxy and portal pages.<br>The following section provides information about this feature:<br>• Options for Configuring HTTP Proxy and the Portal Page, page 8<br>The following commands were added for this feature: **acl, add, deny, error-msg, error-url, list**, and **permit**. |
| RADIUS Accounting | 12.4(9)T | This feature provides for RADIUS accounting for SSL VPN sessions.<br>The following sections provide information about this feature:<br>• RADIUS Accounting, page 17<br>• Configuring RADIUS Accounting for SSL VPN User Sessions, page 37<br>• RADIUS Accounting for SSL VPN Sessions: Example, page 79<br>The following command was added by this feature: **webvpn aaa accounting-list** |
| URL Obfuscation | 12.4(11)T | This feature provides administrators with the ability to obfuscate, or mask, sensitive portions of an enterprise URL, such as IP addresses, hostnames, or port numbers.<br>The following sections provide information about this feature:<br>• URL Obfuscation, page 19<br>• Configuring URL Obfuscation (Masking), page 69<br>• URL Obfuscation (Masking): Example, page 80<br>The following command was added by this feature: **mask-urls** |
| User-Level Bookmarking | 12.4(15)T | This feature allows a user to bookmark URLs while connected through an SSL VPN tunnel.<br>The following sections provide information about this feature:<br>• User-Level Bookmarking, page 19<br>• Configuring User-Level Bookmarks, page 72<br>The following command was added by this feature: **user-profile location** |

# Notices

The following notices pertain to this software license.

# OpenSSL/Open SSL Project

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

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

## License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

**OpenSSL License:**

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

**Original SSLeay License:**



This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].