CHAPTER 12

Configuring Application Acceleration

This chapter describes how to configure the application policies on your WAAS system that determine the types of application traffic that is accelerated over your WAN.

Note Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE appliances, WAE Network Modules (the NME-WAE family of devices), and SM-SRE modules running WAAS.

This chapter contains the following sections:

- About Application Acceleration, page 12-1
- Enabling and Disabling the Global Optimization Features, page 12-2
- Creating a New Traffic Application Policy, page 12-29
- Managing Application Acceleration, page 12-37

About Application Acceleration

The WAAS software comes with over 150 predefined application policies that determine the type of application traffic your WAAS system optimizes and accelerates. These predefined policies cover the most common type of application traffic on your network. For a list of the predefined policies, see Appendix A, "Predefined Application Policies."

Each application policy contains the following elements:

- Application definition—Identifies general information about a specific application, such as the application name, the differentiated services code point (DSCP) marking value that is applied to the traffic, and whether the WAAS Central Manager collects statistics about this application.
- Classifier—Contains a matching condition that identifies specific types of traffic. For example, the default HTTP classifier matches all traffic going to ports 80, 8080, 8000, 8001, and 3128. You can create up to 512 classifiers and 1024 matching conditions.
- Policy—Combines the application definition and classifier into a single policy. This policy also determines what optimization and acceleration features (if any) a WAAS device applies to the defined traffic. You can create up to 512 policies. A policy can also contain a DSCP marking value that is applied to the traffic and that overrides a DSCP value set at the application or global level.

You can use the WAAS Central Manager GUI to modify the predefined policies and to create additional policies for other applications. For more information on creating application policies, see the "Creating a New Traffic Application Policy" section on page 12-29. For more information on viewing reports, restoring policies, monitoring applications, and other functions, see the "Managing Application Acceleration" section on page 12-37.

Note All application definitions configured in the WAAS Central Manager are globally applied to all WAAS devices that register with the WAAS Central Manager, regardless of the device group membership configuration.

Enabling and Disabling the Global Optimization Features

The global optimization features determine if TFO Optimization, Data Redundancy Elimination (DRE), and Persistent Compression are enabled on a device or device group. By default, all of these features are enabled. If you choose to disable one of these features, the device will be unable to apply the full WAAS optimization techniques to the traffic that it intercepts.

In addition, the global optimization features include each of the following application accelerators: EPM, CIFS, HTTP MAPI, NFS, SSL, and video. By default, all of the application accelerators are enabled. The application accelerators also require specific licenses to operate. For information on installing licenses, see the "Managing Software Licenses" section on page 9-3.

You must enable the accelerator on both of the peer WAEs at either end of a WAN link for all application accelerators to operate.

To enable or disable a global optimization feature, follow these steps:

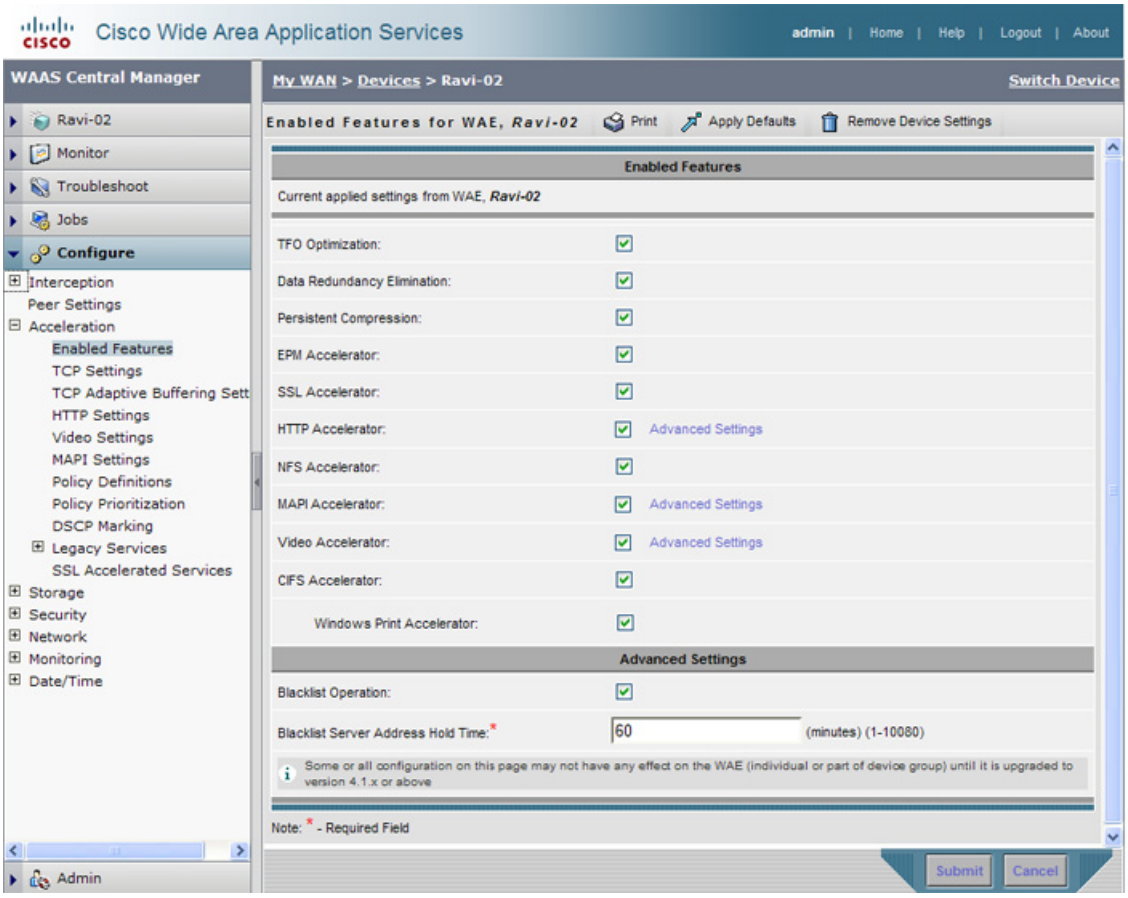
Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to change the global optimization features.

Step 3 From the navigation pane, choose **Configure > Acceleration > Enabled Features**.

The Enabled Features window appears. (See Figure 12-1.) For WAAS Express devices, the only features available are TFO Optimization, Data Redundancy Elimination (on most WAAS Express devices), and Persistent Compression. If you try to enable DRE on a WAAS Express device on which it is not supported, a message tells you that it is not supported.

Figure 12-1 Modifying the Global Optimization Features



Step 4 Place a check next to the optimization features that you want to enable, and uncheck the features that you want to disable. For a description of each of the optimization features, see the "Key Services of Cisco WAAS" section on page 1-4.

Step 5 If you check the HTTP Accelerator check box, you can click the Advanced Settings link as a shortcut to the HTTP Acceleration Configuration window. For more information, see the "Configuring HTTP Acceleration" section on page 12-5.

Step 6 If you check the Video Accelerator check box, you can click the Advanced Settings link as a shortcut to the Video Acceleration Configuration window. For more information, see the "Configuring Video Acceleration" section on page 12-9.

Step 7 If you check the MAPI Accelerator check box, you can click the Advanced Settings link as a shortcut to the MAPI Acceleration Configuration window. For more information, see the "Configuring MAPI Acceleration" section on page 12-8.

Step 8 If you check the CIFS Accelerator check box, you have the following option:

- Windows Print Accelerator—Check this box to accelerate print traffic between clients and a Windows print server. This accelerator is enabled by default when you enable the CIFS accelerator.

Note If you are changing from WAFS legacy mode to the CIFS accelerator, you must disable the WAFS legacy mode before you can enable the CIFS accelerator. To disable WAFS legacy mode, you must disable Data Center and Branch file services. For WAFS configuration information, see Chapter 11, "Configuring Wide Area File Services."

Note Do not disable Windows Print Acceleration during a client session as this can interfere with the client's use of print services. If you must disable Windows Print Acceleration, disconnect and then reestablish the client session.

Step 9 In the Advanced Settings area, uncheck the Blacklist Operation feature if you want to disable it. This feature allows a WAE to better handle situations in which TCP setup packets that have options are blocked or not returned to the WAE device. This behavior can result from network devices (such as firewalls) that block TCP setup packets that have options, and from asymmetric routes. The WAE can keep track of origin servers (such as those behind firewalls) that cannot receive optioned TCP packets and learns not to send out TCP packets with options to these blacklisted servers. WAAS is still able to accelerate traffic between branch and data center WAEs in situations where optioned TCP packets are dropped. We recommend leaving this feature enabled.

Step 10 If you want to change the default Blacklist Server Address Hold Time of 60 minutes, enter the new time in minutes in the Blacklist Server Address Hold Time field. The valid range is 1 minute to 10080 minutes (1 week).

When a server IP address is added to the blacklist, it remains there for configured hold time. After that time, subsequent connection attempts will again include TCP options so that the WAE can redetermine if the server can receive them. It is useful to retry sending TCP options periodically because network packet loss may cause a server to be erroneously blacklisted.

You can shorten or lengthen the blacklist time by changing the Blacklist Server Address Hold Time field.

Step 11 Click **Submit**.

The changes are saved to the device or device group.

To configure TFO optimization, DRE, and persistent compression from the CLI, use the **tfo optimize** global configuration command.

To configure EPM acceleration from the CLI, use the **accelerator epm** global configuration command.

To configure HTTP acceleration from the CLI, use the **accelerator http** global configuration command.

To configure NFS acceleration from the CLI, use the **accelerator nfs** global configuration command.

To configure MAPI acceleration from the CLI, use the **accelerator mapi** global configuration command.

To configure video acceleration from the CLI, use the **accelerator video** global configuration command.

To configure SSL acceleration from the CLI, use the **accelerator ssl** global configuration command.

To configure CIFS acceleration from the CLI, use the **accelerator cifs** and **accelerator cifs preposition** global configuration commands.

To configure Windows print acceleration from the CLI, use the **accelerator windows-print** global configuration command.

To configure the Blacklist Operation feature from the CLI, use the **tfo auto-discovery** global configuration command.

To display status and statistics on the application accelerators from the CLI, use the **show accelerator** and **show statistics accelerator** EXEC commands. To display statistics on the Windows print accelerator, use the **show statistics windows-print requests** EXEC command.

For details on using individual application accelerators, see the following sections:

- Configuring HTTP Acceleration, page 12-5
- Configuring MAPI Acceleration, page 12-8
- Configuring Video Acceleration, page 12-9
- Configuring SSL Acceleration, page 12-11
- For CIFS: Chapter 11, "Configuring Wide Area File Services"

Configuring HTTP Acceleration

The HTTP application accelerator accelerates HTTP traffic. SSL traffic that uses HTTPS can be optimized by both SSL and HTTP optimizations.

The default Web application policy is defined to send traffic to the HTTP accelerator. The Web application policy uses the HTTP classifier, which matches traffic on ports 80, 8080, 8000, 8001, and 3128. If you expect HTTP traffic on other ports, add the other ports to the HTTP classifier.

To enable the HTTP accelerator, check the HTTP Accelerator check box in the Enabled Features window (see Figure 12-1).

To configure the HTTP acceleration settings, follow these steps:

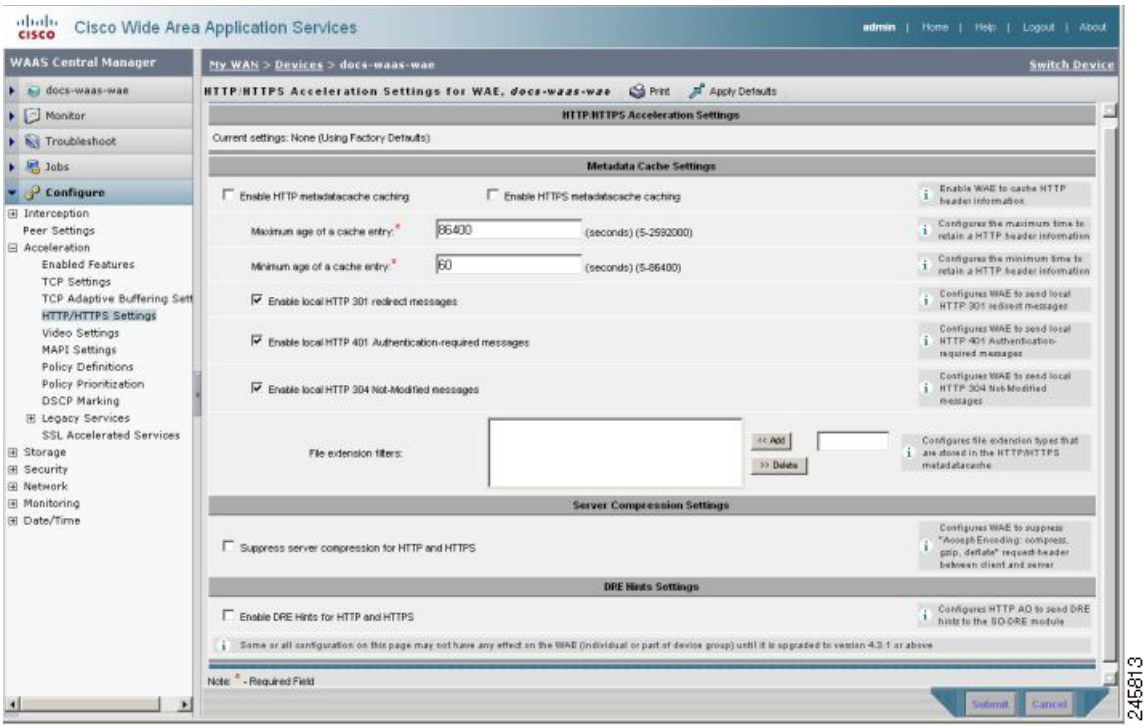
Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to change the HTTP acceleration configuration.

Step 3 From the navigation pane, choose **Configure > Acceleration > HTTP/HTTPS Settings**.

The HTTP Acceleration Settings window appears. (See Figure 12-2.)

Figure 12-2 Modifying the HTTP Acceleration Settings



Step 4 Check the **Enable HTTP metadatacache caching** check box to enable the WAE to cache HTTP header (metadata) information. The default setting is unchecked.

This box must be checked to enable any of the other settings in the Metadata Cache Settings area. If this box is not checked, no header caching is done.

For details on HTTP metadata caching, see the "About HTTP Metadata Caching" section on page 12-7.

Step 5 Check the **Enable HTTPS metadatacache caching** check box to enable the WAE to cache HTTPS header (metadata) information (HTTP as payload in SSL traffic). The default setting is unchecked.

For details on HTTP metadata caching, see the "About HTTP Metadata Caching" section on page 12-7.

Step 6 In the Maximum age of a cache entry field, enter the maximum number of seconds to retain HTTP header information in the cache. The default is 86400 seconds (24 hours). Valid time periods range from 5–2592000 seconds (30 days).

Step 7 In the Minimum age of a cache entry field, enter the minimum number of seconds to retain HTTP header information in the cache. The default is 60 seconds. Valid time periods range from 5 to 86400 seconds (24 hours).

Step 8 Check the **Enable local HTTP 301 redirect messages** check box to enable the WAE to cache and locally serve HTTP 301 messages. The default setting is checked.

Step 9 Check the **Enable local HTTP 401 Authentication-required messages** check box to enable the WAE to cache and locally serve HTTP 401 messages. The default setting is checked.

Step 10 Check the **Enable local HTTP 304 Not-Modified messages** check box to enable the WAE to cache HTTP 200 and 304 messages and locally serve HTTP 304 messages. The default setting is checked.

Step 11 To configure specific file extensions to which metadata caching is to be applied, enter the file extensions in the File extension filters field at the far right. Separate multiple extensions with a comma (for example: jpeg, gif, png) and do not include the dot at the beginning of the file extension. Click the **<< Add** button to add the entered file extensions to the active list, which is shown to the left. You can enter a maximum of 20 file extensions.

To remove an extension from the list, select it in the active list and click the **>> Delete** button.

By default, no file extension filters are defined and therefore metadata caching applies to all file types.

Step 12 Check the **Suppress server compression for HTTP and HTTPS** check box to configure the WAE to suppress server compression between the client and the server. The default setting is unchecked.

By checking this box, you are telling the WAE to remove the Accept-Encoding value from HTTP and HTTPS request headers, preventing the web server from compressing HTTP and HTTPS data that it sends to the client. This allows the WAE to apply its own compression to the HTTP and HTTPS data, typically resulting in much better compression than the web server for most files. For some file types that rarely change, such as .css and .js files, this setting is ignored and web server compression is allowed.

Step 13 Check the **Enable DRE Hints for HTTP and HTTPS** check box to send DRE hints to the DRE module for improved DRE performance. The DRE hint feature is disabled by default.

Step 14 Click **Submit**.

The changes are saved to the device or device group.

To configure HTTP acceleration from the CLI, use the **accelerator http** global configuration command.

To show the contents of the metadata cache, use the **show cache http-metadatacache** EXEC command.

To clear the metadata cache, use the **clear cache http-metadatacache** EXEC command.

About HTTP Metadata Caching

The metadata caching feature allows the HTTP accelerator in the branch WAE to cache particular server responses and respond locally to clients. The following server response messages are cached:

- HTTP 200 OK (Applies to If-None-Match and If-Modified-Since requests)
- HTTP 301 redirect
- HTTP 304 not modified (Applies to If-None-Match and If-Modified-Since requests)
- HTTP 401 authentication required

Metadata caching is not applied in the following cases:

- Requests and responses that are not compliant with RFC standards
- URLs over 255 characters
- 301 and 401 responses with cookie headers
- HEAD method is used
- Pipelined transactions

Note The metadata caching feature is introduced in WAAS version 4.2.1, but version 4.2.1 is needed only on the branch WAE. This feature can interoperate with an HTTP accelerator on a data center WAE that has a lower version.

Configuring MAPI Acceleration

The MAPI application accelerator accelerates Microsoft Outlook Exchange traffic that uses the Messaging Application Programming Interface (MAPI) protocol. Microsoft Outlook 2000–2010 clients are supported. Clients can be configured with Outlook in cached or noncached mode; both modes are accelerated.

Secure connections that use message authentication (signing) or encryption are not accelerated, and MAPI over HTTP is not accelerated.

Note Microsoft Outlook 2007 and 2010 have encryption enabled by default. You must disable encryption to benefit from the MAPI application accelerator.

The EPM application accelerator must be enabled for the MAPI application accelerator to operate. EPM is enabled by default. Additionally, the system must define an application policy of type EPM, specify the MAPI UUID, and have an Accelerate setting of MAPI. This policy, MAPI for the Email-and-Messaging application, is defined by default.

EPM traffic, such as MAPI, does not normally use a predefined port. If your Outlook administrator has configured Outlook in a nonstandard way to use a static port, you must create a new basic application policy that accelerates MAPI traffic with a classifier that matches the static port that was configured for Outlook.

Note If the WAE becomes overloaded with connections, the MAPI application accelerator continues to accelerate MAPI connections by using internally reserved connection resources. If the reserved resources are also exceeded, new MAPI connections are passed through until connection resources become available.

To enable the MAPI accelerator, check the MAPI Accelerator check box in the Enabled Features window (see Figure 12-1).

To configure MAPI acceleration settings, follow these steps:

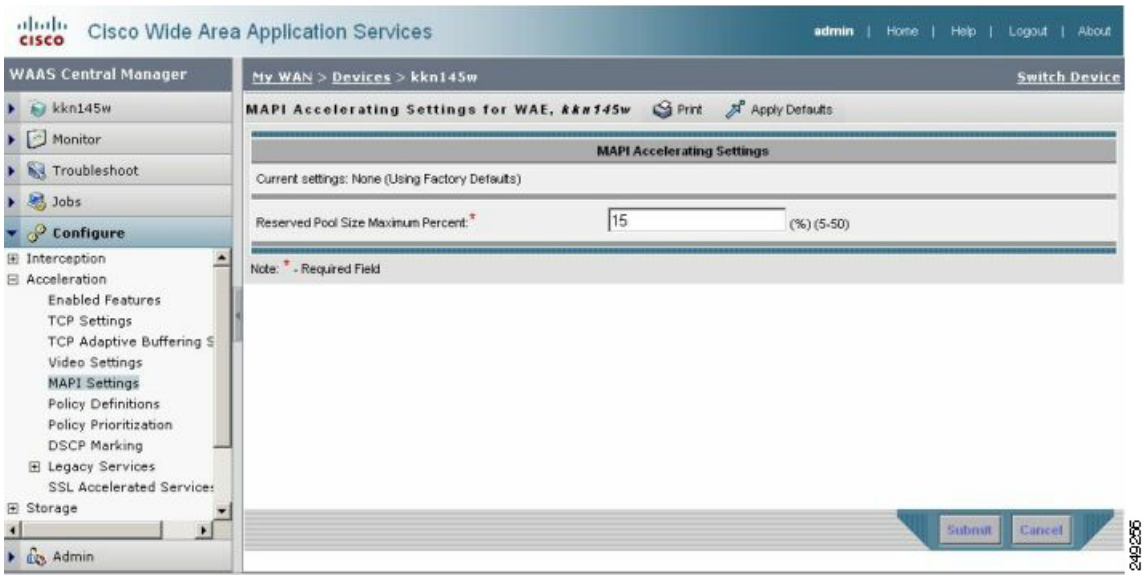
Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to change the MAPI acceleration configuration.

Step 3 From the navigation pane, choose **Configure > Acceleration > MAPI Settings**.

The MAPI Acceleration Settings window appears. (See Figure 12-3.)

Figure 12-3 Modifying MAPI Acceleration Settings



Step 4 In the **Reserved Pool Size Maximum Percent** field, enter the maximum percent of connections to restrict the maximum number of connections reserved for MAPI optimization during TFO overload. It is specified as a percent of the TFO connection limit of the platform. Valid percent ranges from 5%-50%. The default is 15%, which would reserve approximately 0.5 connection for each client-server Association Group (AG) optimized by the MAPI accelerator.

The client maintains at least one AG per server it connects to with an average of about 3 connections per AG. For deployments that observe a greater average number of connections per AG, or where TFO overload is a frequent occurrence, a higher value for reserved pool size maximum percent is recommended.

Reserved connections would remain unused when the device is not under TFO overload. Reserved connections are released when the AG terminates.

Step 5 Click **Submit**. The changes are saved to the device or device group.

Configuring Video Acceleration

The video application accelerator accelerates Windows Media live video broadcasts that use RTSP over TCP. The video accelerator automatically splits one source video stream from the WAN into multiple streams to serve multiple clients on the LAN.

The video accelerator automatically causes the client that is requesting a UDP stream to do a protocol rollover to use TCP (if both the client and server allow TCP).

The default RTSP classifier for the Streaming application policy is defined to send traffic to the video accelerator.

By default, the video accelerator sends any unaccelerated video traffic to be handled by the negotiated standard TCP optimization policy unless the video accelerator is explicitly configured to drop such traffic. You can choose to drop all unaccelerated video traffic or only traffic that is unaccelerated due to an overload condition.

To enable the video accelerator, check the Video Accelerator check box in the Enabled Features window (see Figure 12-1).

To configure the video acceleration settings, follow these steps:

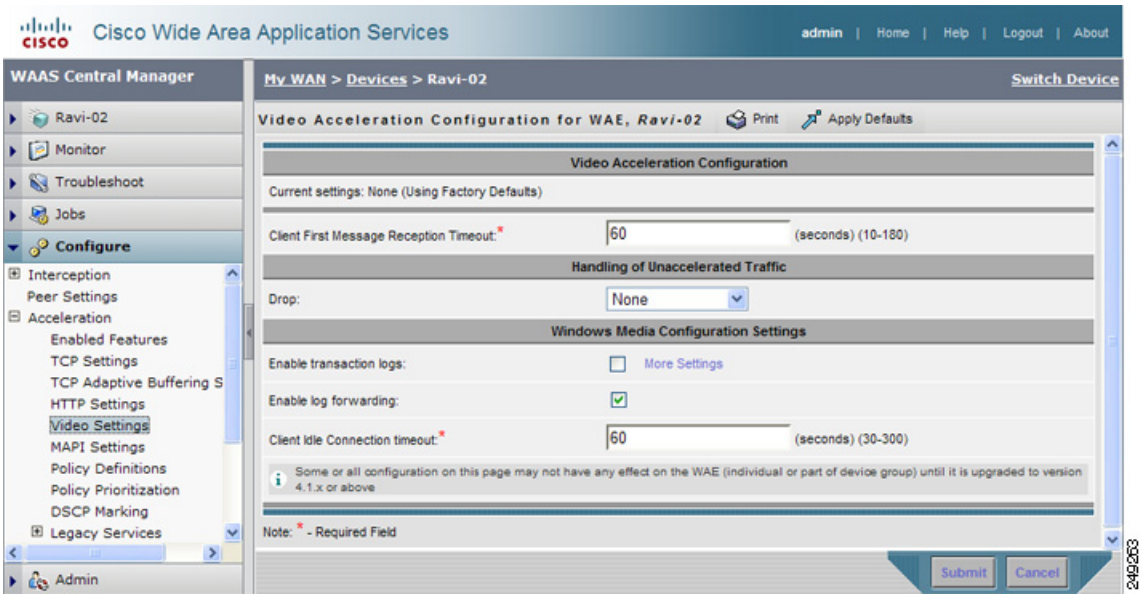
Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to change the video acceleration configuration.

Step 3 From the navigation pane, choose **Configure > Acceleration > Video Settings**.

The Video Acceleration Configuration window appears. (See Figure 12-4.)

Figure 12-4 Modifying the Video Acceleration Configuration



Step 4 In the Client First Message Reception Timeout field, enter the number of seconds to wait for the first message from the client and the first response from the server, after the connection is accepted by the video accelerator, before timing out the connection. Valid values range from 10–180 seconds. The default is 60.

Step 5 In the drop-down list, choose which unaccelerated video traffic to drop, as follows:

- **All**—Drop all video traffic that is not being accelerated due to an unsupported transport or format, or overload. All Windows Media video-on-demand traffic and all non-Windows Media RTSP traffic is dropped.
- **Overload Only**—Drop all video traffic that is not being accelerated due to an accelerator overload only.
- **None**—Handle unaccelerated video connections with the negotiated TCP optimization policy. (The traffic is not dropped.)

Note Under some conditions, the video accelerator is not registered with the policy engine, such as when there is no valid license or in certain error conditions. If you configure the video accelerator to drop all unaccelerated video traffic, the policy engine drops all video traffic (even traffic that would have been accelerated if the video accelerator had been properly registered with the policy engine).

Step 6 Check the **Enable transaction logs** check box to enable transaction logging. This feature will generate a large amount of logging data. This box is unchecked by default. Click the **More Settings** link to go to the Windows Media Transaction Log Settings configuration page.

Step 7 Check the **Enable log forwarding** check box to enable forwarding of Windows Media logs to the upstream Windows Media Server. This box is checked by default.

Step 8 In the **Client Idle Connection timeout** field, enter the maximum number of seconds to wait after the initial client request, while the client connection is idle, before timing out the connection. Valid values range from 30–300 seconds. The default is 60.

Step 9 Click **Submit**.

The changes are saved to the device or device group.

To configure video acceleration from the CLI, use the **accelerator video** global configuration command.

Configuring SSL Acceleration

The SSL application accelerator optimizes traffic on Secure Sockets Layer (SSL) encrypted connections. If SSL acceleration is not enabled, the WAAS software DRE optimizations are not very effective on SSL encrypted traffic. The SSL application acceleration enables WAAS to decrypt and apply optimizations while maintaining the security of the connection.

Note The SSL accelerator does not optimize protocols that do not start their SSL/TLS handshake from the very first byte. The only exception is HTTPS going through a proxy (where the HTTP accelerator detects the start of SSL/TLS). In this case, both HTTP and SSL accelerators optimize the connection.

The SSL application accelerator supports SSL Version 3 (SSLv3) and Transport Layer Security Version 1 (TLSv1) protocols. TLSv1.1 and TLSv1.2 protocols are not supported.

Table 12-1 provides an overview of the steps you must complete to set up and enable SSL acceleration.

Table 12-1 Checklist for Configuring SSL Acceleration

Task	Additional Information and Instructions
1. Prepare for configuring SSL acceleration.	Identifies the information that you need to gather before configuring SSL acceleration on your WAAS devices. For more information, see the "Preparing to Use SSL Acceleration" section on page 12-12.

Table 12-1 Checklist for Configuring SSL Acceleration (continued)

Task	Additional Information and Instructions
2. Enable secure store, the Enterprise License, and SSL acceleration.	Describes how to set up Central Manager secure store, how to enable the Enterprise License, and how to enable SSL acceleration. Secure store mode is required for secure handling of the SSL encryption certificates and keys. For more information, see the "Enabling Secure Store, the Enterprise License, and SSL Acceleration" section on page 12-13.
3. Enable SSL application optimization.	Describes how to activate the SSL acceleration feature. For more information, see the "Enabling and Disabling the Global Optimization Features" section on page 12-2.
4. Configure SSL acceleration settings.	(Optional) Describes how to configure the basic setup of SSL acceleration. For more information, see the "Configuring SSL Global Settings" section on page 12-14.
5. Create and manage cipher lists.	(Optional) Describes how to select and set up the cryptographic algorithms used on your WAAS devices. For more information, see the "Working with Cipher Lists" section on page 12-19.
6. Set up CA certificates.	(Optional) Describes how to select, import, and manage certificate authority (CA) certificates. For more information, see the "Working with Certificate Authorities" section on page 12-21.
7. Configure SSL management services.	(Optional) Describes how to configure the SSL connections used between the Central Manager and WAE devices. For more information, see the "Configuring SSL Management Services" section on page 12-23.
8. Configure SSL peering service.	(Optional) Describes how to configure the SSL connections used between peer WAE devices for carrying optimized SSL traffic. For more information, see the "Configuring SSL Peering Service" section on page 12-25.
9. Configure and enable SSL accelerated services.	Describes how to add, configure, and enable services to be accelerated by the SSL application optimization feature. For more information, see the "Using SSL Accelerated Services" section on page 12-26.

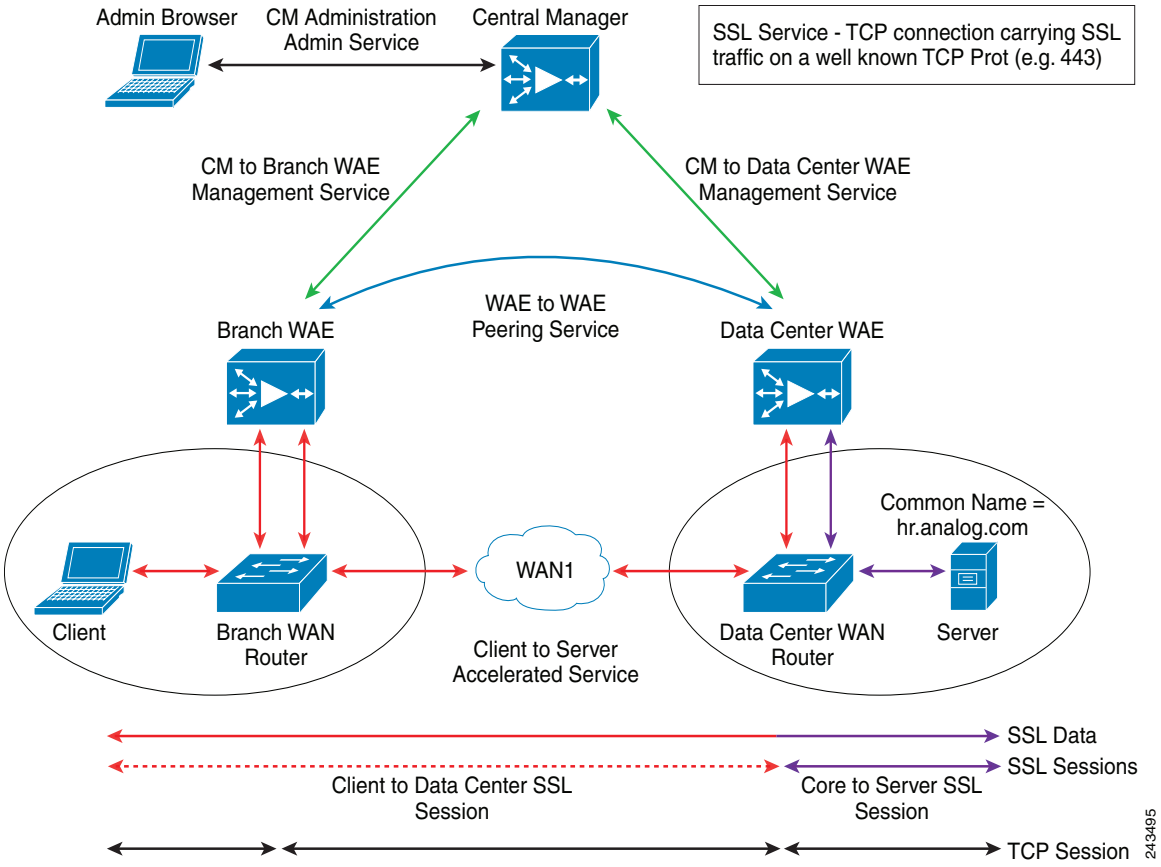
Preparing to Use SSL Acceleration

Before you configure SSL acceleration, you should know the following information:

- The services that you want to be accelerated on the SSL traffic
- The server IP address and port information
- The public key infrastructure (PKI) certificate and private key information, including the certificate common name and certificate authority signing information
- The cipher suites supported
- The SSL versions supported

Figure 12-5 shows how the WAAS software handles SSL application optimization.

Figure 12-5 SSL Acceleration Block Diagram



When you configure SSL acceleration, you must configure SSL accelerated service on the server-side (Data Center) WAE devices. The client-side (Branch) WAE needs to have its secure store initialized and unlocked/opened, but does not need to have the SSL accelerated service configured. However, the SSL accelerator must be enabled on both Data Center and Branch WAEs for SSL acceleration services to work. The WAAS Central Manager provides SSL management services and maintains the encryption certificates and keys.

Enabling Secure Store, the Enterprise License, and SSL Acceleration

Before you can use SSL acceleration on your WAAS system, you must perform the following steps:

Step 1 Enable secure store encryption on the Central Manager.

To enable secure store encryption, see the "Configuring Secure Store Settings" section on page 9-10.

Step 2 Enable the Enterprise license.

To enable the Enterprise license, see the "Managing Software Licenses" section on page 9-3.

Step 3 Enable SSL acceleration on devices.

To enable the SSL acceleration feature, see the "Enabling and Disabling the Global Optimization Features" section on page 12-2.

Note If the SSL accelerator is already running, you must wait 2 datafeed poll cycles when registering a new WAE with a Central Manager before making any configuration changes, otherwise the changes may not take effect.

Configuring SSL Global Settings

To configure the basic SSL acceleration settings, follow these steps:

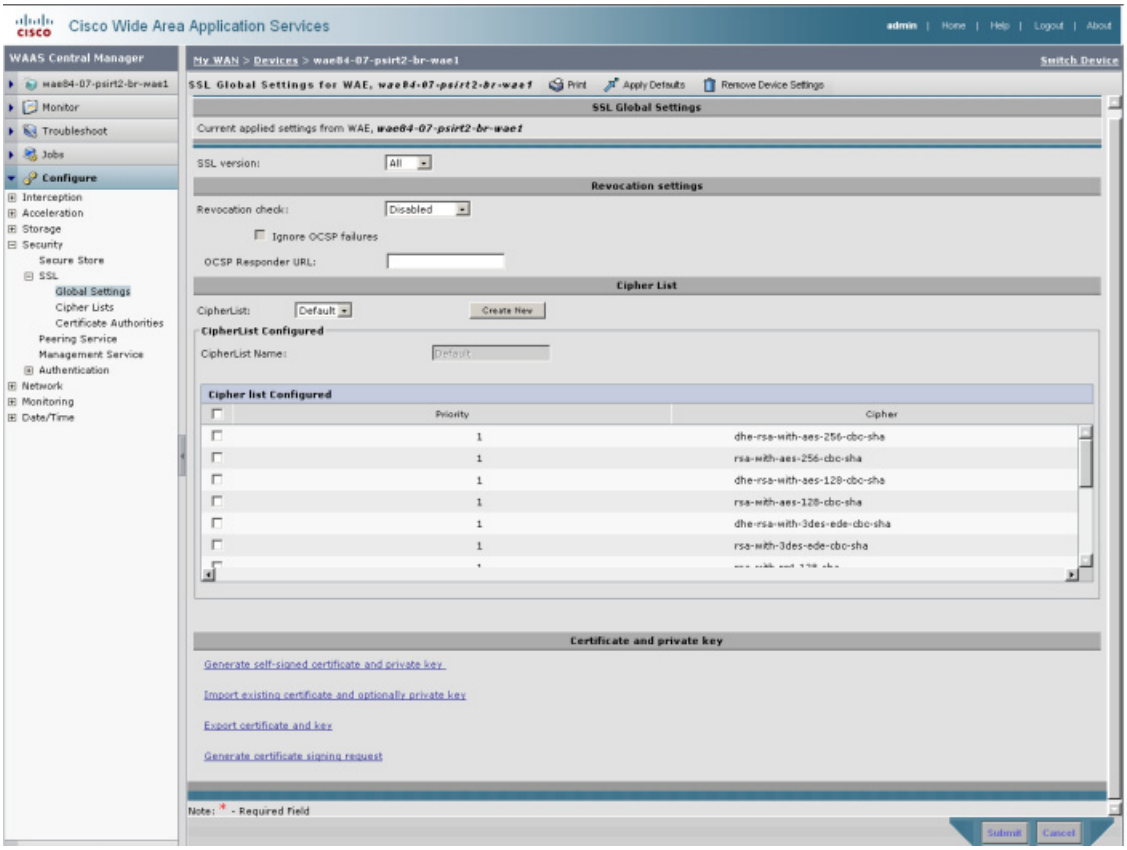
Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to configure SSL acceleration.

Step 3 From the navigation pane, choose **Configure > Security > SSL > Global Settings**.

The SSL Global Settings window appears (see Figure 12-6).

Figure 12-6 SSL Global Settings



Step 4 To configure a device to use the SSL settings from a particular device group, choose the device group from **Select a Device Group** drop-down list located in SSL global settings toolbar. A device can either use its own SSL settings, or SSL settings from a device group. However, it is not possible to configure a device to use SSL settings from multiple device groups.

Step 5 In the SSL version field, choose the type of SSL protocol to use. Choose **SSL3** for the SSL version 3 protocol, choose **TLS1** for the Transport Layer Security version 1 protocol, or choose **All** to accept both SSL3 and TLS1 SSL protocols.

Step 6 (Optional) Set the Online Certificate Status Protocol (OCSP) parameters for certificate revocation:

a. In the OCSP Revocation check drop-down list, select the OCSP revocation method.

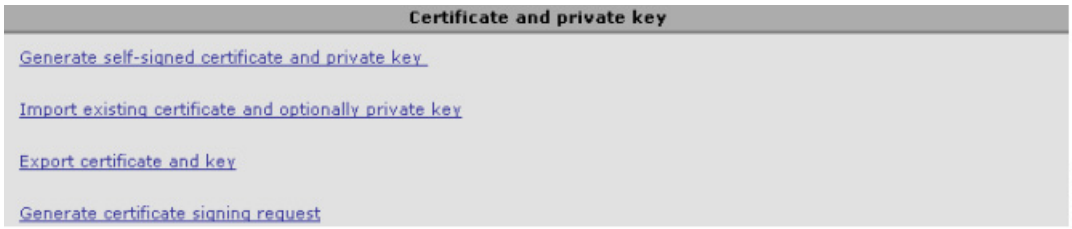
Choose **ocsp-url** SSL accelerator to use OCSP responder specified in the **OCSP Responder URL** field to check the revocation status of certificates. Choose **ocsp-cert-url** to use the OCSP responder URL specified in the Certificate Authority certificate that signed the certificate.

b. If the **Ignore OCSP failures** check box is enabled, the SSL accelerator will treat the OCSP revocation check as successful if it did not get a definite response from the OCSP responder.

Step 7 In the Cipher List field, choose a list of cipher suites to be used for SSL acceleration. For more information, see the "Working with Cipher Lists" section on page 12-19.

Step 8 Choose a certificate/key pair method (see Figure 12-7).

Figure 12-7 Configuring Service Certificate and Private Key



- Click **Generate Self-signed Certificate Key** to have the WAAS devices use a self-signed certificate/key pair for SSL.
- Click **Import Existing Certificate Key** to upload or paste an existing certificate/key pair.
- Click **Export Certificate Key** to export the current certificate/key pair.
- Click **Generate Certificate Signing Request** to renew or replace the existing certificate/key pair. The certificate signing request (CSR) is used by the Certificate Authority to generate a new certificate.

  The file that you import or export must be in either a PKCS12 format or a PEM format.

For service certificate and private key configuration steps, see the "Configuring a Service Certificate and Private Key" section on page 12-15.

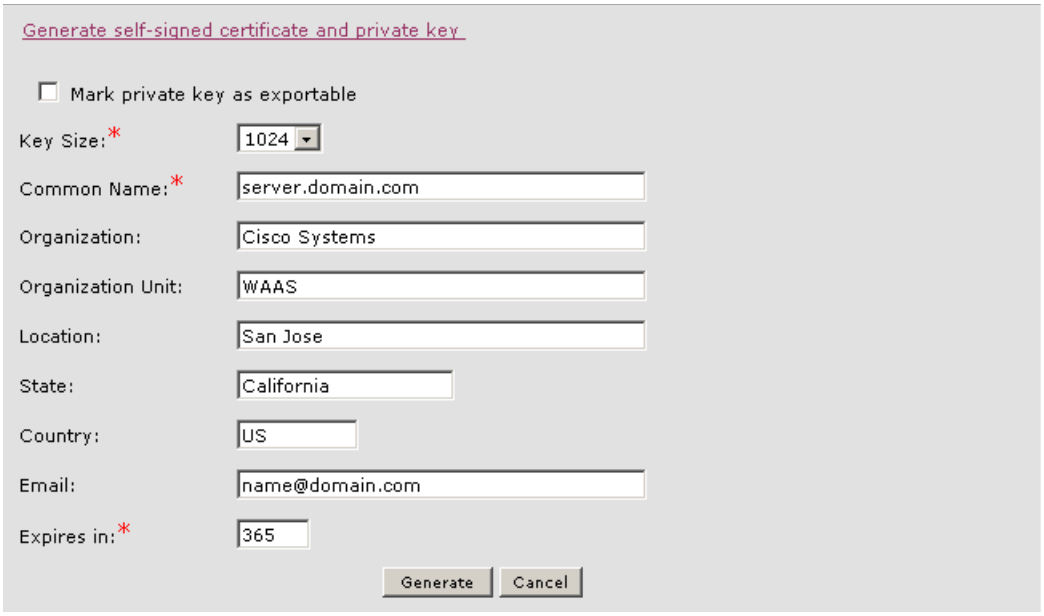
Step 9 Click **Submit**.

Configuring a Service Certificate and Private Key

To configure a service certificate and private key, follow these steps:

Step 1 To generate a self-signed certificate and private key (see Figure 12-8), follow these steps:

Figure 12-8 Self-Signed Certificate and Private Key



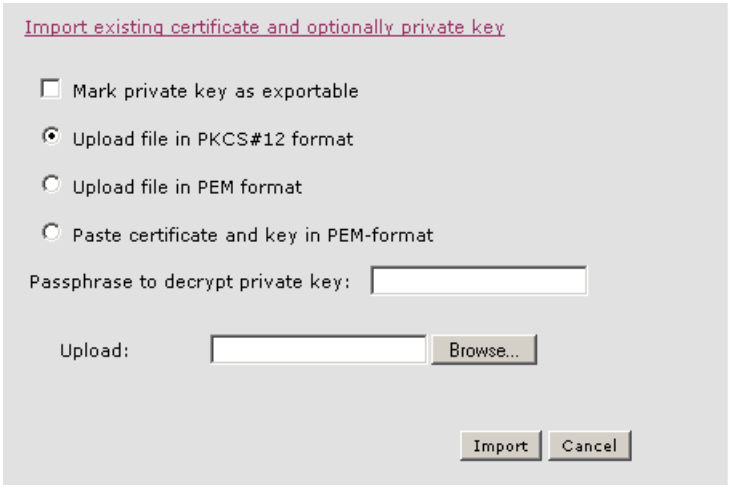
a. Check the **Mark private key as exportable** check box to export this certificate/key in the WAAS Central Manager and device CLI later.

b. Fill in the certificate and private key fields.

Step 2 To import an existing certificate or certificate chain and, optionally, private key (see Figure 12-9), follow these steps:

Note WAAS SSL feature only supports RSA signing/encryption algorithm and keys.

Figure 12-9 Importing Existing Certificate or Certificate Chain



a. Check the **Mark private key as exportable** check box to export this certificate/key in the WAAS Central Manager and device CLI later.

b. To import existing certificate or certificate chain and private key, perform one of the following:

- Upload certificate and key in PKCS#12 format (also as Microsoft PFX format)
- Upload certificate and private key in PEM format
- Paste certificate and private key PEM content

If the certificate and private key are already configured, you can update the certificate only. In this case, the Central Manager constructs the certificate and private key pair using the imported certificate and current private key. This functionality can be used to update an existing self-signed certificate to one signed by the Certificate Authority, or to update an expiring certificate.

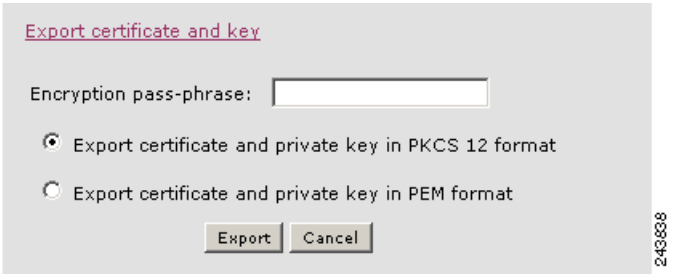
The Central Manager allows importing a certificate chain consisting of an end certificate that must be specified first, a chain of intermediate CA certificates that sign the end certificate or intermediate CA certificate, and end with a root CA.

The Central Manager validates the chain and rejects it if the validity date of the CA certificate is expired, or the signing order of certificates in the chain is not consequent.

c. Enter a pass-phrase to decrypt the private key, or leave this field empty if the private key is not encrypted.

Step 3 To export a configured certificate and private key (see Figure 12-10), follow these steps:

Figure 12-10 Export Certificate and Key



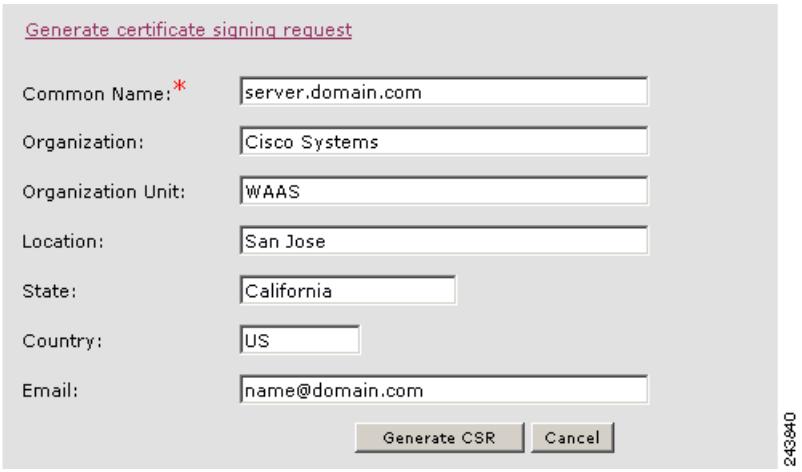
a. Enter the encryption pass-phrase.

b. Export current certificate and private key in either PKCS#12 or PEM formats. In case of PEM format both certificate and private key are included in single PEM file.

Note Central Manager will not allow exporting certificate and private key if the certificate and key were marked as non-exportable when they were generated or imported.

Step 4 To generate a certificate signing request from a current certificate and private key (see Figure 12-11), follow these steps:

Figure 12-11 Generate Certificate Signing Request



To update the current certificate with one signed by the Certificate Authority:

a. Generate PKCS#10 certificate signing request.

b. Send generated certificate signing request to Certificate Authority to generate and sign certificate.

c. Import certificate received from the Certificate Authority using the **Importing existing certificate and optionally private key** option.

Note The size of the key for a generated certificate request is the same as the size of the key in the current certificate.

Working with Cipher Lists

Cipher lists are sets of cipher suites that you can assign to your SSL acceleration configuration. A cipher suite is an SSL encryption method that includes the key exchange algorithm, the encryption algorithm, and the secure hash algorithm.

To configure a cipher list, follow these steps:

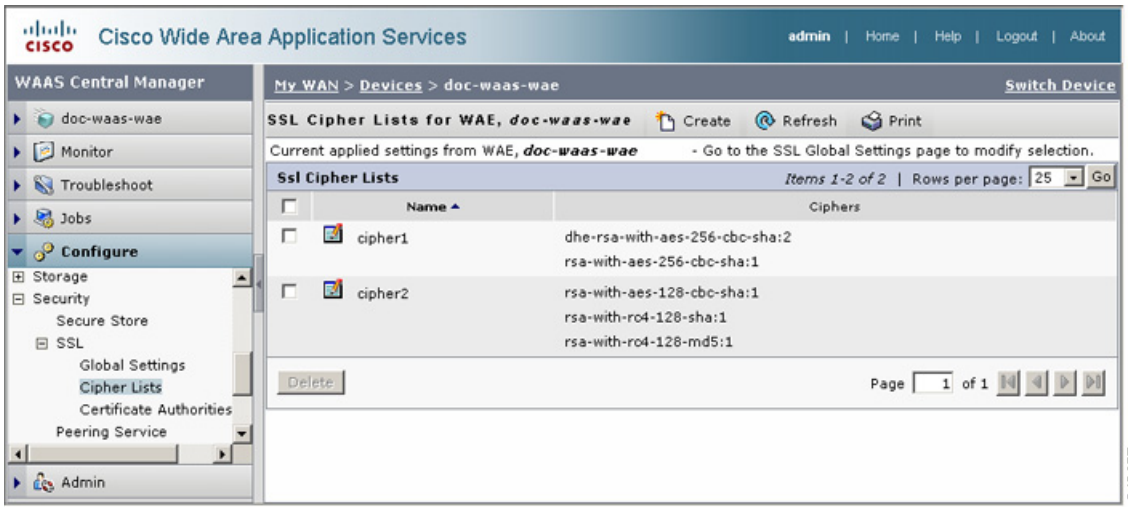
Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to configure cipher lists.

Step 3 From the navigation pane, choose **Configure > Security > SSL > Cipher Lists**.

The SSL Cipher Lists window appears (see Figure 12-12).

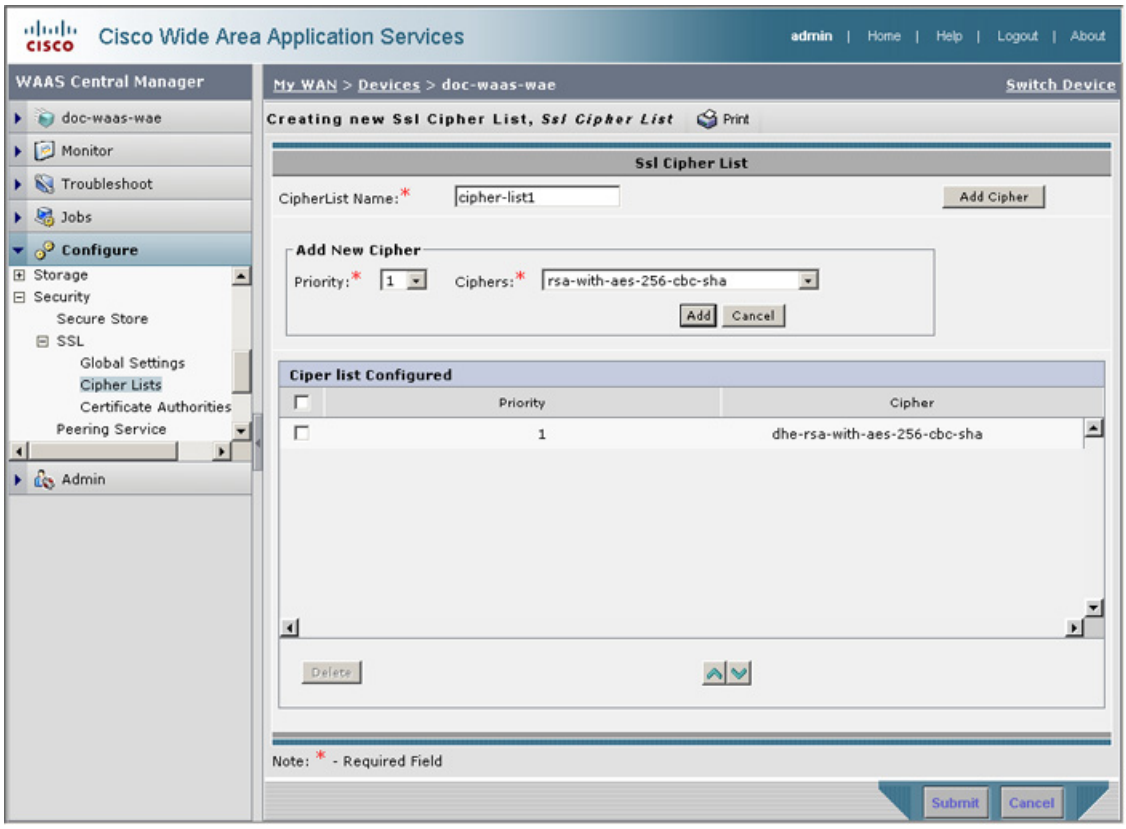
Figure 12-12 Displaying the SSL Cipher Lists



Step 4 Click **Create** to add a new cipher list.

The Creating New SSL Cipher List window appears (see Figure 12-13).

Figure 12-13 Creating a SSL Cipher List



Step 5 Type a name for your cipher list in the Cipher List Name field.

Step 6 Click **Add Cipher** to add cipher suites to your cipher list.

Step 7 Choose the cipher suite that you want to add in the Ciphers field.

Note If you are establishing an SSL connection to a Microsoft IIS server, do not select a DHE-based cipher suite.

Step 8 Choose the priority for the selected cipher suite in the Priority field.

Note When SSL peering service is configured, the priority associated with a cipher list on a core device takes precedence over the priority associated with a cipher list on an edge device.

Step 9 Click **Add** to include the selected cipher suite on your cipher list, or click **Cancel** to leave the list as it is.

Step 10 Repeat Step 6 through Step 9 to add more cipher suites to your list as desired.

Step 11 (Optional) To change the priority of a cipher suite, check the cipher suite check box and then use the up or down arrow buttons located below the cipher list to prioritize.

Note The client-specified order for ciphers overrides the cipher list priority assigned here if the cipher list is applied to an accelerated service. The priorties assigned in this cipher list are only applicable if the cipher list is applied to SSL peering and management services.

Step 12 (Optional) To remove a cipher suite from the list, check the cipher suite's box and then click **Delete**.

Step 13 Click **Submit** when you are done configuring the cipher list.

Working with Certificate Authorities

The WAAS SSL acceleration feature allows you to configure the Certificate Authority (CA) certificates used by your system. You can use one of the many well-known CA certificates that is included with WAAS or import your own CA certificate.

To manage your CA certificates, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to manage CA certificates.

Step 3 From the navigation pane, choose **Configure > Security > SSL > Certificate Authorities**.

The SSL CA Certificate List window appears (see Figure 12-14).

Figure 12-14 Displaying the SSL CA Certificate List

Step 4 Add one of the preloaded CA certificates that is included with WAAS as follows:

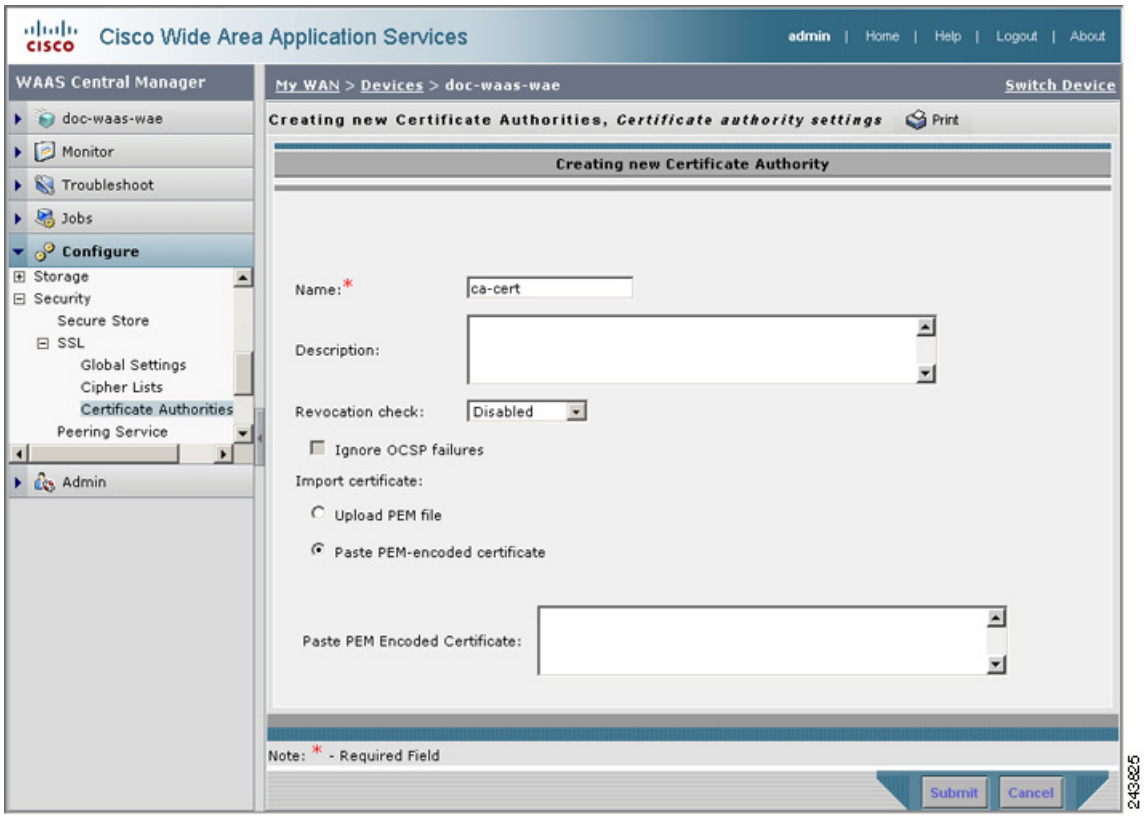
a. Click **Well-known CAs**.

b. Choose the pre-existing CA certificate you want to add and click **Import**. The CA certificate that you selected is added to the list on the SSL CA Certificate List display.

Step 5 Add your own CA certificate as follows:

a. Click **Create**. The Creating New CA Certificate window appears (see Figure 12-15).

Figure 12-15 Creating a New CA Certificate



b. Type a name for the certificate in the Certificate Name field.

c. (Optional) Type a description of the CA certificate in the Description field.

d. Choose **disabled** in the Revocation check drop-down list to disable OCSP revocation of certificates signed by this CA. Check the **Ignore OCSP failures** check box to mark revocation check successful if the OCSP revocation check failed.

e. Add the certificate information by choosing either **Upload PEM File** or **Paste PEM Encoded Certificate**.

If you are uploading a file, it must be in a Privacy Enhanced Mail (PEM) format. Browse to the file that you want to use and click **Upload**.

If you are pasting the CA certificate information, paste the text of the PEM format certificate into the Paste PEM Encoded certificate field.

f. Click **Submit** to save your changes.

Step 6 (Optional) To remove a Certificate Authority from the list, select it and then click the **Delete** icon located in the toolbar.

Step 7 Click **Submit** when you are done configuring the CA certificate list.

Configuring SSL Management Services

SSL management services are the SSL configuration parameters that affect secure communications between the Central Manager and the WAE devices (see Figure 12-5 on page 12-13). The certificate/key pairs used are unique for each WAAS device, and so SSL management services can only be configured for individual devices, not device groups.

To configure SSL management services, follow these steps:

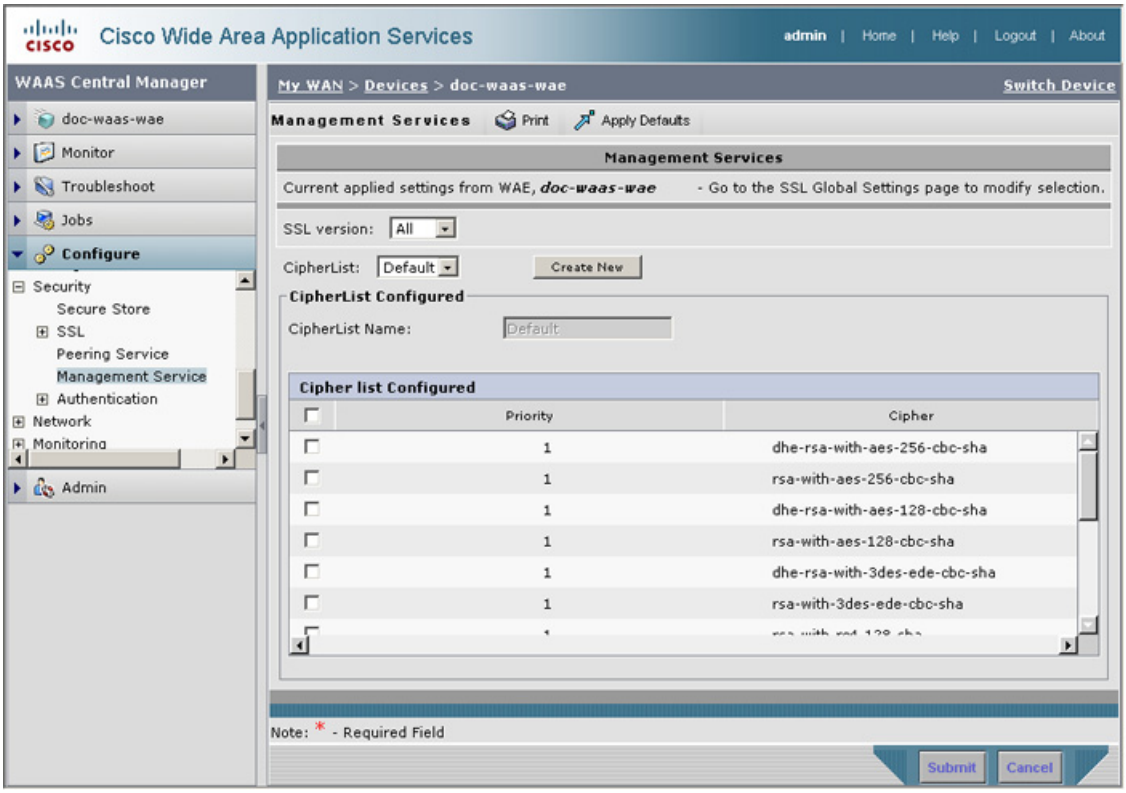
Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices**.

Step 2 Click the **Edit** icon next to the device for which you want to configure SSL management services.

Step 3 From the navigation pane, choose **Configure > Security > Management Service**.

The Management Services window appears (see Figure 12-16).

Figure 12-16 Configuring SSL Management Services



Step 4 In the SSL version field, choose the type of SSL protocol to use. Choose **SSL3** for the SSL version 3 protocol, choose **TLS1** for the Transport Layer Security version 1 protocol, or choose **All** to use both SSL3 and TLS1 SSL protocols.

Note Management service SSL version and cipher settings configured for the WAAS Central Manager are also applied to SSL connections between the WAAS Central Manager and the browser of the user.

Primary and standby Central Managers must share a common management service version or cipher list. Changing the management service version and cipher list settings may result in a loss of connectivity between primary Central Manager and standby Central Manager and WAE devices.

Table 12-2 shows the cipher lists supported with Internet Explorer and Mozilla Firefox:

Table 12-2 Cipher Lists Supported with Internet Explorer and Mozilla Firefox

Cipher	Internet Explorer	Firefox
dhe-rsa-with-aes-256-cbc-sha	Supported in IE7/Vista	Supported
rsa-with-aes-256-cbc-sha	Supported in IE7/Vista	Supported
dhe-rsa-with-aes-128-cbc-sha	Supported in IE7/Vista	Supported
rsa-with-aes-128-cbc-sha	Supported in IE7/Vista	Supported
dhe-rsa-with-3des-ede-cbc-sha	Not enabled by default	Supported
rsa-with-3des-ede-cbc-sha	Not enabled by default	Supported
rsa-with-rc4-128-sha	Supported	Supported
rsa-with-rc4-128-md5	Supported	Supported
dhe-rsa-with-des-cbc-sha	Not Supported	Not enabled by default
rsa-export1024-with-rc4-56-sha	Supported	Not enabled by default
rsa-export1024-with-des-cbc-sha	Supported	Not enabled by default
dhe-rsa-export-with-des40-cbc-sha	Not Supported	Not Supported
rsa-export-with-des40-cbc-sha	Not Supported	Not Supported
rsa-export-with-rc4-40-md5	Supported	Supported

Note Both Mozilla Firefox and Internet Explorer support SSLv3 and TLSv1 protocols, however TLSv1 may not be enabled by default. Therefore, you need to enable it in your browser.

Configuring ciphers or protocols that are not supported in your browser will result in connection loss between the browser and the Central Manager. If this occurs, configure the Central Manager management service SSL settings to the default in the CLI to restore the connection.

Some browsers, such as Internet Explorer, do not correctly handle a change of SSL version and cipher settings on the Central Manager, which can result in the browser showing an error page after submitting changes. If this occurs, reload the page.

Step 5 In the Cipher List pane, choose a list of cipher suites to be used for SSL acceleration. See the "Working with Cipher Lists" section on page 12-19 for additional information.

Configuring SSL Peering Service

SSL peering service configuration parameters control secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections (see Figure 12-5 on page 12-13). The peering service certificate and private key is unique for each WAAS device and can only be configured for individual devices, not device groups.

To configure SSL peering service, follow these steps:

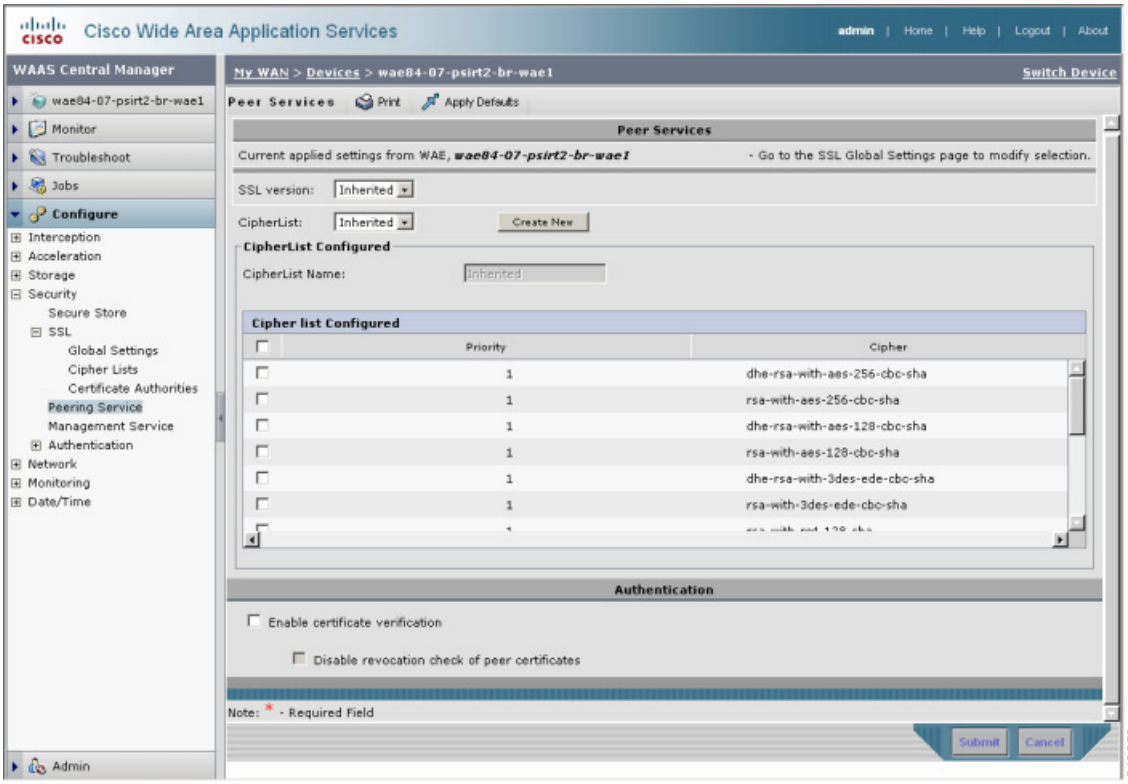
Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices**.

Step 2 Click the **Edit** icon next to the device for which you want to configure SSL peering service.

Step 3 From the navigation pane, choose **Configure > Security > Peering Service**.

The Peering Service window appears (see Figure 12-17).

Figure 12-17 Configuring SSL Peering Service



Step 4 In the SSL Version field, choose the type of SSL protocol to use, or choose **Inherited** to use the SSL protocol configured in global SSL settings. Choose **SSL3** for the SSL version 3 protocol, choose **TLS1** for the Transport Layer Security version 1 protocol, or choose **All** to use both SSL3 and TLS1 SSL protocols.

Step 5 To enable verification of peer certificates check **Enable Certificate Verification** check box. If certificate verification is enabled, WAAS devices that use self-signed certificates will not be able to establish peering connections to each other and, thus, not be able to accelerate SSL traffic.

Step 6 Check the **Disable revocation check for this service** check box to disable OCSP certificate revocation checking.

Step 7 In the Cipher List pane, choose a list of cipher suites to be used for SSL acceleration between the WAE device peers, or choose **Inherited** to use the cipher list configured in SSL global settings. See the "Working with Cipher Lists" section on page 12-19 for additional information.

Step 8 Click **Submit**.

Using SSL Accelerated Services

After you have enabled and configured SSL acceleration on your WAAS system, you must define at least one service to be accelerated on the SSL path. To configure SSL accelerated services, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

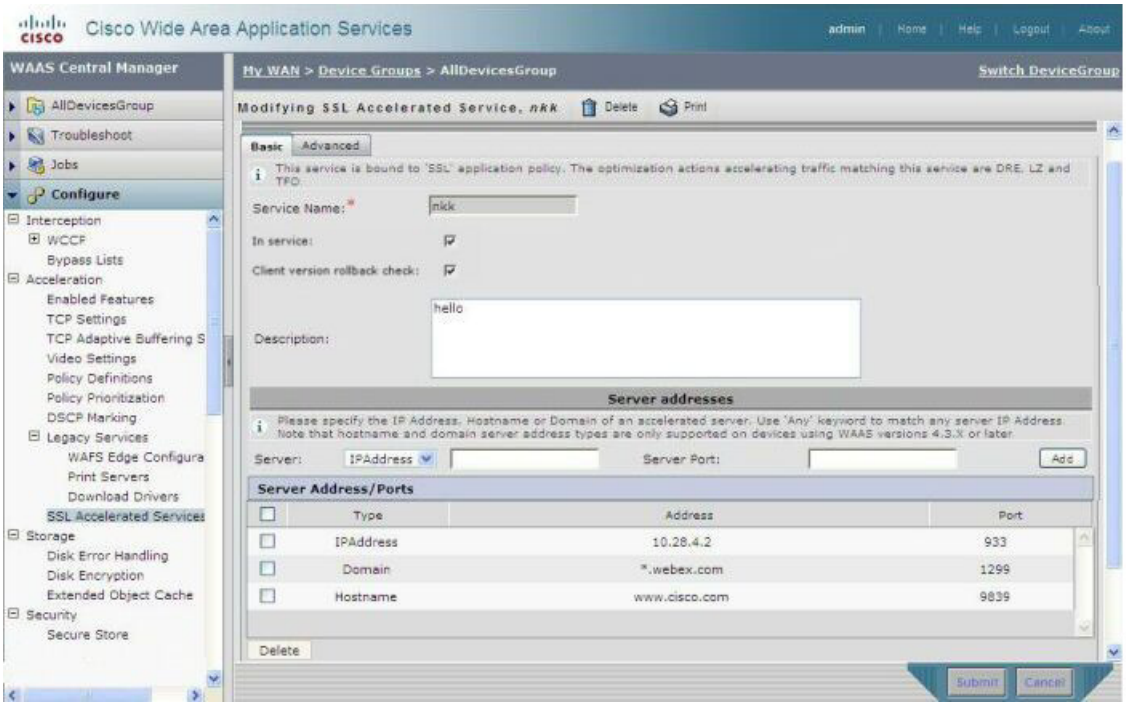
Step 2 Click the **Edit** icon next to the device or device group for which you want to define an accelerated service.

Step 3 From the navigation pane, choose **Configure > Acceleration > SSL Accelerated Services**.

Step 4 To delete an accelerated service, select the service and click **Delete**.

Step 5 Click **Create** to define a new accelerated service. A maximum of 128 accelerated services are allowed. The Basic SSL Accelerated Services Configuration window appears (see Figure 12-18).

Figure 12-18 Configuring SSL Accelerated Services—Basic



Step 6 Type a name for the service in the Service Name field.

Step 7 To enable this accelerated service, check the **In service** check box.

Step 8 To enable client version rollback check, check the **Client version rollback check** check box.

Enabling the client version rollback check does not allow connections with an incorrect client version to be optimized.

Step 9 (Optional) Type a description of the service in the Description field.

Step 10 From the Server drop-down list, choose **IP Address**, **Hostname**, or **Domain** as the SSL service endpoint type. Type the server IP address, hostname, or domain of the accelerated server. Use the keyword **Any** to specify any server IP address. A maximum of 32 IP addresses, 32 hostnames, and 32 domains are allowed.

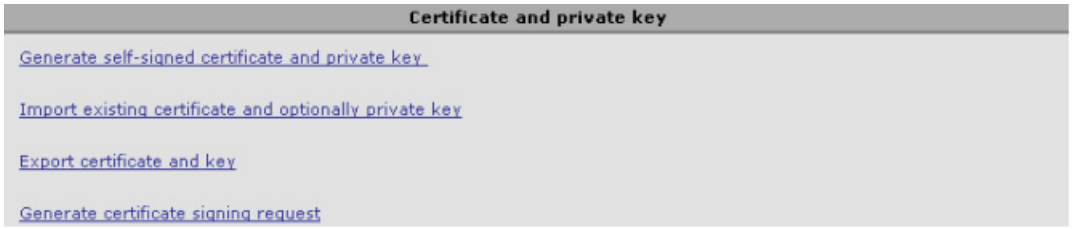
Note Hostname and domain server address types are supported only when using WAAS software version 4.2.x or later. Server IP address keyword **Any** is supported only when using WAAS Software version 4.2.x or later.

Step 11 Type the port associated with the service to be accelerated. Click **Add** to add each address. If you specify a server hostname, the Central Manager resolves the hostname to the IP address and adds it to the Server IP/Ports table.

Step 12 Click **Delete** to remove an IP address from the list.

Step 13 Choose a certificate and key pair method (see Figure 12-19).

Figure 12-19 Configuring Service Certificate and Private Key



- Click **Generate Self-signed Certificate Key** to have the WAAS devices use a self-signed certificate/key pair for SSL.
- Click **Import Existing Certificate Key** to upload or paste an existing certificate/key pair.
- Click **Export Certificate Key** to export the current certificate/key pair.
- Click **Generate Certificate Signing Request** to renew or replace the existing certificate/key pair. The certificate signing request (CSR) is used by the Certificate Authority to generate a new certificate.

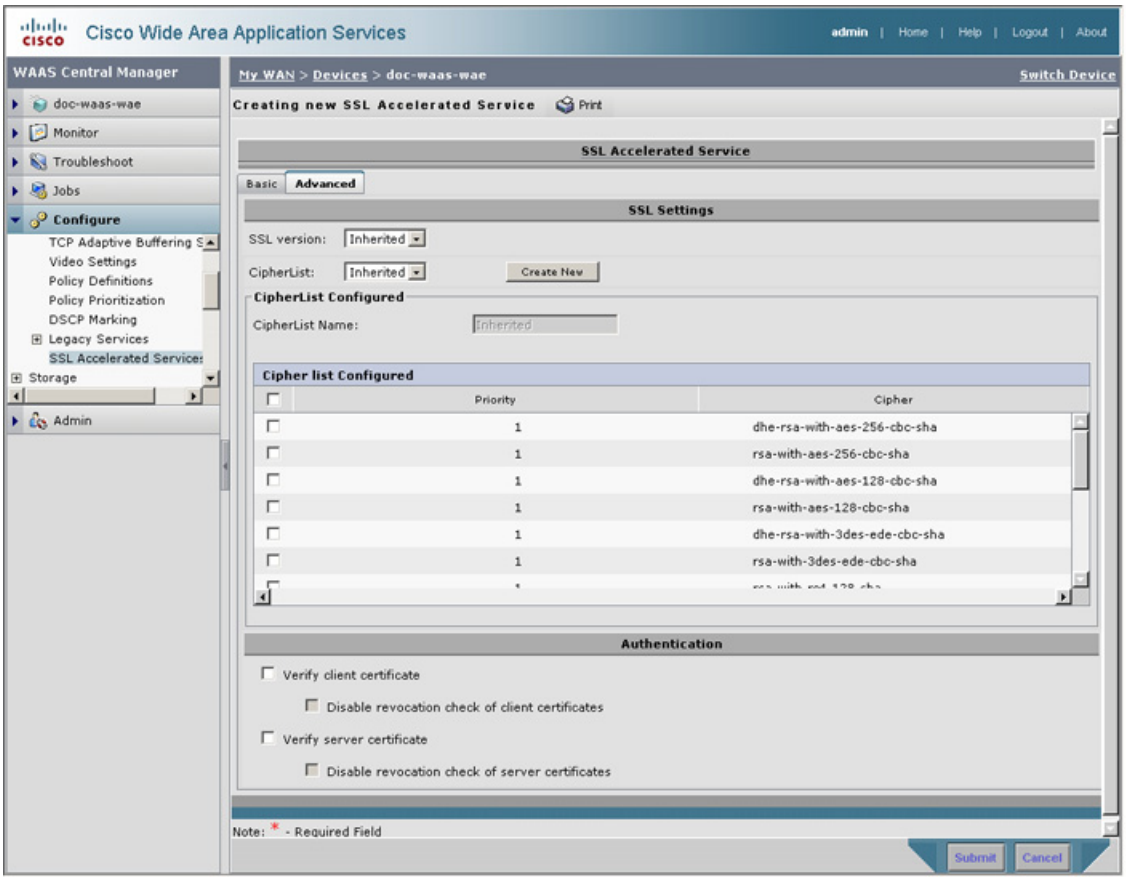
  The file that you import or export must be in either a PKCS12 format or a PEM format.

For service certificate and private key configuration steps, see the "Configuring a Service Certificate and Private Key" section on page 12-15.

Note If you change the certificate or key for an existing SSL accelerated service, you must uncheck the **In service** check box and click **Submit** to disable the service, then wait 5 minutes and check the **In service** check box and click **Submit** to reenable the service. Alternatively, at the WAE, you can use the **no inservice** SSL accelerated service configuration command, wait a few seconds, and then use the **inservice** command. If you are changing the certificate or key for multiple SSL accelerated services, you can restart all accelerated services by disabling and then reenabling the SSL accelerator.

Step 14 Click the **Advanced Settings** tab to configure SSL parameters for the service. The Advanced SSL Accelerated Services Configuration window appears (see Figure 12-20).

Figure 12-20 Configuring SSL Accelerated Services—Advanced



Step 15 (Optional) In the SSL version field, choose the type of SSL protocol to use, or choose **Inherited** to use the SSL protocol configured in global SSL settings. Choose **SSL3** for the SSL version 3 protocol, choose **TLS1** for the Transport Layer Security version 1 protocol, or choose **All** to use both SSL3 and TLS1 SSL protocols.

Step 16 (Optional) In the Cipher List field, choose a list of cipher suites to be used for SSL acceleration between the WAE device peers, or choose **Inherited** to use the cipher list configured in SSL global settings. For more information, see the "Working with Cipher Lists" section on page 12-19.

Step 17 (Optional) Set the Online Certificate Status Protocol (OCSP) parameters for certificate revocation:

a. To enable verification of client certificate check, check the **Verify client certificate** check box.

b. Check the **Disable revocation check for this service** check box to disable OCSP client certificate revocation checking.

c. To enable verification of server certificate check, check the **Verify server certificate** check box.

d. Check the **Disable revocation check for this service** check box to disable OCSP server certificate revocation checking.

Note If the server and client devices are using self-signed certificates and certificate verification is enabled, WAAS devices will not be able to accelerate SSL traffic.

Step 18 Click **Submit** when you have finished configuring the SSL accelerated service.

Creating a New Traffic Application Policy

Table 12-3 provides an overview of the steps that you must complete to create a new traffic application policy.

Table 12-3 Checklist for Creating a New Application Policy

Task	Additional Information and Instructions
1. Prepare for creating an application policy.	Provides the tasks you need to complete before creating a new application policy on your WAAS devices. For more information, see the "Preparing to Create an Application Policy" section on page 12-29.
2. Create an application definition.	Identifies general information about the application you want to optimize, such as the application name and whether the WAAS Central Manager collects statistics about this application. This step also allows you to assign the application definition to a device or device group. For more information, see the "Creating an Application Definition" section on page 12-30.
3. Create an application policy.	Determines the type of action your WAAS device or device group performs on specific application traffic. This step requires you to do the following: • Create application classifiers that allow a WAAS device to identify specific types of traffic. For example, you can create a condition that matches all traffic going to a specific IP address. • Specify the type of action your WAAS device or device group performs on the defined traffic. For example, you can specify that WAAS should apply TFO and LZ compression to all traffic for a specific application. For more information, see the "Creating an Application Policy" section on page 12-31.

Preparing to Create an Application Policy

Before you create a new application policy, complete the following preparation tasks:

- Review the list of application policies on your WAAS system and make sure that none of these policies already cover the type of traffic you want to define. To view a list of the predefined policies that come bundled with the WAAS system, see Appendix A, "Predefined Application Policies."
- Identify a match condition for the new application traffic. For example, if the application uses a specific destination or source port, you can use that port number to create a match condition. You can also use a source or destination IP address for a match condition.
- Identify the device or device group that requires the new application policy. We recommend you create application policies on device groups so the policy is consistent across multiple WAAS devices.

Creating an Application Definition

The first step in creating an application policy is to set up an application definition that identifies general information about the application, such as the application name and whether you want the WAAS Central Manager to collect statistics about the application. After creating the application definition, you assign it to a device or device group. You can create up to 255 application definitions on your WAAS system.

To create an application definition, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **Configure > Acceleration > Applications**.

The Applications window appears, which displays a list of all applications on your WAAS system. From this window, you can perform the following tasks:

- Click the **Edit** icon next to an application to modify or delete the definition.
- Determine if your WAAS system is collecting statistics on an application. The Monitor Enabled column displays Yes if statistics are being collected for the application.
- Create a new application as described in the steps that follow.

Click the **Create New Application** icon in the taskbar. The Creating Application window appears.

Step 2 Enter a name for this application.

The name cannot contain spaces and special characters.

Step 3 Check the **Enable Statistics** check box to allow the WAAS Central Manager to collect data for this application. To disable data collection for this application, uncheck this box.

The WAAS Central Manager GUI can display statistics for up to 20 applications, and an error message is displayed if you try to enable statistics for the twenty-first application. However, you can use the WAAS CLI to view statistics for all applications that have policies on a specific WAAS device. For more information, refer to the *Cisco Wide Area Application Services Command Reference*.

If you are collecting statistics for an application and decide to disable statistics collection, then reenable statistics collection at a later time, the historical data will be retained, but a gap in data will exist for the time period when statistics collection was disabled. However, if you delete an application that you are collecting statistics for, then later recreate the application, the historical data for the application will be lost. Only data since the recreation of the application will be displayed.

Note The WAAS Central Manager does not start collecting data for this application until you finish creating the entire application policy.

Step 4 (Optional) Enter a comment in the **Comments** field.

The comment you enter appears in the Applications window.

Step 5 Click **Submit**.

The application definition is saved, and options appear in the navigation pane that allow you to assign the application to a device or device group.

Step 6 From the navigation pane, click one of the following options:

- **Assign Device Groups**—Assigns the application to one or more device groups.
- **Assign Devices**—Assigns the application to one or more WAAS devices.

The Device Groups Assignments window or the WAE Assignments window is displayed depending on the selected option.

For either view, the assignments window lets you filter your view of the items in the list. Filtering enables you to find items in the list that match the criteria that you set.

Step 7 Choose the devices or device groups that you want to assign to this application. To select the devices, use one of the following procedures:

- Click  in the taskbar to assign all available WAAS devices or device groups.
- Click  next to each WAAS device or device group that you want to assign. The icon changes to  when selected. To unassign a device or device group, click the icon again.

Step 8 Click **Submit**.

The icon next to the selected devices changes to  , showing that the application has been successfully assigned to the devices.

Creating an Application Policy

After you create an application definition, you need to create an application policy that determines the action a WAAS device takes on the specified traffic. For example, you can create an application policy that makes a WAAS device apply TCP optimization and compression to all application traffic that travels over a specific port or to a specific IP address. You can create up to 512 application policies on your WAAS system.

The traffic matching rules are contained in the application classifier. These rules, known as match conditions, use Layer 2 and Layer 4 information in the TCP header to identify traffic.

To create an application policy, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

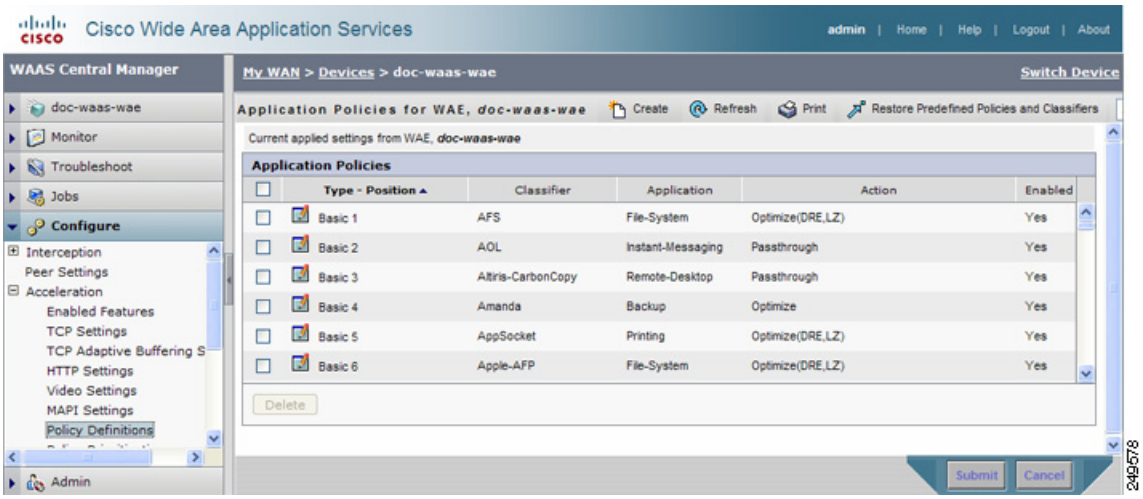
Step 2 Click the **Edit** icon next to the device or device group on which you want to create an application policy.

The Device Dashboard window or the Modifying Device Group window appears.

Step 3 From the navigation pane, choose **Configure > Acceleration > Policy Definitions**.

The Application Policies window appears. (See Figure 12-21.)

Figure 12-21 Application Policies Window



This window displays information about all application policies that reside on the selected device or device group. It shows the type of policy (Basic, WAFS transport, Port Mapper, Other, or waas_global) and the position of the policy within that type. The position determines the order in which WAAS refers to that policy when determining how to handle application traffic. To change the position of a policy, see the "Modifying the Position of an Application Policy" section on page 12-40. This window also displays the classifier, application definition, and action assigned to each policy.

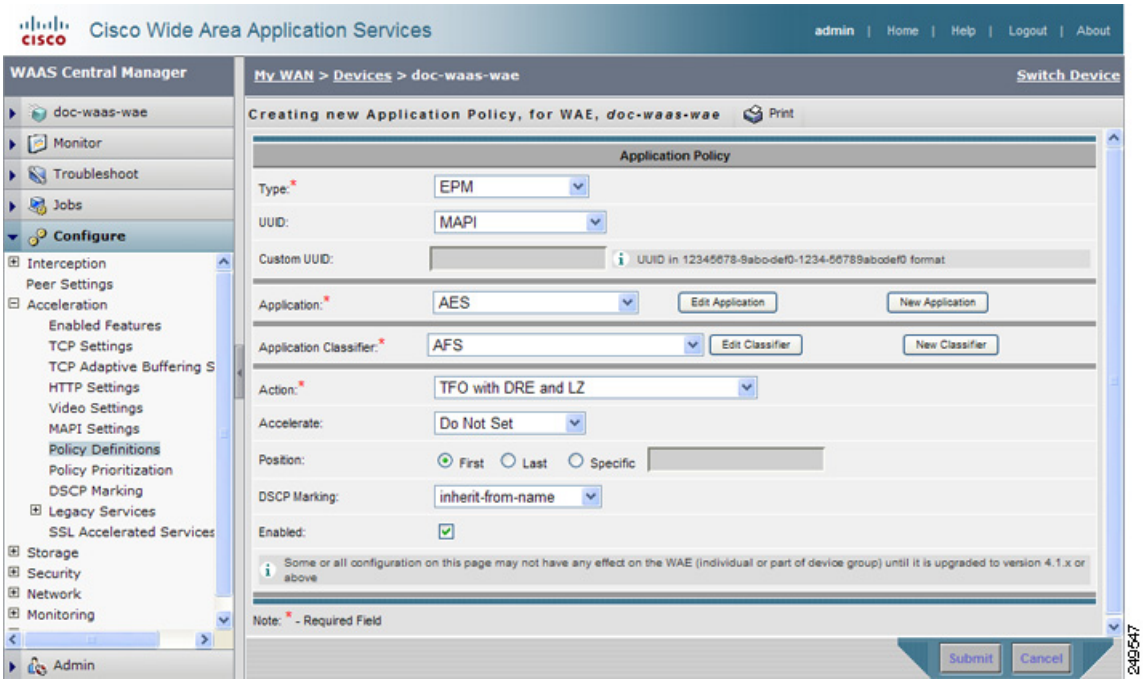
From the Application Policies window, you can perform the following tasks:

- Place a check next to one or more application policies that you want to delete, and click the **Delete** button to delete the checked policies.
- Click the **Edit** icon next to an application policy to modify or delete that policy.
- Restore predefined policies and classifiers. For more information, see the "Restoring Application Policies and Classifiers" section on page 12-38.
- Create an application policy as described in the steps that follow.

Step 4 Click the **Create New Policy** icon in the taskbar to create a new application policy.

The Creating New Application Policy window appears. (See Figure 12-22.)

Figure 12-22 Creating an Application Policy



Step 5 From the Type drop-down list, choose the type of application policy.

Table 12-4 describes the types of application policies.

Table 12-4 Application Policy Types

Option	Description
Basic	Standard type of application policy on WAAS devices. Choose this option if none of the other types apply.
waas_global	Available only on WAAS Express devices and same as the WAAS Basic policy.
WAFS Transport	When you enable wide area file services (WAFS), all CIFS traffic going between a branch WAE and a data center WAE is optimized. Choose the **WAFS Transport** option to specify another action (such as passthrough) for CIFS traffic traveling between branch and data center WAEs. For more information on enabling file services, see Chapter 11, "Configuring Wide Area File Services."
EPM	Type of policy for EPM-based applications. EndPoint Mapper (EPM) is a service that dynamically allocates server ports to certain applications. Unlike most applications that always use the same port, applications that rely on the EPM service can be assigned a different port at every request. Because EPM applications do not use a static port, you must specify the application's UUID as a way to identify the application traffic to your WAAS system. When you select the EPM option, the UUID field is enabled so that you can select a preconfigured EPM application or enter the UUID for a custom application.

Step 6 If you chose EPM for the policy type, choose one of the following EPM applications from the **UUID** drop-down list:

- **MAPI**—Uses the predefined UUID associated with the MAPI application, which is a4f1db00-ca47-1067-b31f-00dd010662da.
- **MS-SQL-RPC**—Uses the predefined UUID associated with the SQL Session Manager application, which is 3f99b900-4d87-101b-99b7-aa0004007f07.
- **MS-AD-Replication**—Uses the predefined UUID associated with the Active Directory application, which is e3514235-4b06-11d1-ab04-00c04fc2dcd2.
- **MS-FRS**—Uses the predefined UUID associated with the file replication service, which is f5cc59b4-4264-101a-8c59-08002b2f8426.
- **Custom**—Allows you to enter the UUID for a custom EPM application in the Custom UUID field.

Step 7 Specify the application that you want to be associated with this policy by doing either of the following:

- From the Application drop-down list, choose an existing application like the one that you created in the "Creating an Application Definition" section on page 12-30. This list displays all predefined and new applications on your WAAS system.

  To modify an existing application, choose the application from the drop-down list and click **Edit Application**. You can then change the application's name, add or remove comments, and enable or disable statistics collection for the application. After making the necessary changes, click **Submit** to save your changes and return to the Application Policy window.

- Click **New Application** to create an application. You can specify the application name, enable statistics collection, and specify the DSCP marking value (except on WAAS Express devices). For the DSCP marking, you can choose to use the global default values (see the "Defining Default DSCP Marking Values" section on page 12-39) or select one of the other defined values. See Table 11-4 on page 11-16 for a description of the supported DSCP marking values. In addition to the values listed in Table 11-4, you can choose copy, which copies the DSCP value from the incoming packet and uses it for the outgoing packet. After specifying the application details, click **Submit** to save the new application and return to the Application Policy window. The new application is automatically assigned to this device or device group.

Step 8 Choose the classifier from the Application Classifier drop-down list to select an existing classifier for this policy.

To modify an existing classifier, select the classifier from the drop-down list and click **Edit Classifier**. You can then change classifier's name, add or remove comments, create a new match condition, or edit the existing match condition. After making the necessary changes, click **Submit** to save your changes and return to the Application Policy window.

Step 9 Click **New Classifier** to create a new classifier for this policy.

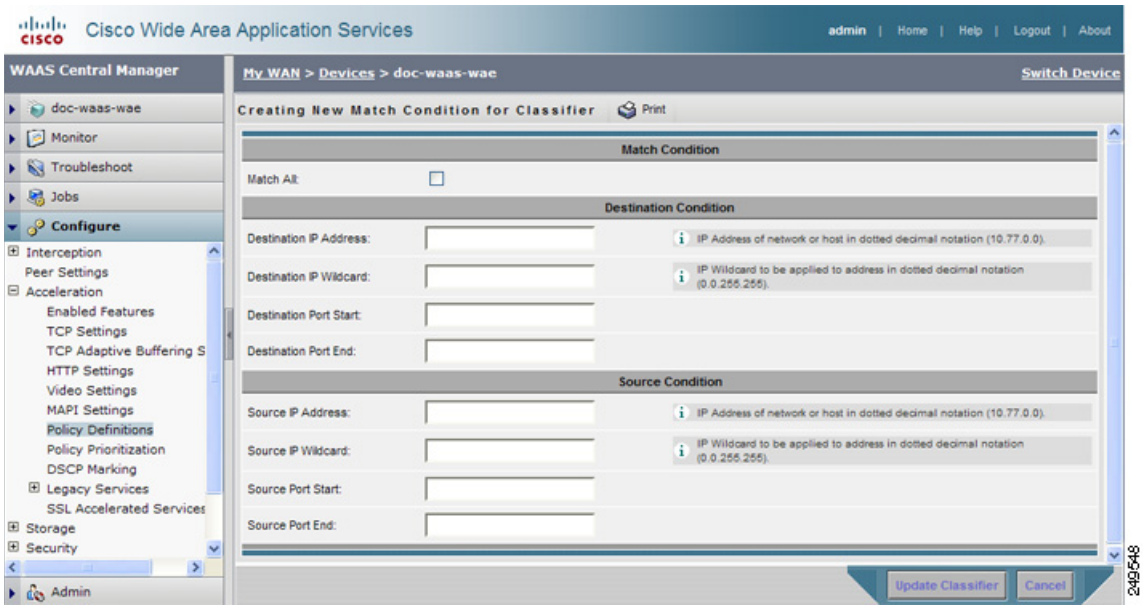
The Creating New Application Classifier window then appears so that you can create a new classifier. Complete the following steps to create a new classifier:

a. Enter a name for this application classifier. The name cannot contain spaces or special characters.

b. (Optional) Enter a comment that will appear on the Application Policies window shown in Figure 12-21 on page 12-32.

c. In the Configure Match Conditions section, click the **Create New Match Condition** icon. (If you get a dialog box asking if you want to navigate away from the page, click **OK**.) The Creating New Match Condition window appears. (See Figure 12-23.)

Figure 12-23 Creating a New Match Condition



d. Check the **Match All** check box to create a condition that matches all traffic. Checking the Match All check box automatically disables all other fields in the window.

e. Enter a value in one of the destination or source condition fields to create a condition for a specific type of traffic.

For example, to match all traffic going to IP address 10.10.10.2, enter that IP address in the Destination IP Address field.

Note To specify a range of IP addresses, enter a wildcard subnet mask in either the destination or source IP Wildcard field.

f. Click **Update Classifier**. You return to the Creating New Application Classifier window. The new match condition appears at the bottom of this window.

g. Click **Submit**. You return to the Creating New Application Policy window.

Step 10 From the Action drop-down list, choose the action that your WAAS device should take on the defined traffic. Table 12-5 describes each action.

Table 12-5 Action Descriptions

Action	Description
Passthrough	Prevents the WAAS device from optimizing the application traffic defined in this policy by using TFO, DRE, or compression. Traffic that matches this policy can still be accelerated if an accelerator is chosen from the Accelerate drop-down list.
TFO Only	Applies a variety of transport flow optimization (TFO) techniques to matching traffic. TFO techniques include BIC-TCP, window size maximization and scaling, and selective acknowledgement. For a more detailed description of the TFO features, see the "TFO Optimization" section on page 1-4.
TFO with Data Redundancy Elimination	Applies both TFO and data redundancy elimination (DRE) to matching traffic. DRE removes redundant information before sending the shortened data stream over the WAN. DRE operates on large data streams (tens to hundreds of bytes or more).
TFO with LZ Compression	Applies both TFO and the LZ compression algorithm to matching traffic. LZ compression functions similarly to DRE but uses a different compression algorithm to compress smaller data streams and maintains a limited compression history.
TFO with DRE and LZ	Applies TFO, DRE, and LZ compression to matching traffic.

Step 11 From the Accelerate drop-down list, choose one of the following additional acceleration actions that your WAAS device should take on the defined traffic:

- **Do Not Set**—No additional acceleration is done.
- **MS Port Mapper**—Accelerate using the Microsoft Endpoint Port Mapper (EPM).
- **CIFS**—Accelerate using the CIFS Accelerator.
- **HTTP**—Accelerate using the HTTP Accelerator.
- **NFS** —Accelerate using the NFS Accelerator.
- **MAPI**—Accelerate using the MAPI Accelerator.
- **VIDEO** —Accelerate using the Video Accelerator.

For WAAS Express devices, the Accelerate drop-down list is not shown.

Step 12 Choose one of the following positions for this application policy by click the appropriate Position radio button:

- **First**—Places this policy at the top of the position list so that the WAAS device tries to classify traffic using this policy before moving onto the second policy in the list. If you already have a policy in the first position, that policy moves down to number two in the list.
- **Last**—Places this policy at the bottom of the position list, making it the last policy that the WAAS device uses to classify traffic. If you already have a policy in the last position, that policy becomes the second to last in the list.

  If a device goes through all the policies in the list without making a match, then the WAAS device passes through the traffic unoptimized.
- **Specific**—Allows you to enter a specific position for this policy. If you already have a policy in the specified position, that policy moves down one in the list.

Step 13 (Optional) Choose a value from the DSCP Marking drop-down list and see Table 11-4 on page 11-16 for a description of the supported values. In addition to the values listed in Table 11-4, you can choose copy, which copies the DSCP value from the incoming packet and uses it for the outgoing packet. If you choose inherit-from-name from the drop-down list, the DSCP value defined at the application or global level is used.

DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. Levels of service are assigned by marking each packet on the network with a DSCP code and associating a corresponding level of service. DSCP is the combination of IP Precedence and Type of Service (ToS) fields. For more information, see RFC 2474.

DSCP marking does not apply to pass-through traffic.

For WAAS Express devices, the DSCP Marking drop-down list is not shown.

The DSCP value set at the application level applies to all classifiers associated with the application. If you set a DSCP value in a policy, it overrides the DSCP value set at the application or global level.

Step 14 Check the **Enabled** check box to activate this policy. To disable this policy, uncheck this box. For WAAS Express devices, this check box is not shown.

Step 15 Click **Submit**.

The new policy appears in the Application Policies window. (See Figure 12-21 on page 12-32.)

Managing Application Acceleration

This section contains the following topics:

- Viewing a List of Applications, page 12-37
- Viewing a Policy Report, page 12-38
- Viewing a Classifier Report, page 12-38
- Restoring Application Policies and Classifiers, page 12-38
- Monitoring Applications, page 12-39
- Defining Default DSCP Marking Values, page 12-39
- Modifying the Position of an Application Policy, page 12-40
- Modifying the Acceleration TCP Settings, page 12-41

Viewing a List of Applications

To view a list of applications that reside on a WAE device or device group, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group on which you want to view applications.

Step 3 From the navigation pane, choose **Configure > Acceleration > Policy Definitions**. The Application Policies window appears.

Step 4 Click the Application column header to sort the column by application name so you can more easily locate a specific application.

You can click the **Edit** icon next to an application to edit the application policy.

If you determine that one or more policies are not needed, check the box next to each unneeded application and click the **Delete** button below the list.

If you determine that a new policy is needed, click the **Create New Policy** taskbar icon to create the policy (see the "Creating an Application Policy" section on page 12-31).

Viewing a Policy Report

To view a report of the policies that reside on each WAE device or device group, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **Configure > Acceleration > Policies**.

The policy report appears. It lists each device or device group and the number of active policies on the device or device group.

Step 2 Click the **Edit** icon next to a device or group to see the application policies that are defined on it.

Viewing a Classifier Report

To view a report of the classifiers that reside on each WAE device or device group, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **Configure > Acceleration > Classifiers**.

The classifier report appears. It lists each classifier that is defined, and the number of devices on which it is configured.

Step 2 Click the **View** icon next to a classifier to see a report of the devices and device groups on which the classifier is configured.

Step 3 Click the **Edit** icon next to a device or group to see the application policies that are defined on it.

Restoring Application Policies and Classifiers

The WAAS system allows you to restore the predefined policies and classifiers that shipped with the WAAS system. For a list of the predefined policies, see Appendix A, "Predefined Application Policies."

If you made changes to the predefined policies that have negatively impacted how a WAAS device handles application traffic, you can override your changes by restoring the predefined policy settings.

To restore predefined policies and classifiers, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or group on which you want to restore policies.

Step 3 From the navigation pane, choose **Configure > Acceleration > Policy Definitions**.

The Application Policies window appears.

Step 4 Click the **Restore Predefined Policies and Classifiers** taskbar icon to restore over 150 policies and classifiers that shipped with the WAAS software and remove any new policies that were created on the system. If a predefined policy has been changed, these changes are lost and the original settings are restored.

Monitoring Applications

After you create an application policy, you should monitor the associated application to make sure your WAAS system is handling the application traffic as expected. To monitor an application, you must have enabled statistics collection for that application, as described in the "Creating an Application Definition" section on page 12-30.

You can use the Traffic Optimization report to monitor a specific application. For more information, see the "Optimization Summary Report" section on page 16-46.

Defining Default DSCP Marking Values

According to policies that you define in an application definition and an application policy, the WAAS software allows you to set a DSCP value on packets that it processes.

A DSCP value is a field in an IP packet that enables different levels of service to be assigned to the network traffic. The levels of service are assigned by marking each packet on the network with a DSCP code and associating a corresponding level of service. The DSCP marking determines how packets for a connection are processed externally to WAAS. DSCP is the combination of IP Precedence and Type of Service (ToS) fields. For more information, see RFC 2474. DSCP values are predefined and cannot be changed.

This attribute can be defined at the following levels:

- Global—You can define global defaults for the DSCP value. This value applies to the traffic if a lower level value is not defined.
- Application—You can define the DSCP value in an application definition at the device or device group level but not at the global application definition level. This value applies to all traffic associated with the application on a particular device or device group and overrides the global default.
- Policy—You can define the DSCP value in an application policy. This value applies only to traffic that matches the classifiers defined in the policy and overrides the application or global DSCP value.

This section contains the following topic:

- Defining the Default DSCP Marking Value, page 12-39

Defining the Default DSCP Marking Value

To define the global default DSCP marking value, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or group where you want to define the default DSCP marking value.

Step 3 From the navigation pane, choose **Configure > Acceleration > DSCP Marking**. The Global DSCP Settings window appears.

Step 4 Choose a value from the Global Default DSCP Marking drop-down list and see Table 11-4 on page 11-16 for a description of the supported values. In addition to the values listed in Table 11-4, the default setting is copy, which copies the DSCP value from the incoming packet and uses it for the outgoing packet.

Step 5 Click **Submit** to save the settings.

Modifying the Position of an Application Policy

Each application policy has an assigned position that determines the order in which a WAAS device refers to the policy in an attempt to classify traffic. For example, when a WAAS device intercepts traffic, it refers to the first policy in the list to try to match the traffic to an application. If the first policy does not provide a match, the WAAS device moves on to the next policy in the list.

For information on how to assign a position to a new policy, see the "Creating an Application Policy" section on page 12-31.

You should consider the position of policies that pass through traffic unoptimized because placing these policies at the top of the list can cancel out optimization policies that appear farther down the list. For example, if you have two application policies that match traffic going to IP address 10.10.10.2, and one policy optimizes this traffic and a second policy in a higher position passes through this traffic, then all traffic going to 10.10.10.2 will go through the WAAS system unoptimized. For this reason, you should make sure that your policies do not have overlapping matching conditions, and you should monitor the applications you create to make sure that WAAS is handling the traffic as expected. For more information on monitoring applications, see Chapter 16, "Monitoring and Troubleshooting Your WAAS Network."

To modify the position of an application policy, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or group that contains the application policy to modify.

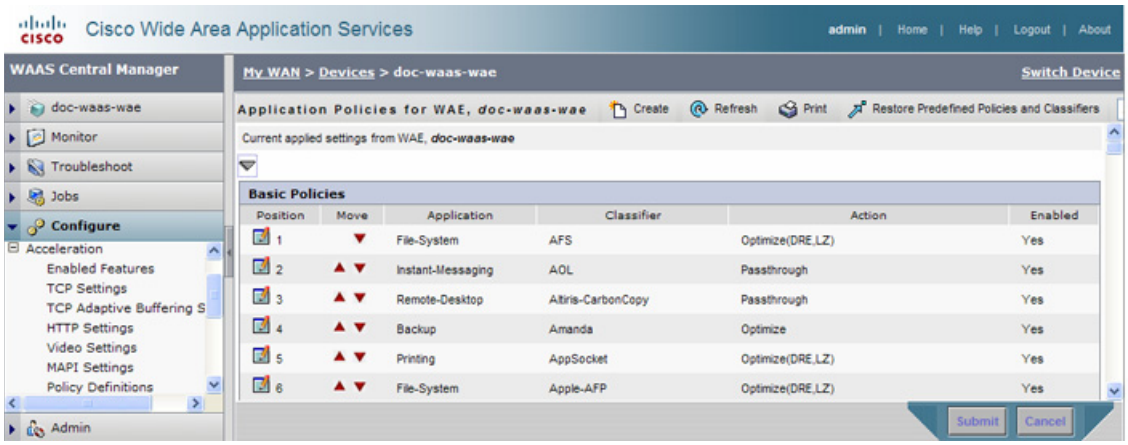
Step 3 From the navigation pane, choose **Configure > Acceleration > Policy Prioritization**.

Step 4 The Application Policies window appears. This window categorizes policies into these categories: Basic, Other, Port Mapper, and WAFS. For WAAS Express devices, all policies are grouped under the waas_global category, which is the same as the Basic WAAS category.

Step 5 Click the arrow next to the appropriate category to display the list of applications for that category. (See Figure 12-24.)

In most cases, the application you want to change the position for will be located under the Basic Policies category (waas_global for WAAS Express devices) because that category contains a majority of the predefined applications that shipped with the WAAS system. For a list of these predefined policies, see Appendix A, "Predefined Application Policies."

Figure 12-24 Modifying the Position of Application Policies



Step 6 Click the arrow next to the policy category to view the list of applications for that category.

Step 7 Use the up and down arrows (▲ ▼) next to a policy to move that policy higher or lower in the list.

For WAAS Express devices, the waas-default policy should be last. This policy is the same as the WAAS Other policy type. This policy cannot be modified or deleted.

Step 8 If you determine that a policy is not needed, follow these steps to delete the policy:

a. Click the **Edit** icon next to the policy you want to delete.

The Modifying Application Policy window appears.

b. Click the **Delete** icon in the taskbar.

Step 9 If you determine that a new policy is needed, click the **Create New Policy** taskbar icon to create the policy (see the "Creating an Application Policy" section on page 12-31).

Modifying the Acceleration TCP Settings

In most cases, you do not need to modify the acceleration TCP settings because your WAAS system automatically configures the acceleration TCP settings based on the hardware platform of the WAE device. WAAS automatically configures the settings only under the following circumstances:

- When you first install the WAE device in your network.
- When you enter the **restore factory-default** command on the device. For more information about this command, see the *Cisco Wide Area Application Services Command Reference*.

The WAAS system automatically adjusts the maximum segment size (MSS) to match the advertised MSS of the client or server for each connection. The WAAS system uses the lower of 1432 or the MSS value advertised by the client or server.

If your network has high BDP links, you may need to adjust the default buffer settings automatically configured for your WAE device. For more information, see the "Calculating the TCP Buffers for High BDP Links" section on page 12-43.

If you want to adjust the default TCP adaptive buffering settings for your WAE device, see the "Modifying the TCP Adaptive Buffering Settings" section on page 12-44.

To modify the acceleration TCP settings, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the device or device group for which you want to change the acceleration TCP settings.

Step 3 From the navigation pane, choose **Configure > Acceleration > TCP Settings**. The Acceleration TCP Settings window appears.

Step 4 Keep the **Send TCP Keepalive** check box checked.

Checking the Send TCP Keepalive check box allows this WAE device or group to disconnect the TCP connection to its peer device if no response is received from the TCP keepalive exchange. In this case, the two peer WAE devices will exchange TCP keepalives on a TCP connection and if no response is received for the keepalives for a specific period, the TCP connection will be torn down. When the keepalive option is enabled, any short network disruption in the WAN will cause the TCP connection between peer WAE devices to be disconnected.

If the Send TCP Keepalive check box is not checked, TCP keepalives will not be sent and connections will be maintained unless they are explicitly disconnected. By default, this setting is enabled.

Step 5 Modify the TCP acceleration settings as needed. See Table 12-6 for a description of these settings.

For information on how to calculate these settings for high BDP links, see the "Calculating the TCP Buffers for High BDP Links" section on page 12-43.

Table 12-6 TCP Settings

TCP Setting	Description
Optimized Side	
Maximum Segment Size	Maximum packet size allowed between this WAAS device and other WAAS devices participating in the optimized connection. The default is 1432 bytes.
Send Buffer Size	Allowed TCP sending buffer size (in kilobytes) for TCP packets sent from this WAAS device to other WAAS devices participating in the optimized connection. The default is 32 KB.
Receive Buffer Size	Allowed TCP receiving buffer size (in kilobytes) for incoming TCP packets from other WAAS devices participating in the optimized connection. The default is 32 KB.
Original Side	
Maximum Segment Size	Maximum packet size allowed between the origin client or server and this WAAS device. The default is 1432 bytes.
Send Buffer Size	Allowed TCP sending buffers size (in kilobytes) for TCP packets sent from this WAAS device to the origin client or server. The default is 32 KB.
Receive Buffer Size	Allowed TCP receiving buffer size (in kilobytes) for incoming TCP packets from the origin client or server. The default is 32 KB.

Step 6 If you are deploying the WAE across a high Bandwidth-Delay-Product (BDP) link, you can set recommended values for the send and receive buffer sizes by clicking the **Set High BDP recommended values** button. For more information about calculating TCP buffers for high BDP links, see the "Calculating the TCP Buffers for High BDP Links" section on page 12-43.

Step 7 Click **Submit**.

To configure TCP keepalives from the CLI, use the **tfo tcp keepalive** global configuration command.

To configure TCP acceleration settings from the CLI, use the following global configuration commands: **tfo tcp optimized-mss**, **tfo tcp optimized-receive-buffer**, **tfo tcp optimized-send-buffer**, **tfo tcp original-mss**, **tfo tcp original-receive-buffer**, and **tfo tcp original-send-buffer**.

To show the TCP buffer sizes, use the **show tfo tcp** EXEC command.

Calculating the TCP Buffers for High BDP Links

WAAS software can be deployed in different network environments, involving multiple link characteristics such as bandwidth, latency, and packet loss. All WAAS devices are configured to accommodate networks with maximum Bandwidth-Delay-Product (BDP) of up to the values listed below:

- WAE-511/512—Default BDP is 32 KB
- WAE-611/612—Default BDP is 512 KB
- WAE-674 —Default BDP is 2048 KB
- WAE-7326 —Default BDP is 2048 KB
- WAE-7341 —Default BDP is 2048 KB
- WAE-7371 —Default BDP is 2048 KB
- WAVE-274 —Default BDP is 2048 KB
- WAVE-474 —Default BDP is 2048 KB
- WAVE-574—Default BDP is 2048 KB

If your network provides higher bandwidth or higher latencies are involved, use the following formula to calculate the actual link BDP:

BDP [Kbytes] = (link BW [Kbytes/sec] * Round-trip latency [Sec])

When multiple links 1..N are the links for which the WAE is optimizing traffic, the maximum BDP should be calculated as follows:

MaxBDP = Max (BDP(link 1),..,BDP(link N))

If the calculated MaxBDP is greater than the DefaultBDP for your WAE model, the Acceleration TCP settings should be modified to accommodate that calculated BDP.

Once you calculate the size of the Max BDP, enter a value that is equal to or greater than twice the Max BDP in the Send Buffer Size and Receive Buffer Size for the optimized connection on the Acceleration TCP Settings window.

Note These manually configured buffer sizes apply only if TCP adaptive buffering is disabled. TCP adaptive buffering is normally enabled, and allows the WAAS system to dynamically vary the buffer sizes. For more information on TCP adaptive buffering, see the "Modifying the TCP Adaptive Buffering Settings" section on page 12-44.

Modifying the TCP Adaptive Buffering Settings

In most cases, you do not need to modify the acceleration TCP adaptive buffering settings because your WAAS system automatically configures the TCP adaptive buffering settings based on the network bandwidth and delay experienced by each connection. Adaptive buffering allows the WAAS software to dynamically vary the size of the send and receive buffers to increase performance and more efficiently use the available network bandwidth.

To modify the acceleration TCP adaptive buffering settings, follow these steps:

Step 1 From the WAAS Central Manager GUI navigation pane, choose **My WAN > Manage Devices** (or **Manage Device Groups**).

Step 2 Click the **Edit** icon next to the name of the device (or device group) for which you want to configure the TCP adaptive buffering settings.

Step 3 In the navigation pane, choose **Configure > Acceleration > TCP Adaptive Buffering Settings**. The TCP Adaptive Buffering Settings window appears.

Step 4 To enable TCP adaptive buffering, check the **Enable** check box. The default is enabled.

Step 5 In the Send Buffer Size and Receive Buffer Size fields, enter the maximum size in kilobytes of the send and receive buffers.

Step 6 Click **Submit**.

To configure the TCP adaptive buffer settings from the CLI, use the **tfo tcp adaptive-buffer-sizing** global configuration command:

```
WAE(config)# tfo tcp adaptive-buffer-sizing receive-buffer-max 8192
```

To disable TCP adaptive buffering from the CLI, use the **no tfo tcp adaptive-buffer-sizing enable** global configuration command.

To show the default and configured adaptive buffer sizes, use the **show tfo tcp** EXEC command.