



## Configuring Web Security

---

The AnyConnect Web Security module is an endpoint component that routes HTTP traffic to a Cisco Cloud Web Security scanning proxy where Cisco Cloud Web Security evaluates it.

Cisco Cloud Web Security deconstructs the elements of a Web page so that it can analyze each element simultaneously. For example, if a particular Web page combined HTTP, Flash, and Java elements, separate “scanlets” analyze each of these elements in parallel. Cisco Cloud Web Security then lets through benign or acceptable content and drops malicious or unacceptable content based on a security policy defined in the Cisco ScanCenter management portal. This prevents “over blocking” where an entire Web page is restricted because a minority of the content is unacceptable or “under blocking” where an entire page is permitted while there is still some unacceptable or possibly harmful content that is being delivered with the page. Cisco Cloud Web Security protects users when they are on or off the corporate network.

With many Cisco Cloud Web Security scanning proxies spread around the world, users taking advantage of AnyConnect Web Security are able to route their traffic to the Cisco Cloud Web Security scanning proxy with the fastest response time to minimize latency.

You can configure the Secure Trusted Network Detection feature to identify endpoints that are on the corporate LAN. If this feature is enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than Cisco Cloud Web Security.

AnyConnect Web Security features and functions are configured using the AnyConnect Web Security client profile which you edit using AnyConnect’s profile editor.

Cisco ScanCenter is the management portal for Cisco Cloud Web Security. Some of the components created or configured using Cisco ScanCenter are also incorporated in the AnyConnect Web Security client profile.

The following sections describe the AnyConnect Web Security client profile and features, and how to configure them:

- [System Requirements](#)
- [Licensing Requirements](#)
- [Installing the AnyConnect Web Security Module for Use with an ASA](#)
- [Installing the AnyConnect Web Security Module for Use without an ASA](#)
- [Creating an AnyConnect Web Security Client Profile](#)
- [Configuring Cisco Cloud Web Security Scanning Proxies in the Client Profile](#)
- [Excluding Endpoint Traffic from Web Scanning Service](#)
- [Configuring Web Scanning Service Preferences](#)

- [Configuring Authentication and Sending Group Memberships to the Cisco Cloud Web Security Proxy](#)
- [Web Security Client Profile Files](#)
- [Creating a Web Security Client Profile with the Standalone Editor](#)
- [Configuring Split Exclusion Policy for Web Security](#)
- [Configuring Cisco ScanCenter Hosted Configuration Support for Web Security Client Profile](#)
- [Switching off and Enabling the Cisco AnyConnect Web Security Agent](#)

You can begin configuring AnyConnect Web Security by [Creating an AnyConnect Web Security Client Profile](#).

## System Requirements

These are the system requirements for AnyConnect Web Security Module:

- [AnyConnect Web Security Module](#)
- [ASA and ASDM Requirements](#)

## AnyConnect Web Security Module

Web Security supports the following operating systems:

- Windows XP SP3 x86 (32-bit)
- Windows Vista x86 (32-bit) or x64 (64-bit)
- Windows 7 x86 (32-bit) or x64 (64-bit)
- Mac OS X v10.6 x86 (32-bit) or x64 (64-bit)
- Mac OS X v10.7 x86 (32-bit) or x64 (64-bit)
- Mac OS X v10.8 x64 (64-bit)

## ASA and ASDM Requirements

The AnyConnect Secure Mobility Client with the Web security module requires these minimum ASA components:

- ASA 8.4(1)
- ASDM 6.4(0)104

## System Limitations

Users running Web Security cannot also run Anywhere Plus. You will need to remove Anywhere Plus before installing Web Security.

# Licensing Requirements

These sections describe the licensing requirements for different deployment methods of the AnyConnect Web Security Module:

- [Web Security Deployed as a Standalone Component, page 6-3](#)
- [Web Security Deployed as a Component of AnyConnect, page 6-3](#)

## Web Security Deployed as a Standalone Component

You can deploy the Web Security module and benefit from Cisco Cloud Web Security without having to install an ASA and without enabling the VPN capabilities of the AnyConnect Secure Mobility Client.

However, you will need a Cisco Cloud Web Security license and a Cisco Cloud Web Security Secure Mobility license for roaming users deploying AnyConnect.

**Note**

You do not need an AnyConnect Essentials or AnyConnect Premium license to use the AnyConnect Secure Mobility Client with only the Web Security module.

## Web Security Deployed as a Component of AnyConnect

**AnyConnect License**

There are no AnyConnect licenses specific to Web Security. The Web Security module will work with either AnyConnect Essentials or AnyConnect Premium.

**Cisco Cloud Web Security Licenses**

You need a Secure Mobility for Cisco Cloud Web Security license in addition to Cisco Cloud Web Security Web Filtering and/or Cisco Cloud Web Security Malware Scanning licenses in order for roaming users to be protected by Cisco Cloud Web Security.

## User Guideline for Web Security Behavior with IPv6 Web Traffic

Unless an exception for an IPv6 address, domain name, address range, or wildcard is specified, IPv6 web traffic will be sent to the scanning proxy where it will perform a DNS lookup to see if there is an IPv4 address for the URL the user is trying to reach. If the scanning proxy finds an IPv4 address, it will use that for the connection. If it does not find an IPv4 address, the connection will be dropped.

If you want all IPv6 traffic to bypass the scanning proxies, you can add this static exception for all IPv6 traffic `::/0`. This means that IPv6 traffic will not be protected by Web Security.

## Installing the AnyConnect Web Security Module for Use with an ASA

The Web Security module requires a client profile when deployed with AnyConnect or when deployed as a standalone module.

- 
- Step 1** Create a Web Security client profile by following the [“Creating an AnyConnect Web Security Client Profile”](#) section on page 6-7 procedure.
- Step 2** Read [Chapter 2, “Deploying the AnyConnect Secure Mobility Client”](#) for instructions on installing the Web Security module using web-deployment and pre-deployment methods.
- 

## Installing the AnyConnect Web Security Module for Use without an ASA

You can deploy the Web Security module as a standalone application to use with Cisco Cloud Web Security without enabling the AnyConnect VPN module and without an ASA. This section includes the following information:

- [Installing the Web Security Module on Windows Using the AnyConnect Installer](#)
- [Installing the Web Security Module on Mac OS X Using the AnyConnect Installer](#)



### Note

On computers running Windows, if AnyConnect cannot determine the user ID, the internal IP address will be used as the user ID. For example, this could happen if the enterprise\_domains profile entry is not specified. You would then need to use the internal IP address for the purpose of generating reports in Cisco ScanCenter.

On computers running Mac OS X, the Web Security module can report the domain the computer is logged into if the Mac is bound to a domain. If it is not bound to a domain, the Web Security Module can report the IP address of the Mac or the username that is currently logged in.

---

## Installing the Web Security Module on Windows Using the AnyConnect Installer

This procedure explains how to configure the Cisco AnyConnect Secure Mobility Client Web Security module on Windows for use with Cisco Cloud Web Security. In general terms, these are the tasks you will perform:





### Note

Refer to chapter 2 for general installation instructions including the enabling of Windows lockdown.

---

1. Download the Cisco AnyConnect Secure Mobility Client ISO image.
2. Extract the contents of the ISO file.
3. Customize the Web Security Module by installing the Standalone Profile Editor, creating a Web Security profile, and by adding the Web Security profile file to the extracted contents of the ISO file.
4. Install the customized Web Security module.

To configure the Cisco AnyConnect Secure Mobility Client Web Security module on Windows for use with Cisco Cloud Web Security, follow this procedure.

- 
- Step 1** Download the Cisco AnyConnect Secure Mobility Client package from the Cisco ScanCenter support area or from Cisco.com.
- Step 2** Create a new directory.
- Step 3** Using an application like WinZip or 7-Zip, extract the contents of the ISO file to the newly created directory.
-  **Note** Do **not** install the Web Security module at this point.
- 
- Step 4** Install the Standalone AnyConnect Profile Editor. For further information, see the [“Installing the Standalone AnyConnect Profile Editor”](#) section on page 2-35.
-  **Note** The Web Security profile editor component is not installed by default. You must select it as part of a Custom installation, or select a Complete installation.
- 
- Step 5** Start the Web Security profile editor and create a profile by following the [“Creating an AnyConnect Web Security Client Profile”](#) section on page 6-7.
- Step 6** Save the profile as **WebSecurity\_ServiceProfile.xml** in a secure location.
- The Web Security profile editor creates an additional obfuscated version of the profile called **WebSecurity\_ServiceProfile.wso** and saves it to the same location as you saved the WebSecurity\_ServiceProfile.xml file.
- Step 7** Copy the obfuscated version of the Web Security profile, called WebSecurity\_ServiceProfile.wso to the **Profiles\websecurity** folder you extracted in [Step 3](#).
- Step 8** Start **Setup.exe** to install the client software.
- Step 9** In the Cisco AnyConnect Secure Mobility Client Install Selector:
- Ensure the **AnyConnect Web Security Module** check box is selected.
  - Ensure the **Cisco AnyConnect VPN Module** is cleared. Doing so switches off the VPN functionality of the core client, and the Install Utility installs the Network Access Manager and Web Security as standalone applications with no VPN functionality.
  - (Optional) Select the **Lock Down Component Services** check box. The lock down component service prevents users from switch off or stopping the Windows Web Security service.
- Step 10** Click **Install Selected** and then click **OK**. When the installation has successfully completed, you will see the Cisco AnyConnect Secure Mobility Client icon in your system tray.
- 

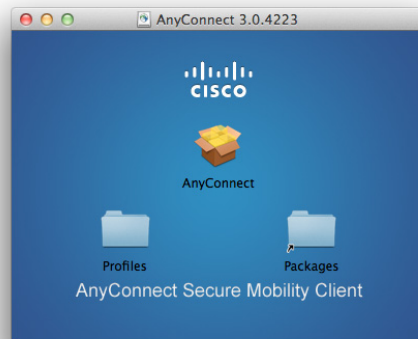
## Installing the Web Security Module on Mac OS X Using the AnyConnect Installer

The following procedure explains how to customize the Web Security Module by installing the Standalone Profile Editor, creating a Web Security profile, and adding that Web Security profile to the DMG package.

- 
- Step 1** Download the Cisco AnyConnect Secure Mobility Client DMG package from the Cisco ScanCenter support area or from the download area of Cisco.com.

- Step 2** Open the file to access the installer (Figure 6-1). The downloaded image is a read only file.

**Figure 6-1** AnyConnect Installer Image



- Step 3** Make the installer image writable by either running the **Disk Utility** or using the **Terminal** application, as follows:

```
Hdiutil convert <source dmg> -format UDRW -o <output dmg>
```

- Step 4** Install the Standalone AnyConnect Profile Editor on a computer running a Windows operating system. For further information, see the [“Installing the Standalone AnyConnect Profile Editor”](#) section on page 2-35.



**Note** The Web Security profile editor component is not installed by default. You must select it as part of a Custom installation, or select a Complete installation.

- Step 5** Start the Web Security profile editor and create a profile by following the [“Creating an AnyConnect Web Security Client Profile”](#) section on page 6-7.

- Step 6** Save the profile as **WebSecurity\_ServiceProfile.xml** in a secure location.

The Web Security profile editor creates an additional obfuscated version of the profile called **WebSecurity\_ServiceProfile.wso** and saves it to the same location as you saved the **WebSecurity\_ServiceProfile.xml** file.

- Step 7** Copy the **WebSecurity\_ServiceProfile.wso** file from the Windows machine to the **AnyConnect 3.x.xxxxx/Profiles/websecurity** Mac OS X installer package.

Alternatively you can also use the **Terminal** application, as follows:

```
Copy WebSecurity_ServiceProfile.wso
cp <path to the wso> \Volumes\AnyConnect <VERSION>\Profiles\websecurity\
```

- Step 8** In the Mac OS X installer, go to the **AnyConnect 3.x.xxxxx/Profiles** directory and open the **ACTransforms.xml** file in TextEdit to edit the file. Set the **<DisableVPN>** element to **True** ensure the VPN functionality is not installed:

```
<ACTransforms>
  <DisableVPN>True</DisableVPN>
</ACTransforms>
```

- Step 9** In the Download area for AnyConnect Secure Mobility Client **3.x.xxxxx** on Cisco.com, find the **VPNDisable\_ServiceProfile.xml** file and download it to the computer on which you are going to install AnyConnect Web Security.

- Step 10** Save the **VPNDisable\_ServiceProfile.xml** file to the **AnyConnect 3.x.xxxxx/profiles/vpn** directory of the AnyConnect installer.



**Note** When installing the Web Security module only for AnyConnect 3.x.xxxxx on Mac OS X, the AnyConnect user interface should be set to start automatically on boot-up. This enables AnyConnect to provide the necessary user and group information for the Web Security module. Steps 9 and 10 provide the proper configuration to allow the AnyConnect user interface to start automatically on boot up.

- Step 11** The AnyConnect DMG package is now ready to distribute to your users.

## Installing the Web Security Module on Windows Using the Command Line Installation

To install the Web Security module from the command prompt, follow this procedure:

- Step 1** Follow [Step 1 - Step 6](#) in [Installing the Web Security Module on Windows Using the AnyConnect Installer](#).
- Step 2** Install the AnyConnect Secure Mobility Client VPN module with VPN functionality switched off:
- ```
msiexec /package anyconnect-win-<version>-pre-deploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* c:\test.log
```
- Step 3** Install the Web Security Module.
- ```
msiexec /package anyconnect-websecurity-win-<version>-pre-deploy-k9.msi /norestart
/passive /lvx* c:\test.log
```
- Step 4** (Optional) Install DART.
- ```
msiexec /package annyconnect-dart-win-<version>-k9.msi /norestart /passive /lvx*
c:\test.log
```
- Step 5** Save a copy of the obfuscated Web Security client profile to the proper Windows folder as defined in [Table 2-12 on page 2-33](#).
- Step 6** Restart the Cisco AnyConnect Web Security Agent windows service using the [“Switching off and Enabling the Cisco AnyConnect Web Security Agent” section on page 6-28](#).



**Note** These commands can also be used for Systems Management Server (SMS) deployment.

## Creating an AnyConnect Web Security Client Profile

To create an AnyConnect Web Security client profile, follow this procedure:

- Step 1** Start the Web Security Profile Editor using one of these methods:

- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**, and click **Add** to create a client profile.
- In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.

- Step 2** If you are using the standalone profile editor, give the client profile a **name**.
- Step 3** Click the **Profile Usage** field, and select **Web Security**.
- Step 4** Accept the default Profile Location or click **Browse** to specify an alternate file location.
- Step 5** (Optional) Select a **Group Policy** to attach the client profile or leave the client profile <Unassigned>.
- Step 6** Save the AnyConnect Web Security client profile.
- 

When you have created the AnyConnect Web Security client profile, you will need to configure these aspects of the profile:

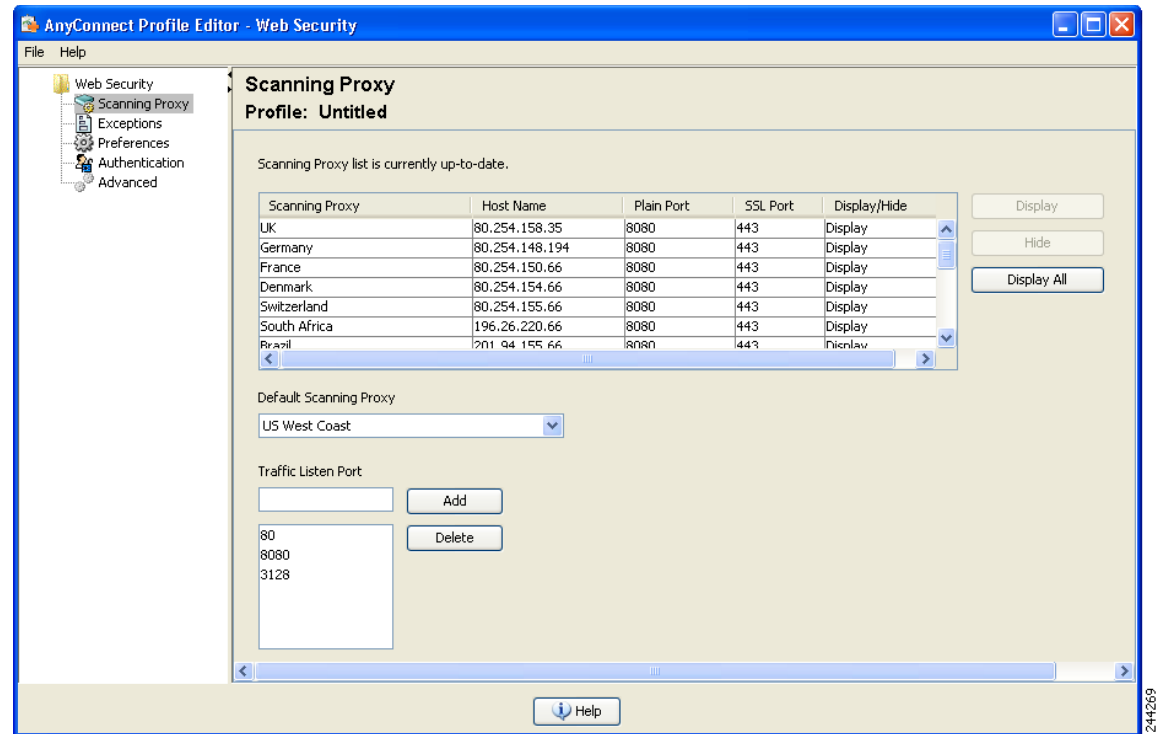
- [Configuring Cisco Cloud Web Security Scanning Proxies in the Client Profile, page 6-8](#)
- [Excluding Endpoint Traffic from Web Scanning Service, page 6-12](#)
- [Configuring User Controls and Calculating Fastest Scanning Proxy Response Time, page 6-15](#)
- [Configuring Secure Trusted Network Detection, page 6-16](#)
- [Configuring Authentication and Sending Group Memberships to the Cisco Cloud Web Security Proxy, page 6-17](#)

After you create and save the AnyConnect Web Security client profile, ASDM makes two copies of the XML file; one file is obfuscated and the other is in plain text. To learn more about these files see the [“Web Security Client Profile Files” section on page 6-23](#).

## Configuring Cisco Cloud Web Security Scanning Proxies in the Client Profile

Cisco Cloud Web Security analyzes Web content; it allows benign content to be delivered to your browser and blocks malicious content based on a security policy. A scanning proxy is a Cisco Cloud Web Security proxy server on which Cisco Cloud Web Security analyzes the Web content. The Scanning Proxy panel in the AnyConnect Web Security profile editor defines to which Cisco Cloud Web Security scanning proxies the AnyConnect Web Security module sends Web network traffic.



**Figure 6-2 Web Security Client Profile Scanning Proxy Panel**

Use these procedures to define Cisco Cloud Web Security scanning proxies in an AnyConnect Web Security client profile:

- [Creating an AnyConnect Web Security Client Profile, page 6-7](#)
- [Displaying or Hiding Scanning Proxies from Users, page 6-10](#)
- [Selecting a Default Scanning Proxy, page 6-11](#)
- [Specifying an HTTP\(S\) Traffic Listening Port, page 6-12](#)

## Updating the Scanning Proxy List

The Scanning Proxy list in the Web Security profile editor is not editable. You cannot add or remove Cisco Cloud Web Security scanning proxies from the table in the Web Security profile editor.

After you start the Web Security profile editor, it updates the scanning proxy list automatically by contacting a Cisco Cloud Web Security website, which maintains the current list of scanning proxies.

When you add or edit an AnyConnect Web Security client profile, the profile editor compares the existing list of Cisco Cloud Web Security scanning proxies to those in the scanning proxy list it downloaded from the <http://www.scansafe.cisco.com/> website. If the list is out of date, you see a message saying “Scanning Proxy list is out of date” and a command button labeled Update List. Click the **Update List** button to update the scanning proxy list with the most recent list of Cisco Cloud Web Security scanning proxies.

When you click **Update List**, the profile editor takes care to maintain as much of your existing configuration as possible. Profile editor preserves your default scanning proxy setting and the display/hide settings for the existing Cisco Cloud Web Security scanning proxies.

## Default Scanning Proxy Settings in a Web Security Client Profile

By default, the profile you create has these Cisco Cloud Web Security scanning proxy attributes:

- The scanning proxy list is populated with all the Cisco Cloud Web Security scanning proxies your users have access to and they are all marked “Display.” See the [“Displaying or Hiding Scanning Proxies from Users” section on page 6-10](#) for more information.
- A default Cisco Cloud Web Security scanning proxy is pre-selected. To configure the default Cisco Cloud Web Security scanning proxy see the [“Selecting a Default Scanning Proxy” section on page 6-11](#).
- The list of ports on which the AnyConnect Web Security module listens for HTTP traffic is provisioned with several ports. See the [“Specifying an HTTP\(S\) Traffic Listening Port” section on page 6-12](#) for more information.

## Displaying or Hiding Scanning Proxies from Users

After users establish a VPN connection to the ASA, the ASA downloads a client profile to the endpoint. The AnyConnect Web Security client profile determines which Cisco Cloud Web Security scanning proxies are displayed to users.

Users interact with the scanning proxies marked “Display” in the scanning proxy list of the AnyConnect Web Security client profile in these ways:

- The Cisco Cloud Web Security scanning proxies are displayed to users in the Advanced settings of the Web Security panel of their Cisco AnyConnect Secure Mobility Client interface.
- The AnyConnect Web Security module tests Cisco Cloud Web Security scanning proxies marked “Display” when ordering scanning proxies by response time.
- Users can choose which Cisco Cloud Web Security scanning proxy they connect to if their profile allows for user control.
- Cisco Cloud Web Security scanning proxies marked “Hide” in the scanning proxy table of the AnyConnect Web Security client profile are not displayed to users or evaluated when ordering scanning proxies by response time. Users cannot connect to the scanning proxies marked “Hide.”

**Note**

For the maximum benefit to roaming users, we recommend you “Display” all Cisco Cloud Web Security scanning proxies to all users.

To hide or display Cisco Cloud Web Security scanning proxies to users, follow this procedure:

- 
- Step 1** Start the Web Security Profile Editor using one of these methods:
- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
  - In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile you wish to edit.
- Step 3** To hide or display Cisco Cloud Web Security scanning proxies:
- **To hide a scanning proxy**, select the scanning proxy you want to hide and click **Hide**.

- **To display a scanning proxy**, select the name of scanning proxy you want to display and click **Display**. Displaying all Cisco Cloud Web Security scanning proxies is the recommended configuration.

**Step 4** Save the AnyConnect Web Security client profile.

---

## Selecting a Default Scanning Proxy

To define a default Cisco Cloud Web Security scanning proxy, follow this procedure:

- 
- Step 1** Start the Web Security Profile Editor using one of these methods:
- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
  - In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile you wish to edit.
- Step 3** Select a default scanning proxy from the **Default Scanning Proxy** field.
- Step 4** Save the AnyConnect Web Security client profile.
- 

## How Users Get Connected to Scanning Proxies

1. When users first connect to the network, they are routed to their default scanning proxy.
2. After that, depending on how their profile is configured, users may choose a scanning proxy or the AnyConnect Web Security module connects them to the scanning proxy with the fastest response time.
  - If their client profile allows user control, users will be able to select a scanning proxy from the Settings tab for the Cisco AnyConnect Secure Mobility Client Web Security tray.
  - If their client profile has the Automatic Scanning Proxy Selection preference enabled, AnyConnect Web Security orders the scanning proxies from fastest to slowest and connects users to the scanning proxy with the fastest response time.
  - If their client profile does not allow for user control but **Automatic Scanning Proxy Selection** is enabled, AnyConnect Web Security will switch users from their default scanning proxy to the scanning proxy with the fastest response time, provided that the response time is significantly faster than the default scanning proxy to which they originally connected.
  - If users start to roam away from their current scanning proxy and **Automatic Scanning Proxy Selection** is configured in their client profile, AnyConnect Web Security could switch users to a new scanning proxy, provided that its response time is significantly faster than their current scanning proxy.

Users will know what scanning proxy they are connected to because AnyConnect Web Security displays the enabled scanning proxy name in the expanded AnyConnect tray icon on Windows, the Advanced Settings tab, and the Advanced Statistics tab of the AnyConnect GUI.

## Specifying an HTTP(S) Traffic Listening Port

The Scan Safe web scanning service analyzes HTTP Web traffic by default and can be configured to filter HTTPS Web traffic. In the Web Security client profile, you can specify the ports on which you want Web Security to “listen” for these types of network traffic.

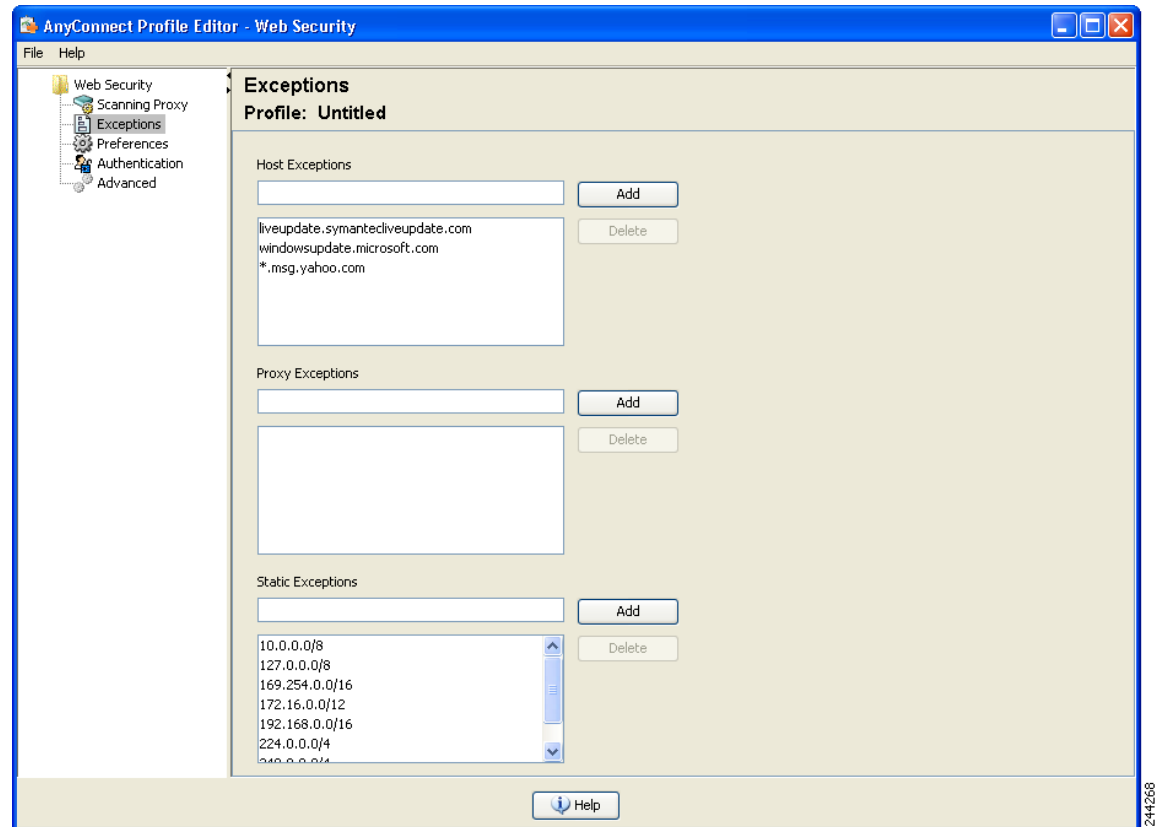
- 
- Step 1** Start the Web Security Profile Editor using one of these methods:
- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
  - In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile you wish to edit.
- Step 3** In the **Traffic Listen Port** field, enter the logical port number you want Web Security module to “listen” to for HTTP or HTTPS traffic or both.
- Step 4** Save the Web Security client profile.
- 

## Excluding Endpoint Traffic from Web Scanning Service

If you do not want network traffic, originating from a particular IP address, to be evaluated by Cisco Cloud Web Security, you can configure an exception for that address in one of these categories:

- [Host Exceptions](#)
- [Proxy Exceptions](#)
- [Static Exceptions](#)

These exclusions are configured in the Exceptions panel of the Web Security profile editor. See [Figure 6-3](#).

**Figure 6-3 Web Security Profile Editor Exceptions Panel**

## Host Exceptions

In the Host Exceptions list, add internal subnets and any public websites you want to bypass the Cisco Cloud Web Security.



### Note

Host exceptions for HTTPS must be in IP format. Host names will not work because in HTTPS communications the host name is encrypted.

See [Figure 6-3](#) for a picture of the Exceptions panel.

You should add any internal subnets you use that are not already included in the default, for example:

```
192.0.2.0/8
```

You should also add any internal or external websites for which you want to enable direct access. For example:

```
update.microsoft.com
*.salesforce.com
*.mycompanydomain.com
```

Also, you must add any public IP addresses you use for intranet services; otherwise, you will not be able to access those intranet servers through Web Security.

You can enter subnets and IP addresses using this syntax:

| Syntax                                                    | Example                                                                                                                                     |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Individual IPv4 and IPv6 addresses                        | 80.254.145.118<br>2001:0000:0234:C1AB:0000:00A0:AABC:003F                                                                                   |
| Classless Inter-Domain Routing (CIDR) notation            | 10.0.0.0/8<br>2001:DB8::/48                                                                                                                 |
| Fully Qualified Domain Names                              | windowsupdate.microsoft.com<br>ipv6.google.com<br><b>Note</b> Partial domains are not supported; for example, example.com is not supported. |
| Wildcards in fully qualified domain names or IP addresses | 127.0.0.*<br>*.cisco.com                                                                                                                    |



**Caution**

Do not use wildcards on both sides of a top level domain, for example \*.cisco.\*, as this could include phishing sites.



**Caution**

Do not delete or change any of the default host exception entries.

## Proxy Exceptions

In the Proxy Exceptions area, enter the IP addresses of authorized internal proxies. For example: 192.168.2.250. See [Figure 6-3](#) for a picture of the Exceptions panel.

You can specify IPv4 and IPv6 addresses in the field, but you cannot specify a port number with them. You cannot specify IP addresses using CIDR notation.

Specifying IP addresses prevents Cisco Cloud Web Security from intercepting Web data bound for these servers and tunneling the data through them using SSL. This allows proxy servers to operate without disruption. If you do not add your proxy servers here, they will see Cisco Cloud Web Security traffic as SSL tunnels.

For proxies not on this list, Web Security attempts to tunnel through them using SSL, so if your users are at a different company site that requires a proxy to get out of the network for Internet access, Cisco Cloud Web Security will provide the same level of support as if they were on an open Internet connection.

## Static Exceptions

Add a list of individual IP addresses or IP address ranges in Classless Inter-Domain Routing (CIDR) notation for which traffic should bypass Cisco Cloud Web Security. In the list, include the ingress IP addresses of your VPN gateways. See [Figure 6-3](#).

Private IP addresses described in [RFC 1918](#) are included in the static exception list by default.

**Note**

If you have a Proxy Server that has an IP address in one of the ranges that appear in the static exception list, then you must move that exception to the host exception list. For example, 10.0.0.0/8 appears in the static exception list. If you have a proxy at 10.1.2.3 then you must move 10.0.0.0/8 to the host exception list, otherwise traffic sent to this proxy will bypass Cloud Web Security.

You can specify IPv4 and IPv6 addresses or ranges of addresses using CIDR notation. You cannot specify fully qualified domain names or use wildcards in IP addresses. These are examples of correct syntax:

```
10.10.10.5
192.0.2.0/24
```

**Note**

Make sure to add the IP addresses of your SSL VPN concentrators to the static exclusion list.

### User Guideline for IPv6 Web Traffic

Unless an exception for an IPv6 address, domain name, address range, or wildcard is specified, IPv6 web traffic will be sent to the scanning proxy where it will perform a DNS lookup to see if there is an IPv4 address for the URL the user is trying to reach. If the scanning proxy finds an IPv4 address, it will use that for the connection. If it does not find an IPv4 address, the connection will be dropped.

If you want all IPv6 traffic to bypass the scanning proxies, you can add this static exception for all IPv6 traffic `::/0`. Doing this will make all IPv6 traffic bypass all scanning proxies. This means that IPv6 traffic will not be protected by Web Security.

## Configuring Web Scanning Service Preferences

Use this panel to configure these preferences:

- [Configuring User Controls and Calculating Fastest Scanning Proxy Response Time, page 6-15](#)
- [Configuring Secure Trusted Network Detection, page 6-16](#)

### Configuring User Controls and Calculating Fastest Scanning Proxy Response Time

To allow users to choose the Cisco Cloud Web Security scanning proxy they connect to, follow this procedure:

- 
- Step 1** Start the Web Security Profile Editor using one of these methods:
- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
  - In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile you wish to edit.
- Step 3** Click **Preferences**.
- Step 4** Select **User Controllable**. (This is the default setting.) User Controllable determines if the User is allowed to change the Automatic Tower Selection and Order Scanning Proxies by Response Time settings in the AnyConnect interface.

**Step 5** Select **Enable Cloud-Hosted Configuration** to enable updating the profile via Cisco ScanCenter. For further information see the [ScanCenter Administrator Guide, Release 5.2](#).

**Step 6** If you would like Web Security to automatically select a scanning proxy, select **Automatic Scanning Proxy Selection**. If you do this, **Order Scanning Proxies by Response Time** is selected automatically.

- If you select **Automatic Scanning Proxy Selection**, Web Security determines which scanning proxy has the fastest response time and automatically connects the user to that scanning proxy.
- If you do not select **Automatic Scanning Proxy Selection**, and you still have **Order Scanning Proxies by Response Time** selected, users will be presented with a list of scanning proxies, to which they can connect, ordered from fastest to slowest response time.
- If you do not select **Automatic Scanning Proxy Selection**, the user is still free to enable this feature from the AnyConnect user interface, but once enabled they will not be able to switch it off again.

**Note**

When you enable Automatic Scanning Proxy Selection, transient communications interruptions and failures can cause the active scanning proxy selection to change automatically. Changing the scanning proxy can sometimes be undesirable, as it can cause unexpected behavior such as returning search results from a scanning proxy in a different country using a different language.

**Step 7** If you selected **Order Scanning Proxies by Response Time**, configure these settings for calculating which scanning proxy has the fastest response time.

- **Test Interval:** The time, in minutes, between running each performance test, two minutes by default. You can switch off the test interval to prevent the test from running by clearing the **Enable Test Interval** check box.
- **Test Inactivity Timeout:** The time, in minutes, after which Web Security suspends the response time test because of user inactivity. Web Security resumes the testing as soon as scanning proxies encounter connection attempts. You should not change this setting unless instructed to do so by customer support.

**Note**

The **Ordering Scanning Proxies by Response Time** test runs continuously, based on the Test Interval time, with these exceptions:

- Secure Trusted Network Detection is enabled and has detected that the machine is on the Corporate LAN.
- The Web Security license key is missing or invalid.
- The user is inactive for a configured amount of time and, as a result, the Test Inactivity Timeout threshold has been met.

**Step 8** Save the Web Security client profile.

## Configuring Secure Trusted Network Detection

The Secure Trusted Network Detection feature detects when an endpoint is on the corporate LAN, either physically or by means of a VPN connection. If the Secure Trusted Network Detection feature is enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than Cisco Cloud Web Security.



**Note**

For the equivalent feature for the VPN module, see [Trusted Network Detection, page 3-22](#).

Secure Trusted Network Detection verifies the client is connected to the corporate network using the SHA-256 hash (thumbprint) of an SSL certificate on a server at a known URL (address, IP, or FQDN). The encryption algorithm used by the certificate does not matter but only an SHA-256 hash can be used.

If you choose not to use Secure Trusted Network Detection and you have any proxies on your network, for example Cisco Cloud Web Security Connector, you must add each proxy to the list of proxy exceptions in the Exceptions panel in profile editor. See [Proxy Exceptions, page 6-14](#).

When operating from outside your internal network, Secure Trusted Network Detection makes DNS requests and attempts to contact the HTTPS server you provisioned. Cisco strongly recommends the use of aliasing to ensure that the name and internal structure of your organization are not revealed through these request by a machine being used outside your internal network.

Ensure you have a direct connection to the server where the SSL certificate is hosted and then follow this procedure to configure Web Security's interaction with Secure Trusted Network Detection:

- Step 1** Start the Web Security Profile Editor using one of these methods:
- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
  - In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile you wish to edit.
- Step 3** Click **Preferences** in the Web Security tree pane.
- Step 4** Select **Enable Trusted Network Detection**.
- Step 5** In the **https** box, enter the URL of each Trusted Server you want to add, then click **Add**. The URL may include the port address (default 443). The profile editor attempts to connect to Trusted Server. If this is not possible for some reason, but you know the SHA-256 hash of the server's certificate, you can enter it in the **Certificate hash** box and click **Set**.

**Note**

Trusted servers behind proxies are not supported.

- Step 6** Save the Web Security client profile.

## Configuring Authentication and Sending Group Memberships to the Cisco Cloud Web Security Proxy

- Step 1** Start the Web Security Profile Editor using one of these methods:
- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
  - In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile you wish to edit.

- Step 3** Click **Authentication**. See [Figure 6-4](#) for an illustration of the fields you configure in this procedure.
- Step 4** In the **Proxy Authentication License Key** field, enter the license key that corresponds to the company key, group key, or user key you created in Cisco ScanCenter. If you are going to authenticate users based on their Enterprise domain, enter the company key you created. If you are going to authenticate users based on their Cisco ScanCenter or Active Directory group, enter the group key you created. By default the tag is empty. If it is left empty, Web Security operates in pass-through mode.
- Step 5** Enter a **Service Password**. The default password for Web Security is **websecurity**. You can change this password when customizing the profile. The password must contain only alphanumeric characters (a-z, A-Z, 0-9) and the following special characters as other characters may be mistaken for control characters by the Windows command shell or may have special meaning in XML.

~ @ # \$ % \* - \_ + = { } [ ] : , . ? /

With this password, a user with administrator privileges can stop the Web Security service. Users with or without administrator privileges can start the Web Security service without this password. See the [“The service password used in this procedure is configured in the Authentication panel of the Web Security profile editor.”](#) section on [page 6-28](#) for more information.

- Step 6** You can send the scanning proxy server Enterprise Domain information and Cisco Cloud Web Security or Active Directory group information with every HTTP request. The scanning proxy will apply traffic filtering rules based on what it knows of the user’s domain and group membership.



**Note**

If you want to send the scanning server proxy a custom username and custom group information for a user, or your enterprise does not use Active Directory, skip this step and go to [Step 7](#).

- Click **Enable Enterprise Domains**. In the list, click **All Domains**. When the **All Domains** option is selected, and the machine is on a domain, then whatever domain the user belongs to will be matched and the username and group membership information will be sent to the Cisco Cloud Web Security scanning proxy. This is useful for companies where there is more than one domain present.
- Alternatively, click **Specify Individual Domains**.

Enter each domain name in NetBIOS format then click **Add**. For example the NetBIOS format of **example.cisco.com** is **cisco**. Do not enter domain names using the DNS format: **abc.def.com**.

If you specify a domain name in the Enterprise Domain name field, then Cisco Cloud Web Security identifies the currently logged-in Active Directory user and enumerates that user’s Active Directory groups and that information gets sent to the scanning proxy with every request.

- In the **Use** list, click **Group Include List** or **Group Exclude List** to either include or exclude group information in HTTP requests to the Cisco Cloud Web Security scanning proxy. Values can be any substring of the string to be matched.

**Group Include List.** After selecting **Group Include List**, add the Cisco Cloud Web Security or Active Directory group names to the Group Include list that you want to send to the Cisco Cloud Web Security scanning proxy server with HTTP requests. If a request comes from a user in the specified Enterprise Domain, the HTTP request will be filtered in accordance with the user’s group membership. If the user has no group membership, HTTP requests will be filtered using a default set of filtering rules.

**Group Exclude List.** After selecting **Group Exclude List**, add the Cisco Cloud Web Security or Active Directory group names to the Group Exclude list that you do not want to send to the Cisco Cloud Web Security scanning proxy server with HTTP requests. If the user belong to one of the groups in the Group Exclude List, that group name will not be sent to the scanning proxy server and

the user's HTTP requests will be filtered either by other group memberships or, at the minimum, by a default set of filtering rules defined for users with no Active Directory or Cisco Cloud Web Security group affiliation.

Now go to step 8.

**Step 7** Click **Custom matching and reporting for machines not joined to domains** to send the scanning proxy server custom name.

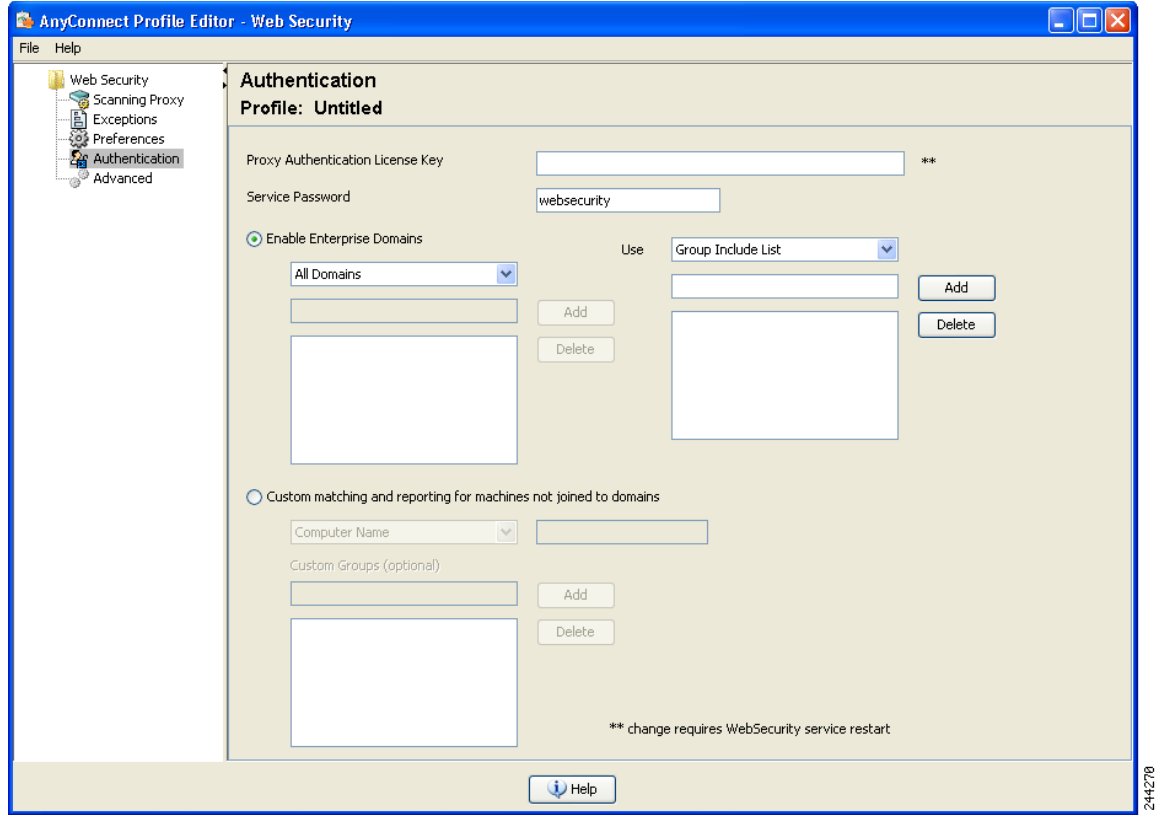
- In the list, click **Computer Name** to use the name of the computer. Alternatively, click **Local User** to use the local user name. Alternatively, click **Custom Name** and enter a custom user name. It could be defined by any string. If you do not enter a string, the IP address of the computer will be sent to the scanning proxy server instead. This username or IP address will be used in any Cisco ScanCenter reports that identify HTTP traffic from the custom user.
- In the **Authentication Group** field, enter a custom group name of up to 256 alphanumeric characters and click **Add**.

When HTTP requests are sent to the scanning proxy server, if a custom group name was sent, and there is a corresponding group name on the scanning proxy server, the HTTP traffic will be filtered by the rules associated with the custom group name. If there is not a corresponding custom group defined on the scanning proxy server, HTTP requests are filtered by the default rules.

If you only configured a custom user name and no custom group, HTTP requests will be filtered by the scanning proxy server default rules.

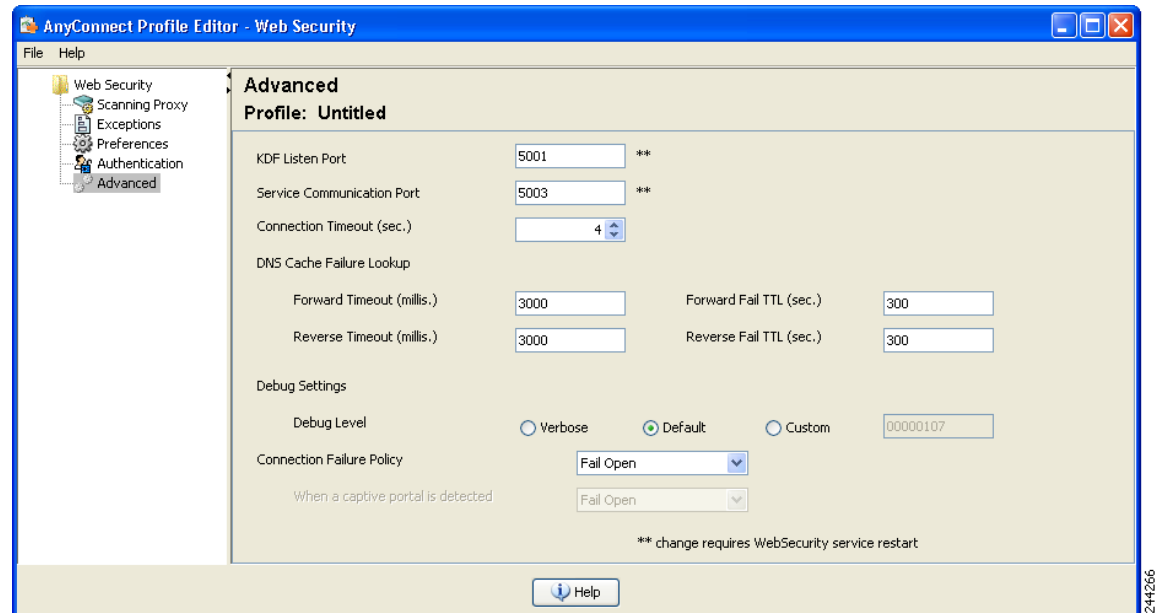
**Step 8** Save the Web Security client profile.

---

**Figure 6-4** Configuring Cisco Cloud Web Security Scanning Proxy Authentication

## Configuring Advanced Web Security Settings

The Advanced panel of a web security client profile exposes several settings that may help Cisco customer support engineers troubleshoot problems. You should not change the setting on this panel unless you are instructed to do so by customer support.

**Figure 6-5 Web Security Client Profile Advanced Panel**

From the Advanced panel in profile editor, you can perform these tasks:

- [Configuring KDF Listening Port, page 6-21](#)
- [Configuring Service Communication Port, page 6-22](#)
- [Configuring Connection Timeout, page 6-22](#)
- [Configuring DNS Cache Failure Lookup, page 6-23](#)
- [Configuring Debug Settings, page 6-23](#)
- [Configuring Fail Behavior, page 6-23](#)

## Configuring KDF Listening Port

The Kernel Driver Framework (KDF) intercepts all connections which use one of the Traffic Listening Ports as their destination port and forwards the traffic to the KDF Listening Port. The web scanning service analyzes all the traffic forwarded to the KDF Listening Port.

You should not change this setting unless instructed to do so by customer support.

- 
- Step 1** Start the Web Security Profile Editor using one of these methods:
- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
  - In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile you wish to edit.
- Step 3** Click **Advanced** in the Web Security tree pane. See [Figure 6-5](#) for an illustration of the **Advanced** panel in the Web Security profile editor.
- Step 4** Specify the KDF Listen Port in the **KDF Listen Port** field.

- Step 5** Save the Web Security client profile.
- 

## Configuring Service Communication Port

The Service Communication Port is the port on which the web scanning service listens for incoming connections from the AnyConnect GUI component, and some other utility components. You should not change this setting unless instructed to do so by customer support.

- 
- Step 1** Start the Web Security Profile Editor using one of these methods:
- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
  - In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Select the Web Security client profile you wish to edit and click **Edit**. Click **Advanced** in the Web Security tree pane. See [Figure 6-5](#) for an illustration of the **Advanced** panel in the Web Security profile editor.
- Step 3** Edit the **Service Communication Port** field.
- Step 4** Save the Web Security client profile.



**Note** If you change the port from the default value of 5300 you must restart the Web Security service and the AnyConnect GUI component.

---

## Configuring Connection Timeout

The connection timeout setting enables you to set the time-out before Web Security tries to go direct to the Internet without using the scanning proxies. If left blank, it will use the default value of four seconds. This allows users to get access to paid network services faster as they will not have to wait so long for the time-out to happen before retrying.

Follow this procedure to configure the Connection Timeout field:

- 
- Step 1** Start the Web Security Profile Editor using one of these methods:
- From ASDM, open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.
  - In Standalone mode on Windows, select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Open the Web Security client profile you wish to edit.
- Step 3** Click **Advanced** in the Web Security tree pane. See [Figure 6-5](#) for an illustration of the **Advanced** panel in the Web Security profile editor.
- Step 4** Change the **Connection Timeout** field.

**Step 5** Save the Web Security client profile.

---

## Configuring DNS Cache Failure Lookup

In the Advanced panel of profile editor you will see several fields for managing Domain Name Server lookups. These settings have been configured with optimal values for DNS lookups. You should not change this setting unless instructed to do so by customer support.

## Configuring Debug Settings

The Debug Level is a configurable field; however, you should not change this setting unless instructed to do so by customer support.

## Configuring Fail Behavior

In the **Connection Failure Policy** list, select **Fail Close** to block traffic if a connection to the Cisco Cloud Web Security proxy server cannot be established. Alternatively, select **Fail Open** to allow traffic.

In the **When a captive portal is detected** list, select **Fail Open** to allow traffic if a connection to the Cisco Cloud Web Security proxy server cannot be established but a captive portal, such as a Wi-Fi hot spot, is detected. Alternatively, select **Fail Close** to block traffic.



### Note

If host, proxy, or static exceptions are configured to include the captive portal address then Fail Close will not block traffic.

---

## Web Security Logging

### Windows

All Web Security messages are recorded in the Windows Event Viewer in the **Event Viewer (Local)\Cisco AnyConnect Web Security Module** folder. The events Web Security records in the event viewer are intended to be analyzed by Cisco Technical Assistance Center engineers.

### Mac OS X

You can view Web Security messages from the syslog or console.

## Web Security Client Profile Files

After you create and save the Web Security client profile using the profile editor bundled with AnyConnect, the profile editor makes two copies of the XML file; one file is obfuscated and has the file naming convention *filename.wso*; the other is in plain text and has the file naming convention *filename.wsp*.

After you create and save the Web Security client profile using the standalone profile editor, the plain text version of the client profile has the file naming convention *filename.xml* and the obfuscated file naming convention is *filename.wso*.

Having these two formats allows administrators to perform this special processing if needed:

- Administrators can export the obfuscated Web Security client profile from the ASA and can distribute it to endpoint devices.
- Administrators can edit the plain text Web Security client profile and perform edits that are not supported by the AnyConnect Web Security profile editor. You should not change the plain text version of the Web Security client profile unless instructed to do so by customer support.

## Exporting the Plain Text Web Security Client Profile File

- 
- |               |                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Open ASDM and choose <b>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Client Profile</b> .                                       |
| <b>Step 2</b> | Select the Web Security client profile you wish to edit and click <b>Export</b> .                                                                                    |
| <b>Step 3</b> | Browse to a local folder in which to save the file. Editing the file name in the Local Path field will save the Web Security client profile with that new file name. |
| <b>Step 4</b> | Click <b>Export</b> . ASDM exports the plain text <i>filename.wsp</i> version of the web security client profile.                                                    |
- 

## Exporting the Plain Text Web Security Client Profile File for DART Bundle

If you need to send a Diagnostic AnyConnect Reporting Tool (DART) bundle to Cisco customer service, you need to send the plain text version of the Web Security client profile file, *filename.wsp* or *filename.xml*, along with the DART bundle. Cisco Customer service will not be able to read the obfuscated version.

To gather the plain text version of the Web Security client profile created by the profile editor on ASDM, use the [Exporting the Plain Text Web Security Client Profile File](#) procedure.

The standalone version of Profile editor creates two versions of the Web Security profile file; one file is obfuscated and has the file naming convention *filename.wso* and the other is in plain text and has the file naming convention *filename.xml*. Gather the plain text version of the file, *filename.xml*.

Before sending the DART bundle to Cisco customer service, add the plain text version of your Web Security client profile to the DART bundle.

## Editing and Importing Plain Text Web Security Client Profile Files from ASDM

When you have exported the plain text Web Security client profile file, you can edit it on your local computer using any plain text or XML editor. Use this procedure to import it.

**Caution**

Importing the file **overwrites** the contents of the Web Security client profile you selected.

---

- 
- |               |                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Open ASDM and choose <b>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Client Profile</b> .                                  |
| <b>Step 2</b> | Select the Web Security client profile you wish to edit and click <b>Export</b> .                                                                               |
| <b>Step 3</b> | After making the changes to the <i>filename.wsp</i> file, return to the AnyConnect Client Profile page and select the Profile Name of the file that you edited. |
| <b>Step 4</b> | Click <b>Import</b> .                                                                                                                                           |



- Step 5** Browse to the edited version of the Web Security client profile and click **Import**.
- 

## Exporting the Obfuscated Web Security Client Profile File

- Step 1** Open ASDM and choose **Tools > File Management**.
- Step 2** In the File Management screen click **File Transfer > Between Local PC and Flash** and use the File Transfer dialog to transfer the obfuscated *filename.wso* client profile file to your local computer.
- 

## Creating a Web Security Client Profile with the Standalone Editor

- Step 1** Open the Web Security Standalone Profile Editor by choosing **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.
- Step 2** Create a Web Security client profile using the [“Creating an AnyConnect Web Security Client Profile” section on page 6-7](#).
- Step 3** Save the Web Security client profile by choosing **File > Save**. The standalone profile editor makes two copies of the XML file; one file is obfuscated and has the file naming convention *filename.wso*; the other is in plain text and has the file naming convention *filename.xml* (equivalent of the *wsp* file generated by the ASDM tool).
- Step 4** Rename or save the obfuscated *filename.wso* client profile file with the name **WebSecurity\_ServiceProfile.wso** to one of these directories:
- For Windows XP users, put the file in this folder:  
**%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security**
  - For Windows Vista and Windows 7 users, put the file in the this folder:  
**%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security**
  - For Mac users, put the file in this folder:  
**/opt/cisco/anyconnect/websecurity**
- Step 5** Restart the Cisco AnyConnect Web Security Agent windows service using the [“Switching off and Enabling the Cisco AnyConnect Web Security Agent” section on page 6-28](#).
- 

## Configuring Split Exclusion Policy for Web Security

### Information about the Split Exclusion Policy

When a user has established a VPN session, all network traffic is sent through the VPN tunnel. However, when AnyConnect users are using web security, the HTTP traffic originating at the endpoint needs to be excluded from the tunnel and sent directly to the Cloud Web Security scanning proxy.

To set up the split tunnel exclusions for traffic meant for the Cloud Web Security scanning proxy, use the **Set up split exclusion for Web Security** button in a group policy.

## Prerequisites

- Web security needs to be configured for use with the AnyConnect client.
- You have created a Group Policy and assigned it a Connection Profile for AnyConnect clients configured with Web Security.

## Detailed Steps

- 
- Step 1** Start an ASDM session for the head end you want to configure and select **Remote Access VPN > Configuration > Group Policies**.
  - Step 2** Select the Group Policy you want to configure and click **Edit**.
  - Step 3** Select **Advanced > Split Tunneling**.
  - Step 4** Click **Set up split exclusion for Web Security**.
  - Step 5** Enter a new, or select an existing, access list used for Web Security split exclusion. ASDM will set up the access list for use in the network list.
  - Step 6** Click **Create Access List** for a new list or **Update Access List** for an existing list.
  - Step 7** Click **OK**.
- 



### Tip

If you use the Secure Trusted Network Detection feature and want to ensure that Web Security and VPN are active at the same time, configure your network so that the HTTPS server is not reachable over the VPN Tunnel. In this way, the Web Security functionality will go into bypass mode, only when the user is on the corporate LAN.

---

## What to do next

When additional scanning proxies are added, update the unified access list you created in this procedure with new information.

# Configuring Cisco ScanCenter Hosted Configuration Support for Web Security Client Profile

Starting in AnyConnect release 3.0.4, the Cisco ScanCenter Hosted Configuration for the Web Security Hosted Client Profile gives administrators the ability to provide new configurations to Web Security clients. This is done by allowing devices with Web Security to download a new Web Security Hosted Client Profile from the cloud (hosted configuration files reside on the Cisco ScanCenter server). The only prerequisite for this feature is for the device to have Web Security installed with a valid client profile. Administrators use the Web Security Profile Editor to create the client profile files and then upload the clear text XML file to a Cisco ScanCenter server. This XML file must contain a valid license key from Cisco Cloud Web Security. The client will retrieve the new config file, at most, eight hours after it is applied to the hosted config server.

The Hosted Configuration feature uses the license key when retrieving a new client profile file from the Hosted Configuration (Cisco ScanCenter) server. Once the new client profile file is on the server, devices with Web Security automatically poll the server and download the new client profile file, provided that the license in the existing Web Security client profile is the same as a license associated with a client profile on the Hosted server. When a new client profile has been downloaded, Web Security will not download the same file again until the administrator makes a new client profile file available.

The process for creating client profile files and making them available for downloading to Web Security devices is as follows:

**Note**

Web Security client devices must be pre-installed with a valid client profile file containing a Cisco Cloud Web Security license key before it can use the Hosted Configuration feature.

- 
- Step 1** Using the Web Security profile editor, create a new client profile for the Web Security device. This client profile must contain the Cisco Cloud Web Security license key. Refer to the [Cisco ScanCenter Administration Guide, Release 5.2](#) for more information about license keys.
- Step 2** Save the client profile file as a clear text XML file. Upload this file to Cisco ScanCenter server. When the file is uploaded, you can make the new client profile available to Web Security clients. For more information on hosted configurations in Cisco Cloud Web Security, refer to [Cisco ScanCenter Administration Guide, Release 5.2](#).
- Step 3** The new client profile can be uploaded and applied via the Cisco ScanCenter for the company, provided that the Hosted Configuration feature has been enabled for the company. A hosted client profile is associated with a license. This means that if there are different licenses in use (for example, different group license keys), each license can have its own client profile associated with it. This allows the administrator to push down a different client profile to different users, depending on which license they have been configured to use. The administrator can store various configurations per license and set a default client profile for clients to download. It is then possible to switch to one of the other revisions of configurations stored in the Hosted Configuration area of Cisco ScanCenter by selecting that client profile as the default. Only one client profile can be associated with a license which means that if there are more than one revision associated with the license that only one can be the default.

**Note**

The restart Web Security agent service option is available only to users who have necessary rights to restart the service.

## Secure Trusted Network Detection

The Secure Trusted Network Detection feature detects when an endpoint is on the corporate LAN, either physically or through a VPN connection. If the Secure Trusted Network Detection feature is enabled, any network traffic originating from the corporate LAN bypasses Cisco Cloud Web Security scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than Cisco Cloud Web Security.

If you choose not to use Secure Trusted Network Detection and you have any proxies on your network, for example Cisco Cloud Web Security Connector, you must add each proxy to the list of proxy exceptions in the Exceptions panel in profile editor. See [Proxy Exceptions, page 6-14](#) for more information.

Configuring Secure Trusted Network Detection is also required for some third-party solutions, such as data loss prevention (DLP) appliances, which requires traffic to be unaffected by Web Security.

## Switching off and Enabling the Cisco AnyConnect Web Security Agent

An administrator can switch off and enable the Cisco AnyConnect Web Security Agent's ability to intercept web traffic by executing the following steps:

### Switching Off and Enabling Filters using Windows

The service password used in this procedure is configured in the Authentication panel of the Web Security profile editor.

- 
- |               |                                                                                                                                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Open a command prompt window.                                                                                                                                                                                                                           |
| <b>Step 2</b> | Change to the <code>%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client</code> folder.                                                                                                                                                         |
| <b>Step 3</b> | Switch filtering on or off: <ul style="list-style-type: none"><li>• To enable filtering, enter <code>acwebsecagent.exe -enablesvc</code></li><li>• To switch off filtering, enter <code>acwebsecagent.exe -disablesvc -servicepassword</code></li></ul> |
- 

### Switching Filters On and Off Using Mac OS X

The service password used in this procedure is configured in the Authentication panel of the Web Security profile editor.

- 
- |               |                                                                                                                                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Launch the Terminal application.                                                                                                                                                                                                                        |
| <b>Step 2</b> | Change to the <code>/opt/cisco/anyconnect/bin</code> folder.                                                                                                                                                                                            |
| <b>Step 3</b> | Switch off or enable filtering: <ul style="list-style-type: none"><li>• To enable filtering, enter <code>./acwebsecagent -enablesvc</code></li><li>• To switch off filtering, enter <code>./acwebsecagent -disablesvc -servicepassword</code></li></ul> |