CHAPTER 6

Configuring Web Security

The AnyConnect Web Security module is an endpoint component that routes HTTP traffic to a ScanSafe scanning proxy where the ScanSafe web scanning service evaluates it.

The ScanSafe web scanning service 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. The ScanSafe web scanning service then lets through benign or acceptable content and drops malicious or unacceptable content based on a security policy defined in the 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. The ScanSafe web scanning service protects users when they are on or off the corporate network.

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

You can configure one or more instances of Beacon Server to identify endpoints that are on the corporate LAN. This is the “Detect-on-LAN” feature. If the Detect-On-LAN feature is enabled, any network traffic originating from the corporate LAN bypasses ScanSafe scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than the ScanSafe web scanning service. Beacon Server uses a unique public/private key pair for your organization to ensure that only ScanSafe Web Security customers with the correct public key can bypass the ScanSafe scanning proxies while connected to your network. When deploying multiple instances of Beacon Server on your network, each instance must use the same private/public key pair.

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

ScanCenter is the management portal for ScanSafe web scanning services. Some of the components created or configured using 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:

- Configuring ScanSafe Scanning Proxies in the Client Profile
- Excluding Endpoint Traffic from Web Scanning Service
- Configuring Web Scanning Service Preferences
- Installing Beacon Server
- Configuring Authentication and Sending Group Memberships to the ScanSafe Scanning Proxy
- Web Security Client Profile Files
- Installing a Standalone Web Security Client Profile
- Configuring Split-Tunneling for Web Security Traffic
- Configuring ScanCenter Hosted Configuration Support for Web Security Client Profile
- Disabling 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
- Requirements for Beacon Server

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)
- OS X v10.5 x86 (32-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)

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

Requirements for Beacon Server

Beacon Server is supported on the following operating systems:

- Windows Server 2003 R1 x86 (32-bit) or x64 (64-bit)
- Windows Server 2003 R2 x86 (32-bit) or x64 (64-bit)
- Windows Server 2008 R1 x86 (32-bit) or x64 (64-bit)
- Windows Server 2008 R2 x64 (64-bit)

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 the ScanSafe web scanning services without having to install an ASA and without enabling the VPN capabilities of the AnyConnect Secure Mobility Client.

You still need a Secure Mobility for ScanSafe license in addition to ScanSafe Web Filtering and/or ScanSafe Malware Scanning licenses in order for roaming users to be protected by ScanSafe web scanning services.

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.

ScanCenter Licenses

You need a Secure Mobility for ScanSafe license in addition to ScanSafe Web Filtering and/or ScanSafe Malware Scanning licenses in order for roaming users to be protected by ScanSafe web scanning services.

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 6-8 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 the ScanSafe ScanCenter without enabling the AnyConnect VPN module and without an ASA. This section includes the following information:

- Installing the Web Security Module On a Windows OS 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 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 a Windows OS Using the AnyConnect Installer

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

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 OS for use with ScanSafe, follow this procedure.

Step 1 Download the Cisco AnyConnect Secure Mobility Client package from the 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 2-41.

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 6-8.

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 checked.
- 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 disabling 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 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 writeable 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 2-41.

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 6-8.

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 3.0.5074/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 3.0.5074/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 **3.0.4235** 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 3.0.5074/profiles/vpn** directory of the AnyConnect installer.

Note When installing the Web Security module only for AnyConnect 3.0.4235 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 a Windows OS 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 a Windows OS 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.

```
misexec /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 2-15 on page 2-39.

Step 6 Restart the Cisco AnyConnect Web Security Agent windows service using the "Disabling and Enabling the Cisco AnyConnect Web Security Agent" section on page 6-37.

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**.
- In Standalone mode on Windows OS, Select **Start > Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**.

Step 2 Click **Add** to create a client profile.

Step 3 Give the client profile a **name**.

Step 4 Click the **Profile Usage** field and select **Web Security**.

Step 5 Accept the default Profile Location or click **Browse** to specify an alternate file location.

Step 6 (Optional) Select a **Group Policy** to attach the client profile or leave the client profile <Unassigned>.

Step 7 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:

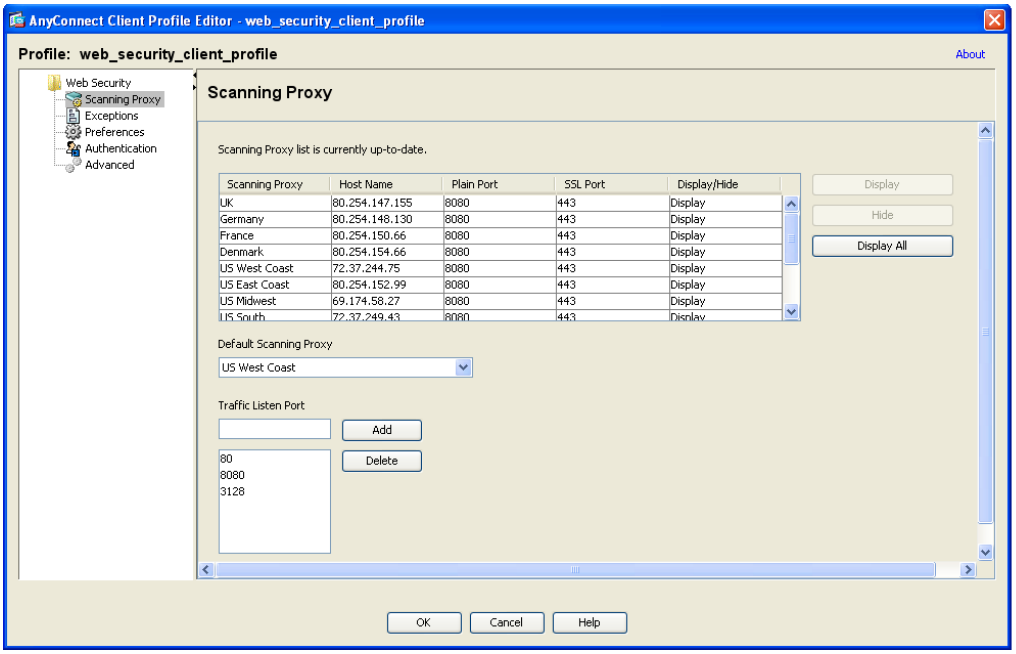
- Configuring ScanSafe Scanning Proxies in the Client Profile, page 6-9
- Excluding Endpoint Traffic from Web Scanning Service, page 6-12
- Configuring User Controls and Calculating Fastest Scanning Proxy Response Time, page 6-15
- Configuring Beacon Server Connections for Detect-On-LAN, page 6-17
- Configuring Authentication and Sending Group Memberships to the ScanSafe Scanning Proxy, page 6-27

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 6-32.

Configuring ScanSafe Scanning Proxies in the Client Profile

The ScanSafe web scanning service 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 ScanSafe proxy server on which the ScanSafe web scanning service analyzes the Web content. The Scanning Proxy panel in the AnyConnect Web Security profile editor defines to which ScanSafe 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 ScanSafe scanning proxies in an AnyConnect Web Security client profile:

- Creating an AnyConnect Web Security Client Profile, page 6-8
- 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 6-11

Updating the Scanning Proxy List

The Scanning Proxy list in the Web Security profile editor is not editable. You cannot add or remove ScanCenter 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 ScanCenter 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 ScanSafe scanning proxies to those in the scanning proxy list it downloaded from the ScanSafe 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 ScanSafe 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 ScanSafe scanning proxies.

Default Scanning Proxy Settings in a Web Security Client Profile

By default, the profile you create has these ScanSafe scanning proxy attributes:

- The scanning proxy list is populated with all the ScanSafe 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 ScanSafe scanning proxy is pre-selected. To configure the default ScanSafe 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 6-11 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 ScanSafe 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 ScanSafe 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 ScanSafe scanning proxies marked "Display" when ordering scanning proxies by response time.
- Users can choose which ScanSafe scanning proxy they connect to if their profile allows for user control.
- ScanSafe 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 ScanSafe scanning proxies to all users.

To hide or display a ScanSafe scanning proxies to users, follow this procedure:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the AnyConnect Web Security client profile you want to edit and click **Edit**. The Web Security profile editor opens and displays the Scanning Proxy panel (see Figure 6-2).

Step 3 To hide or display ScanSafe 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 ScanSafe scanning proxies is the recommended configuration.

Step 4 Save the AnyConnect Web Security client profile.

Selecting a Default Scanning Proxy

To define a default ScanSafe scanning proxy, follow this procedure:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the AnyConnect Web Security client profile you want to edit and click **Edit**. The Web Security profile editor opens and displays the Scanning Proxy panel (see Figure 6-2).

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 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the AnyConnect Web Security client profile you want to edit and click **Edit**. The Web Security profile editor opens and displays the Scanning proxy panel (see Figure 6-2).

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.

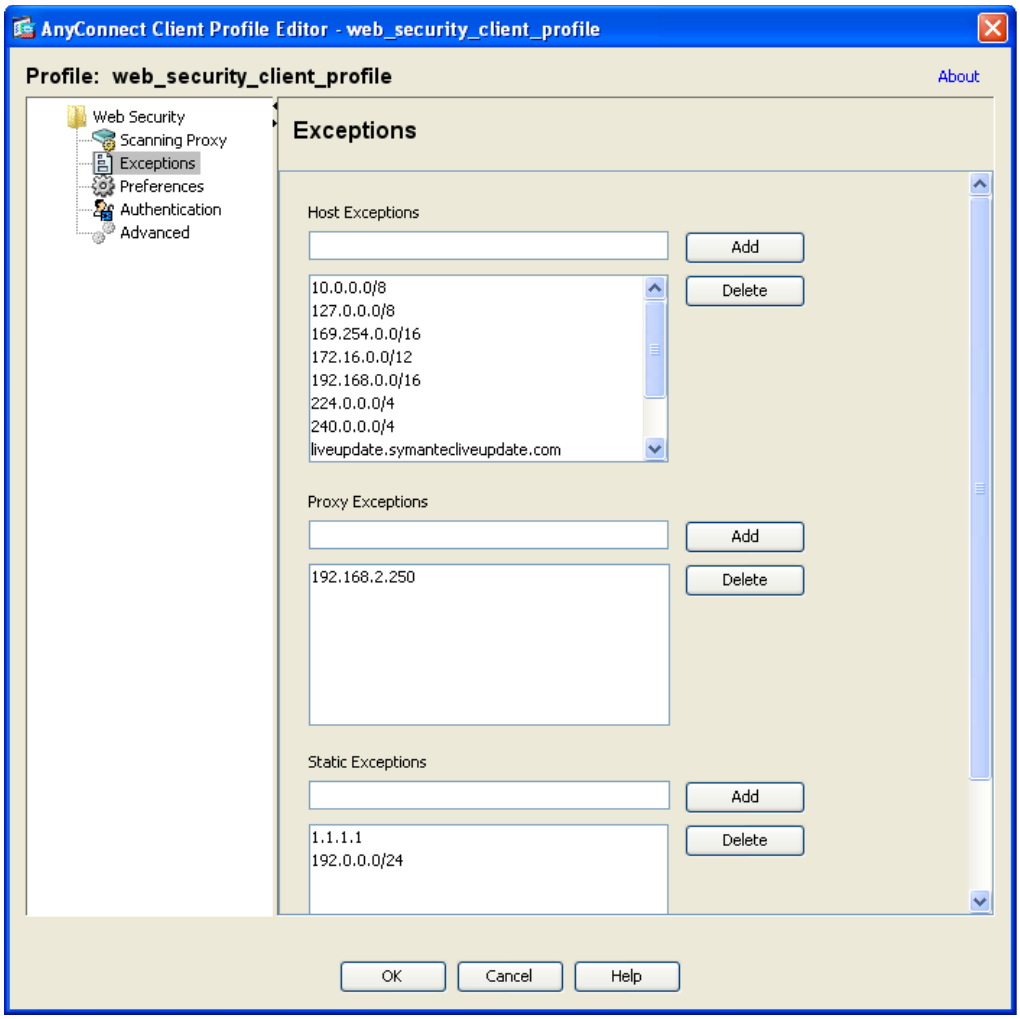
Excluding Endpoint Traffic from Web Scanning Service

If you do not want network traffic, originating from a particular IP address, to be evaluated by the ScanSafe web scanning service, 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 ScanSafe web scanning service. 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.

All private IP addresses described in RFC 1918 are included in the host exception list by default.

You can enter subnets and IP addresses using this syntax:

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

Specifying IP addresses prevents the ScanSafe web scanning service 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 ScanSafe web scanning service 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, the ScanSafe web scanning service 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 the ScanSafe web scanning service. In the list, include the ingress IP addresses of your VPN gateways. See Figure 6-3.

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 Beacon Server Connections for Detect-On-LAN, page 6-17

Configuring User Controls and Calculating Fastest Scanning Proxy Response Time

To allow users to choose the ScanSafe scanning proxy they connect to, follow this procedure:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile.**

Step 2 Select the Web Security client profile you wish to edit and click **Edit**.

Step 3 Click **Preferences**. See Figure 6-4 for an illustration of the fields you configure in this procedure.

Step 4 Check **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 If you would like Web Security to automatically select a scanning proxy, check **Automatic Scanning Proxy Selection**. If you do this, **Order Scanning Proxies by Response Time** is checked 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.

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

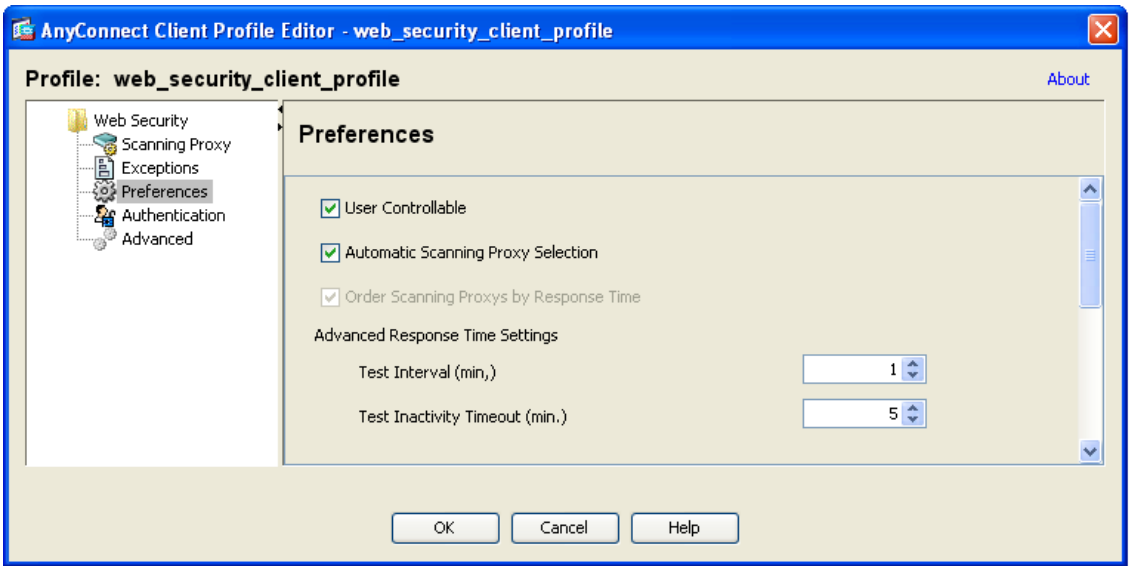
- **Test Interval**: The time, in minutes, between running each performance test. You should not change this setting unless instructed to do so by customer support.
- **Test Inactivity Timeout**: The time, in minutes, after which Web Security suspends the response time test because of user inactivity. 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:

- "Detect-On-LAN" is enabled and Beacon Server 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 7 Save the Web Security client profile.

Figure 6-4 User Controls and Order Scanning Proxies by Response Time Controls



Configuring Beacon Server Connections for Detect-On-LAN

The Detect-On-LAN feature detects when an endpoint is on the corporate LAN, either physically or by means of a VPN connection. If the Detect-On-LAN feature is enabled, any network traffic originating from the corporate LAN bypasses ScanSafe scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than the ScanSafe web scanning service. For further information see Detect-On-LAN, page 6-35.

Beacon Server uses a unique public/private key pair for your organization to ensure that only ScanSafe Web Security customers with the correct public key can bypass the ScanSafe scanning proxies while connected to your network. When deploying multiple instances of Beacon Server on your network, each instance must use the same private/public key pair.

Note If you choose not to use Beacon Server and you have any proxies on your network, for example ScanSafe 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.

Follow this procedure to configure Web Security's interaction with Beacon Server:

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Edit**.

Step 3 Click **Preferences**. See Figure 6-5 for a picture of the Preferences panel.

Step 4 If you have installed Beacon Server on your network and you have configured it to receive traffic from Web Security users, check **Beacon Check**.

Step 5 In the **Public Key File** field, click **Browse** and select your company's public key certificate. Beacon Server uses RSA public/private key pairs for authentication. Private keys must be a minimum of 512 bits in length; however, Cisco recommends using keys of 1,024 bits.

Step 6 In the **New Beacon Address** field, identify the computer where Beacon Server is installed. Use either a valid IP address or domain name. Here are examples of proper syntax:

Syntax	Example
Individual IPv4 addresses	`10.10.10.123`
Fully Qualified Domain Names	`beaconserver.cisco.com` **Note** Partial domains are not supported; for example, cisco.com would not be supported.

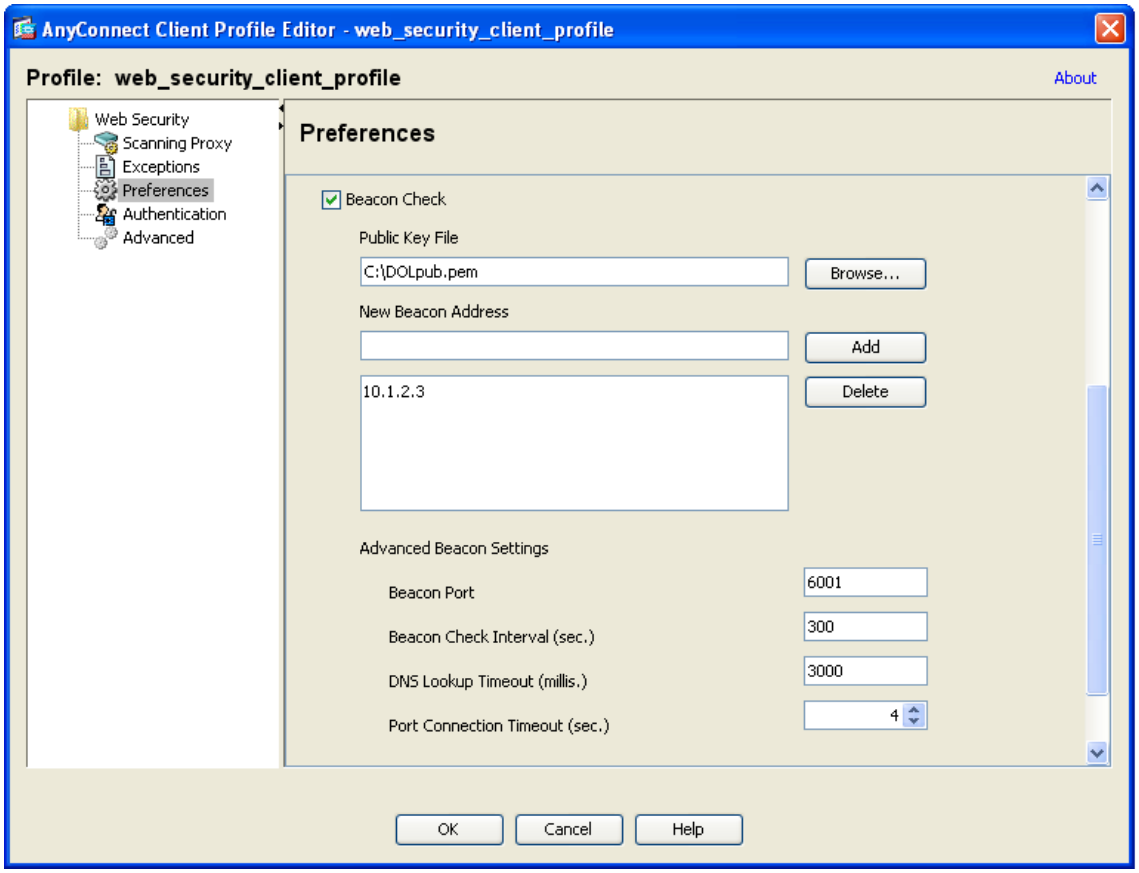
Step 7 Configure these Advanced Beacon Settings:

- **Beacon Port**: This element specifies the TCP/IP port used by the service. If you already have a service running on port 6001, you can change this element. You will also need to change the corresponding element in the websecurity.config file on the computer where Beacon Server is installed.
- **Beacon Check Interval:** Web Security will wait this time, specified in seconds, in between attempts to contact Beacon Server and thus determine if it is on a LAN.

- **DNS Lookup Timeout:** Timeout, in milliseconds, for DNS lookups on the hostnames (if any) provided in the <Beacons> setting. You should not change this setting unless instructed to do so by customer support.
- **Port Connection Timeout**: This element specifies the time, in seconds, after which a connection that is not sending any data to Beacon Server will be closed. You should not change this setting unless instructed to do so by customer support.

Step 8 Save the Web Security client profile.

Figure 6-5 Beacon Server Check Configuration

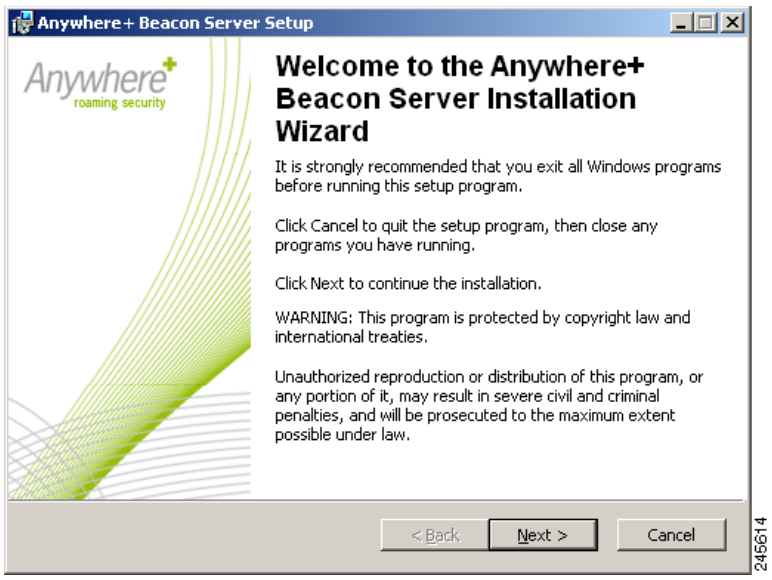


Installing Beacon Server

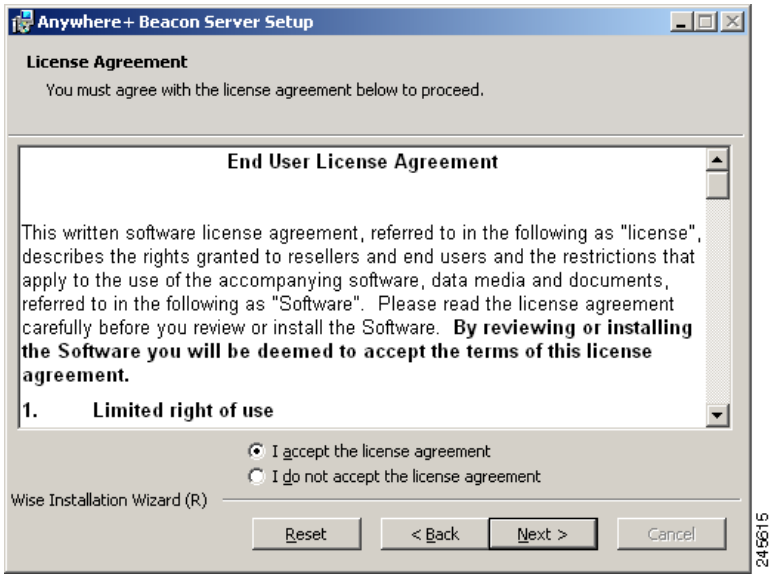
Before installing Beacon Server you should copy the DOLprv.pem file to the installation folder containing the BeaconServer.msi program file. See Generating Public and Private Keys, page 6-36. If you copy a BeaconServer.config file to the same folder, this will be installed in place of the default configuration file. This is not necessary unless you are installing more than one copy of Beacon Server because the configuration file can be edited after installation. See Configuring Beacon Server, page 6-24. In addition to the standard installation method you may choose to perform a silent install. See Silent Install, page 6-21.

To install Beacon Server:

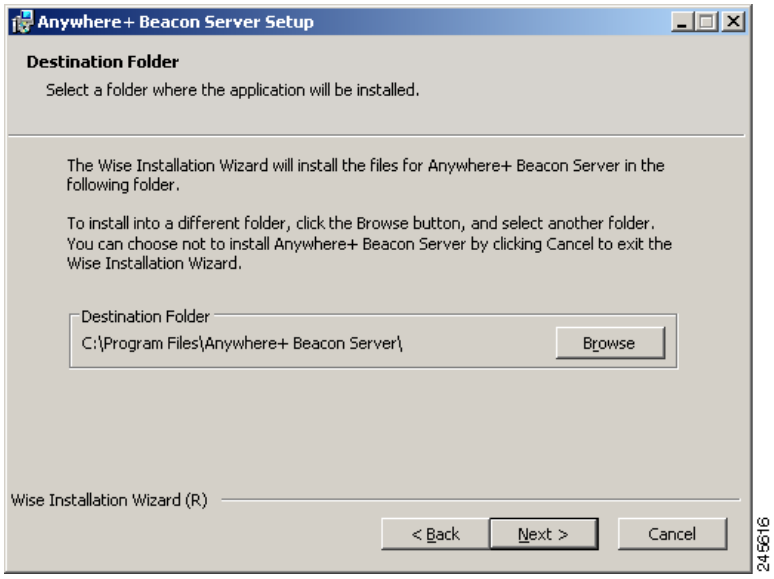
Step 1 Double-click the BeaconServer.msi program file to run the installation wizard.



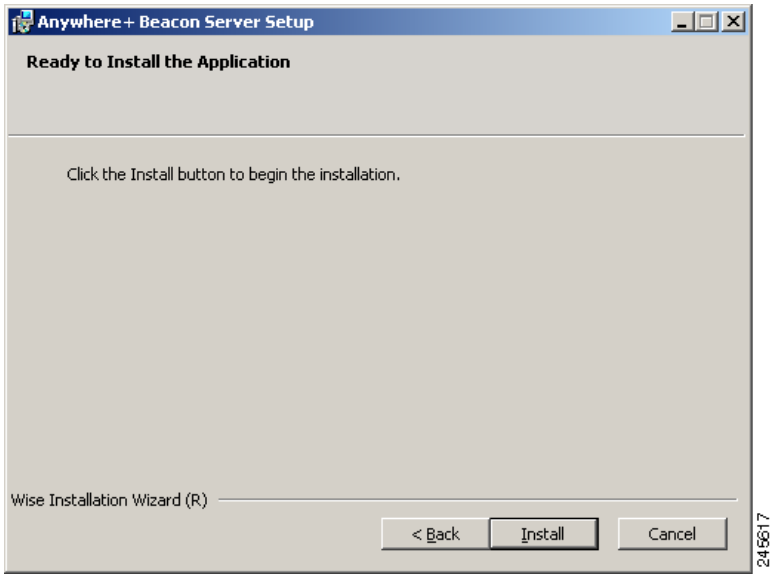
Step 2 Click **Next** to display the License Agreement dialog.



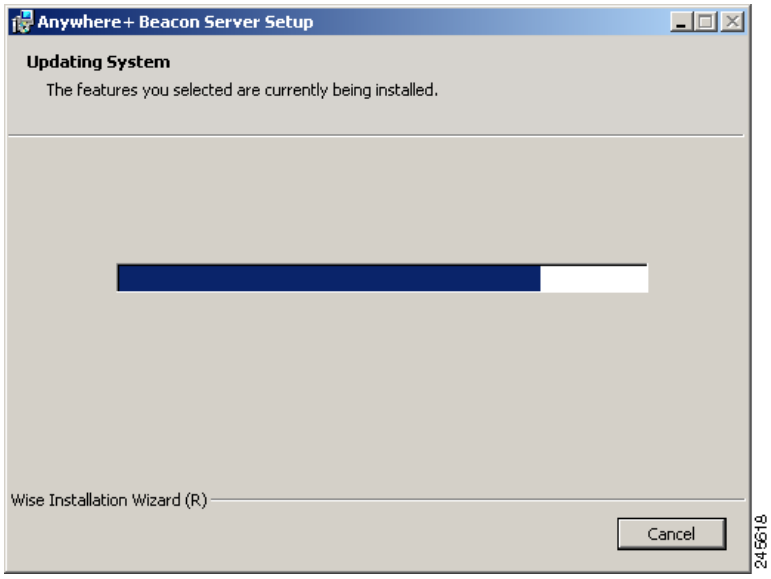
Step 3 Read the End User License Agreement. If you agree to the terms, click **I accept the license agreement** then click **Next** to display the Destination Folder dialog. Alternatively, if you do not agree to the terms, click **Cancel** to stop the installation.



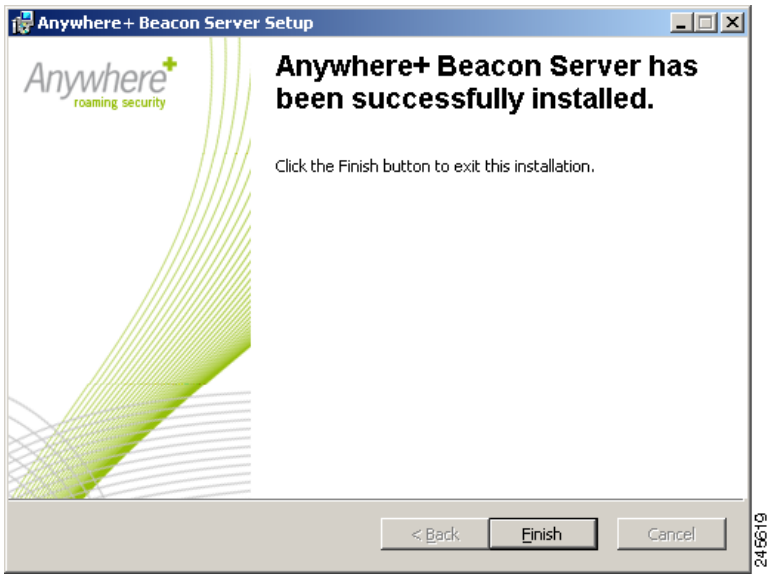
Step 4 Click **Next** to accept the default installation folder. Alternatively, click **Browse** and navigate to the required folder, then click **Next** to display the Ready to Install the Application dialog.



Step 5 Click **Install** to begin the installation.



Step 6 When the installation tasks have completed successfully, the following dialog is displayed:



Note If you encounter any installation issues, you can launch the installer from the command prompt. Enter msiexec /i <path>/BeaconServer.msi /l*vx install.log. This will create a log file called install.log.

Silent Install

Beacon Server supports the silent mode of the MSI installer using the following command:

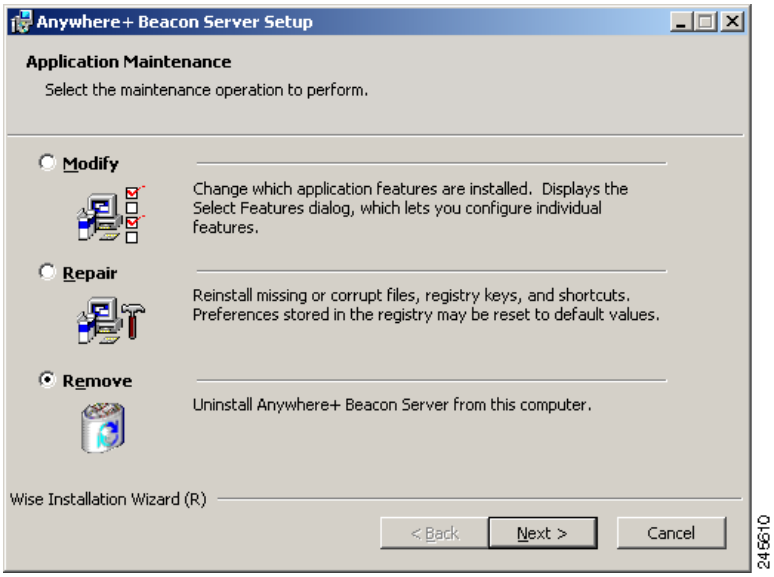
```
msiexec /i <path>/BeaconServer.msi /l*vx install.log /qn
```

The path can be a local folder, for example C:\temp, or a network share, for example \\server\share.

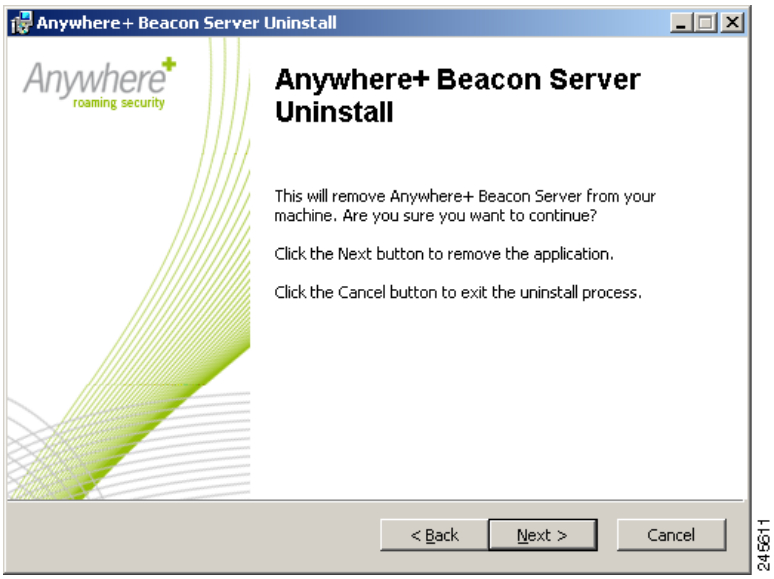
Removing Beacon Server

Before removing Beacon Server, ensure the Beacon Server service is stopped. Beacon Server can be removed using the Add/Remove Programs control panel, or from the command prompt by entering **`msiexec /x <path>BeaconServer.msi /l*vx uninstall.log /qn`**. Alternatively, to remove Beacon Server from a server using the wizard:

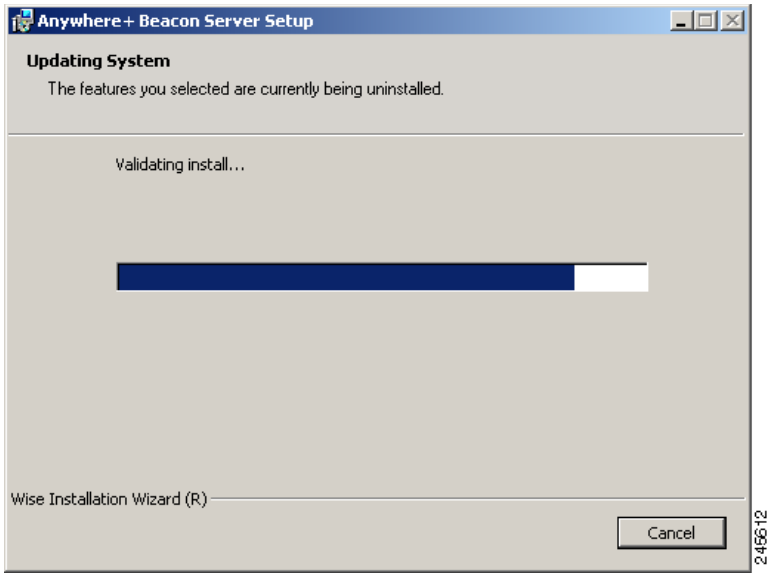
Step 1 Double-click the BeaconServer.msi program file to run the wizard.



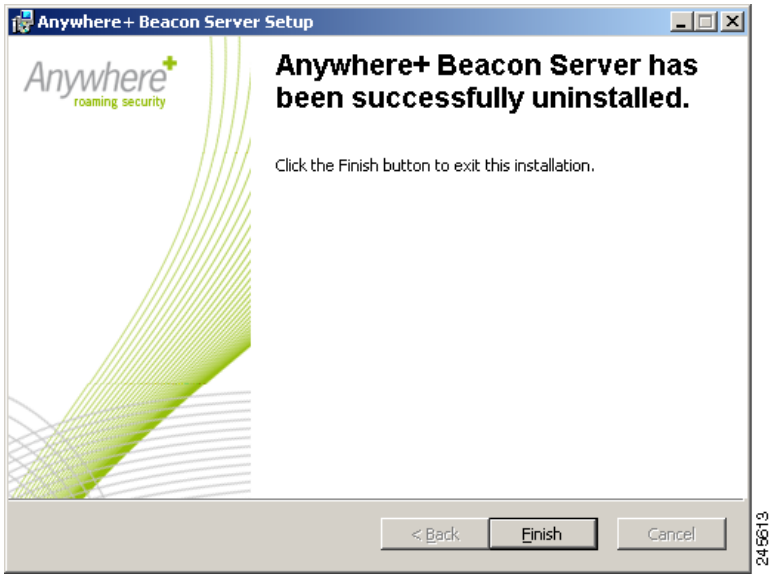
Step 2 Click **Remove** then click **Next** to display the Beacon Server Uninstall dialog.



Step 3 Click **Next** to remove Beacon Server. Alternatively, click **Cancel** to abandon the removal process.



Step 4 When the removal tasks have completed successfully, the following dialog is displayed:



Step 5 Click Finish to close the wizard.

Configuring Beacon Server

Beacon Server is configured by editing the BeaconServer.config XML file. This can be found in the folder where Beacon Server was installed, typically C:\Program Files\Anywhere+ Beacon Server\. The default configuration is as follows:

```
<DetectOnLANServer>
    <ConfigurationParameters>
        <!-- Beacon Port, default 6001 -->
        <BeaconPort>6001</BeaconPort>
        <!-- Connection Timeout in secs, default 10 -->
        <ConnectionTimeout>10</ConnectionTimeout>
        <!-- Disallowed Source IP addresses ';' separated -->
        <DisallowedSourceIP></DisallowedSourceIP>
        <Logging>
            <debug_level>00000107</debug_level>
            <!-- Log file size in kilobytes (KB) -->
            <LogFileSize>1000</LogFileSize>
            <!-- Number of log files to retain -->
            <NumLogFilesToRetain>10</NumLogFilesToRetain>
            <!-- This setting specifies the time for which a log file can be retained
before being deleted -->
            <LogFileRetentionTime>
                <Days>7</Days>
                <Hours>0</Hours>
                <Minutes>0</Minutes>
            </LogFileRetentionTime>
        </Logging>
    </ConfigurationParameters>
</DetectOnLANServer>
```

Unless instructed to do so by support, you should change only the following elements:

BeaconPort	This element specifies the TCP/IP port used by the service. If you already have a service running on port 6001, you can change this element. You will also need to change the corresponding element in the Admin.cfg file on each client computer.
ConnectionTimeout	This element specifies the time in seconds after which a connection that is not sending any data to Beacon Server will be closed.
DisallowedSourceIP	This element contains any IP addresses that you want to prevent bypassing the AnyConnect service via Beacon Server. Rather than using multiple elements, only a single element is used with each IP address separated by a semi-colon (;).
Logging	See Logging.

Logging

Contains a set of sub-tags that control log file cycling:

debug_level	This should not be changed unless you are explicitly instructed to do so by a customer support representative.
LogFileSize	The maximum permitted log file size in kilobytes (100 to 10000). When the current log file reaches the maximum allowed size, it will be backed up and a new log file will be created. The default size is 100KB.
NumLogFilesToRetain	The number of old log files to retain. The default is 10. When the permitted limit is reached older log files will be deleted.
LogFileRetentionTime	The time after which a log file will be deleted, whether or not the maximum number of log files has been reached. It is specified with the following sub-tags: • Days • Hours • Minutes

System Tray Icons

A system tray icon indicates the status of the service:


The service is running


There is a problem with the service.

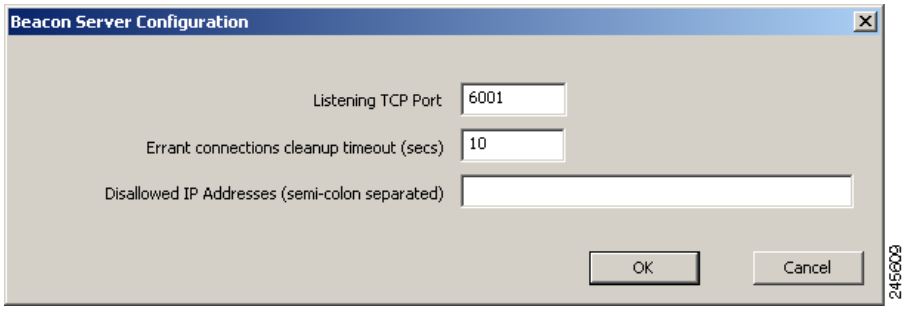

The service is stopped, or there is no private key file, or the private key file is corrupted

To start the service, right-click the icon then click **Start Beacon Server**.

To stop the service, right-click the icon then click **Stop Beacon Server**.

To configure Beacon Server:

Step 1 Right-click the icon then click **Preferences** to display the Beacon Configuration dialog.



Step 2 Enter the TCP/IP port the service will use in the “Listening TCP port” box.

Step 3 Enter the time in seconds that a connection should remain open in the “Errant connections cleanup timeout (secs)” box.

Step 4 Enter any IP addresses or host names that you want to bypass the AnyConnect service, separated by a semi-colon (;) in the “Disallowed IP Addresses (semi-colon separated)” box.

Step 5 Click **OK** to save your changes in the BeaconServer.config file. Alternatively, click **Cancel** to abandon your changes.

To close the system tray application, right-click the icon then click **Terminate GUI**. This does not stop the service if it is running. To restart the system tray icon, enter the following at the command prompt:

```
<BeaconServerInstallFolder>\BeaconServer -BD
```

Configuring Detect-On-LAN

To configure the Detect-On-LAN feature, follow this procedure:

Step 1 Install one or more copies of Beacon Server on your network. See Installing Beacon Server, page 6-18.

Note Beacon Server must be accessible to all Web Security installations that are brought into the corporate LAN physically and to those connected over a full tunnel VPN.

Step 2 Create a Web Security client profile using the “Creating an AnyConnect Web Security Client Profile” section on page 6-8. Ensure that the client profile specifies the group policy you want to deploy to your AnyConnect users.

Step 3 Using the “Configuring Beacon Server Connections for Detect-On-LAN” section on page 6-17, configure these settings in the Preferences Panel of the Web Security client profile:

- Check **Beacon Check** to enable it.
- In the Public Key File field, point to the public key file (DOLpub.pem) you created as part of your public/private key pair.
- Add the IP addresses of each instance of Beacon Server to the **New Beacon Address** field.

Step 4 Configure and save the remainder of the Web Security client profile.

Step 5 To receive this Web Security client profile with the Detect-On-LAN feature configured, users must select the name of this client profile in the VPN combo box of the AnyConnect Secure Mobility Client, when they attempt to establish a VPN connection to the ASA.

Configuring Authentication and Sending Group Memberships to the ScanSafe Scanning 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 OS, 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**.

Step 3 Click **Authentication**. See Figure 6-6 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 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 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) 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 non-administrator privileges can start and stop the Web Security service. Users with administrator privileges can start and stop 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 6-37 for more information.

Step 6 You can send the scanning proxy server Enterprise Domain information and ScanSafe or Active Directory group information with every HTTP request. The scanning proxy will the 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 the **Use Enterprise Domains** radio button.

  Enter the domain names in NetBIOS format. 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 ScanCenter 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.

  You can enter an asterisk (*) as an Enterprise Domain to indicate one of the following:

  - The (*) is used as a wildcard indicating any domain. For both Windows and Mac OS X computers, if the Enterprise Domain entry is a (*), 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 ScanSafe scanning proxy. This is useful for companies where there is more than one domain present.
  - The Mac OS X client should use the username instead of the IP address for users who do not have an Active Directory domain user name.

- Use the **Group Include List** and **Use Group Exclude List** areas to either include or exclude group information in HTTP requests to the ScanSafe scanning proxy:

  Group Include List. After selecting **Group Include List**, add the ScanSafe or Active Directory group names to the Group Include list that you want to send to the ScanSafe 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 ScanSafe or Active Directory group names to the Group Exclude list that you do not want to send to the ScanSafe 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 filtererd either by other group memberships or, at the minimum, by a default set of filtering rules defined for users with no Active Directory or ScanSafe group affiliation.

Step 7 Click the **Use Authenticated User/Group** radio button to send the scanning proxy server a custom username and group name.

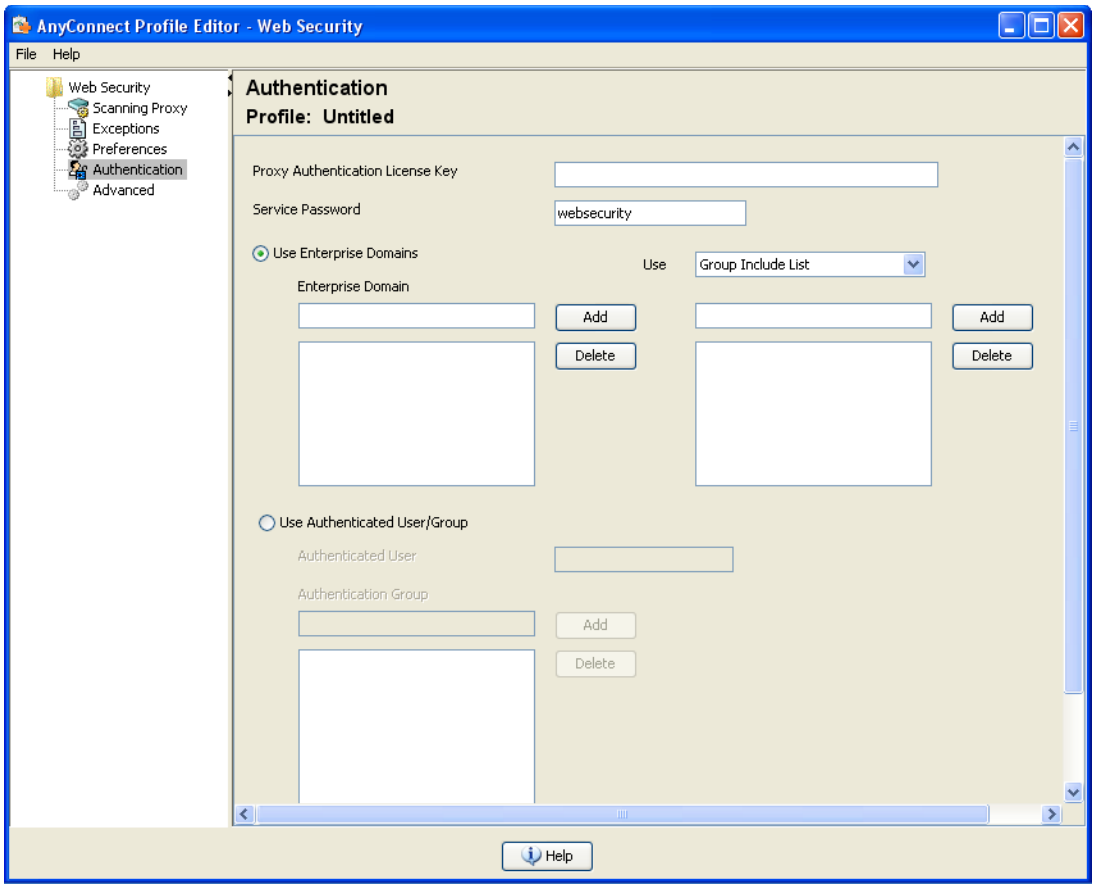
- In the **Authenticated User** field, enter a custom user name. It could be defined by any string. If you do not enter a string, the IP address of the computer will be sent to the scanning proxy server instead. This username or IP address will be used in any ScanCenter reports that identify HTTP traffic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

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 associtaed 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.

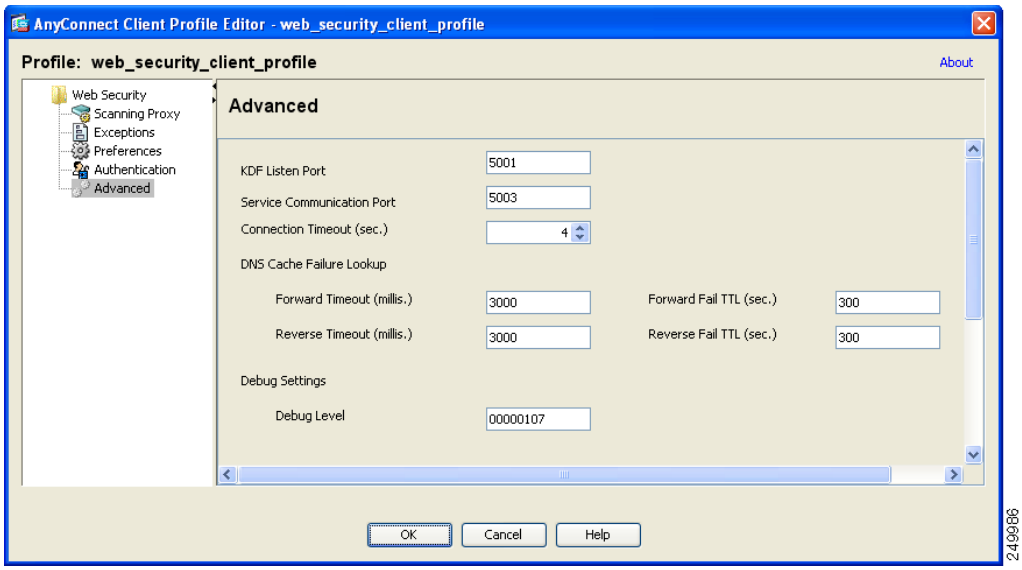
Figure 6-6 Configuring ScanSafe Scanning Proxy Authentication



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 6-7 Web Security Client Profile Advanced Panel



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

- Configuring KDF Listening Port, page 6-30
- Configuring Service Communication Port, page 6-31
- Configuring Connection Timeout, page 6-31
- Configuring DNS Cache Failure Lookup, page 6-31
- Configuring Debug Settings, page 6-31

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 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

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 6-7 for an illustration of the **Advanced** panel in the Web Security profile editor.

Step 3 Specify the KDF Listen Port in the **KDF Listen Port** field.

Step 4 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 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

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 6-7 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.

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 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

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 6-7 for an illustration of the **Advanced** panel in the Web Security profile editor.

Step 3 Change the **Connection Timeout** field.

Step 4 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.

Web Security Logging

Windows OS

All Web Security messages are recorded in the Windows Event Viewer in the **Event Viewer (Local)\Cisco AnyConect 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

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Export**.

Step 3 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.

Step 4 Click **Export**. ASDM exports the plain text *filename*.wsp 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.

Step 1 Open ASDM and choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**.

Step 2 Select the Web Security client profile you wish to edit and click **Export**.

Step 3 After making the changes to the *filename*.wsp file, return to the AnyConnect Client Profile page and select the Profile Name of the file that you edited.

Step 4 Click **Import**.

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.

Installing a Standalone Web Security Client Profile

Use the standalone profile editor to create a Web Security client profile when you do not have an ASA.

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 6-8.

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 "Disabling and Enabling the Cisco AnyConnect Web Security Agent" section on page 6-37.

Configuring Split-Tunneling for Web Security Traffic

Web Security and VPN can be used simultaneously. For optimal performance in this configuration, we recommend that the IP address to ScanSafe scanning proxies are excluded from the tunnel.

No other Split Exclusion needs to be configured as all decisions as to what traffic is sent to the ScanSafe scanning proxies is determined by the Web Security configuration.

To obtain a list of ScanSafe Scanning Proxy IP Addresses, refer to the following live document which contains the list of addresses:

http://80.254.145.118/websecurity-config-v2ip.xml

If you use the Detect On LAN feature and want to ensure that Web Security and VPN are active at the same time, configure your network so that Beacon 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.

Configuring ScanCenter Hosted Configuration Support for Web Security Client Profile

Starting in AnyConnect release 3.0.4, the 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 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 ScanCenter server. This XML file must contain a valid license key from ScanSafe. 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 (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 ScanSafe 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 ScanSafe license key. Refer to the ScanCenter Administration Guide, Release 5.1 for more information about license keys.

Save the client profile file as a clear text XML file. Upload this file to 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 ScanSafe, refer to ScanCenter Administration Guide, Release 5.1.

The new client profile can be uploaded and applied via the ScanCenter portal of 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 on the Hosted configuration portal 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.

Step 2 After the client has downloaded a hosted client profile, the new client profile is automatically used but will require that the user do one of the following:

- Put the device in sleep mode and then resume. On resume the client uses the new configuration.
- Reboot the device.
- Restart the Web Security agent service on the device

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

Detect-On-LAN

The Detect-On-LAN feature detects when an endpoint is on the corporate LAN, either physically or through a VPN connection. If the Detect-On-LAN feature is enabled, any network traffic originating from the corporate LAN bypasses ScanSafe scanning proxies. The security of that traffic gets managed by other methods and devices sitting on the corporate LAN rather than the ScanSafe web scanning service.

Beacon Server uses a unique public/private key pair for your organization to ensure that only Web Security clients with the correct public key can bypass the scanning proxies while connected to your network.You can also deploy multiple copies of Beacon Server if required, providing they use the same private/public key pair. You generate the private/public key pair on the ScanCenter portal.

If you choose not to use Beacon Server and you have any proxies on your network, for example ScanSafe 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 Detect-On-LAN is also required for some third-party solutions, such as data loss prevention (DLP) appliances, which requires traffic to be unaffected by Web Security.

Generating Public and Private Keys

Beacon Server uses RSA public/private key pairs for authentication. Private keys must be a minimum of 512 bits in length; however, Cisco recommends using keys of 1,024 bits.

The private key filename must be DOLprv.pem, and the public key filename must be DOLpub.pem. The public key will be embedded in the configuration file.

You will need a tool such as Microsoft C ertificate Services (a component of Windows Server operating systems) or OpenSSL (http://www.openssl.org/) to generate the RSA key pair. For information on using Microsoft Certificate Services refer to your vendor documentation.

Generating the Private Key Using OpenSSL

Navigate to the folder containing the openssl.exe program file and enter:

```
openssl genrsa -out DOLprv.pem 1024
```

Copy the DOLprv.pem file to the folder containing the BeaconServer.msi file. Alternatively, if you have already installed Beacon Server, copy the DOLprv.pem file to the folder where it was installed.

Generating the Public Key Using OpenSSL

Before generating the public key you must have created a private key called DOLprv.pem which should be located in the same folder as the openssl.exe program. To create the public key, enter:

```
openssl rsa -in DOLprv.pem -out DOLpub.pem -outform PEM -pubout
```

Copy the DOLpub.pem file to the folder where the AnyConnect Web Security module was installed.

Caution If you do not deploy the public key when installing the AnyConnect Web Security module, you will have to manually install it on every computer where AnyConnect is installed.

Disabling and Enabling the Cisco AnyConnect Web Security Agent

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

Disabling and Enabling Filters using Windows

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

Step 1 Open a command prompt window.

Step 2 Change to the **%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client** folder.

Step 3 Disable or enable filtering:

- To enable filtering, enter **acwebsecagent.exe -enablesvc**
- To disable filtering, enter **acwebsecagent.exe -disablesvc -*servicepassword***

Disabling and Enabling Filters Using Mac OS X

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

Step 1 Launch the Terminal application.

Step 2 Change to the **/opt/cisco/anyconnect/bin** folder.

Step 3 Disable or enable filtering:

- To enable filtering, enter **acwebsecagent -enablesvc**
- To disable filtering, enter **acwebsecagent -disablesvc -*servicepassword***

Windows Lockdown Option

Cisco recommends that end users are given limited rights on the device hosting the AnyConnect Secure Mobility client. If an end user warrants additional rights, installers can provide a lockdown capability that prevents users and local administrators from switching off or stopping those Windows services established as locked down on the endpoint. It is still possible to stop the services from the command prompt with the service password.

Each MSI installer supports a common property (LOCKDOWN) which, when set to a non-zero value, prevents the Windows service(s) associated with that installer from being controlled by users or local administrators on the endpoint device. We recommend that you use the sample transform provided at the time of install to set this property and apply the transform to each MSI installer that you want to have locked down.

If you deploy the core client plus one or more optional modules, you must apply the lockdown property to each of the installers. This operation is one way only and cannot be removed unless you re-install the product.

Note This feature is not available in the Mac OS X client.