



Configuring Application Acceleration

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



Note

Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco Wide Area Application Services (Cisco WAAS) Central Managers and Cisco Wide Area Application Engines (WAEs) in your network. The term WAE refers to WAE and Cisco Wide Area Virtualization Engine (WAVE) appliances, Cisco Services Ready Engine (SRE) service modules (SMs) running WAAS, and Cisco Virtual WAAS (vWAAS) instances.

This chapter contains the following sections:

- [About Application Acceleration](#)
- [Enabling and Disabling the Global Optimization Features](#)
- [Creating a New Traffic Optimization Policy](#)
- [Managing Application Acceleration](#)

About Application Acceleration

The Cisco WAAS software comes with over 150 predefined optimization 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 Optimization Policy.”](#)

Each optimization policy contains the following elements:

- **Application definition**—Identifies general information about a specific application, such as the application name and whether the WAAS Central Manager collects statistics about this application.
- **Class map**—Contains a matching condition that identifies specific types of traffic. For example, the default HTTP class map matches all the traffic going to ports 80, 8080, 8000, 8001, and 3128. You can create up to 512 class maps and 1024 matching conditions.
- **Policy**—Combines the application definition and class map into a single policy. This policy also determines the optimization and acceleration features, if any, that a WAAS device applies to the defined traffic. You can create up to 512 policies. A policy can also contain a differentiated services code point (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 optimization policies, see [Creating a New Traffic Optimization Policy](#). For more information on viewing reports, restoring policies, monitoring applications, and other functions, see [Managing Application Acceleration](#).

**Note**

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

WAAS policies can apply two kinds of optimizations to matched traffic:

- Layer 4 optimizations that include TFO, DRE, and LZ compression. These features can be applied to all types of TCP traffic.
- Layer 7 optimizations that accelerate application-specific protocols. The application accelerators control these kinds of optimizations.

For a given optimization policy, the DRE feature can use different caching modes (beginning with WAAS Software Version 4.4.1):

- Bidirectional—The peer WAEs maintain identical caches for inbound and outbound traffic. This caching mode is best suited for scenarios where a significant portion of the traffic seen in one direction between the peers is also seen in the reverse direction. In WAAS software versions prior to 4.4.1, this mode is the only supported caching mode.
- Unidirectional—The peer WAEs maintain different caches for inbound and outbound traffic. This caching mode is best suited for scenarios where a significant portion of the traffic seen in one direction between the peers is not seen in the reverse direction.
- Adaptive—The peer WAEs negotiate either bidirectional or unidirectional caching based on the characteristics of the traffic seen between the peers.

The predefined optimization policies are configured to use the optimal DRE caching mode, depending on the typical application traffic, although you can change the mode if you want.

Enabling and Disabling the Global Optimization Features

The global optimization features determine if traffic flow optimization (TFO), 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, HTTP, ICA, MAPI, SMB, and SSL. By default, all of the application accelerators are enabled. The application accelerators also require specific licenses to operate. For information on installing licenses, see [Managing Software Licenses](#) in Chapter 10, “Configuring Other System Settings.”

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 menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).

Step 2 Choose **Configure** > **Acceleration** > **Enabled Features**.

The Enabled Features window appears.



Note On WAAS Express devices, only a subset of the standard features are available. On ISR-WAAS devices, the SMB application accelerator is enabled by default. In the Enabled Features window for a device group, two SMB Accelerator options are shown, one for ISR-WAAS devices and one for all other kinds of WAEs.

For WAAS Express, the following Express versions of application accelerators are supported:

- HTTP accelerator express (See the [Configuring HTTP Acceleration](#))
- SSL accelerator express (See the [Configuring SSL Acceleration](#))

Not all of the properties in the standard WAAS device are available in the WAAS Express version of the application accelerators.



Note If you try to enable DRE on a WAAS Express device on which it is not supported, a message stating that it is not supported is displayed.

The Restore Predefined Settings icon for WAAS Express applies the predefined settings for HTTP/HTTPS, and SSL cipher list and peering service.

Step 3 Check the check boxes adjacent to the optimization features that you want to enable, and uncheck the check boxes adjacent to the features that you want to disable. For a description of each of the optimization features, see [Key Services of Cisco WAAS](#) in Chapter 1, “Introduction to Cisco WAAS.”

Some features have additional settings that you can configure by clicking the link next to the setting name. Hover your cursor over the small target icon next to the link to see a dialog box that shows the current settings.

- If you check the **Data Redundancy Elimination** check box, you can click the DRE Settings link as a shortcut to the DRE Settings Configuration window. For more information, see [Configuring DRE Settings](#).

- If you check the **HTTP Accelerator** check box, you can click the **HTTP Settings** link as a shortcut to the HTTP/HTTPS Settings window. For more information, see [Configuring HTTP Acceleration](#).
- If you check the **ICA Accelerator** check box, you can click the **ICA Settings** link as a shortcut to the ICA Acceleration Configuration window. For more information, see [Configuring ICA Acceleration](#).
- If you check the **MAPI Accelerator** check box, you can click the **MAPI Settings** link as a shortcut to the MAPI Settings window. For more information, see [Configuring MAPI Acceleration](#).



Note When you check the **MAPI Accelerator** check box, Encrypted MAPI Traffic Optimization is enabled by default.

- If you check the **Encrypted MAPI Traffic Optimization** check box, you can click the **Mandatory Encryption Configuration** link as a shortcut to the Encrypted Services Configuration window. For more information, see [Configuring Encrypted MAPI Acceleration](#).



Note You must enable MAPI acceleration first for Encrypted MAPI acceleration to be enabled.

- If you check the **SMB Accelerator** check box, you can click the **SMB Settings** link as a shortcut to the SMB Acceleration Configuration window. For more information, see [Configuring SMB Acceleration](#).
- If you check the **SSL Accelerator** check box, you must configure additional settings to enable SSL acceleration. For more information, see [Configuring SSL Acceleration](#).

Step 4 To enable the object cache, in the **Object Cache Settings** section, check the **Object Cache** check box. WAAS performs object caching to increase client application performance for SMB file access. Object caching also minimizes bandwidth and latency over the WAN, by avoiding the repeated transfer of data over the WAN.

To enable an individual application accelerator object cache, use the following guideline:

- Controls to enable and disable an individual object cache are displayed in that application accelerator's **Advanced Settings** screen.



Note To ensure that the object cache and individual application accelerator object cache work successfully, note these guidelines:

- Each application accelerator object cache can be enabled or disabled independent of whether or not the global object cache is enabled or disabled.
- Enabling the object cache does not automatically enable individual application accelerator object caches.
- You can enable or disable an individual application accelerator object cache whether or not the associated application accelerator is enabled or disabled.
- Verify that disk assignments have been made to object cache before you enable object cache.
- The object cache has a limit of 15 GB. A request of a size larger than this limit will not cache the complete file. For example, for a file size of 25 GB, only 15 GB of this file would be cached.

**Note**

To ensure that the object cache and SMB application accelerator work successfully, enable the object cache before you enable the SMB application accelerator.

Step 5 In the **Advanced Settings** area, uncheck the **Blacklist Operation** check box 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 that you leave this feature enabled.

Step 6 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 the 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 7 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 ICA acceleration from the CLI, use the **accelerator ica** global configuration command.

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

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

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

To configure global object cache from the CLI, use the **object-cache enable** global configuration command.

When object cache is enabled, you are prompted to confirm the repurposing of SMB resources if the disk has not already been partitioned for object cache.

If this is the first time disk resources are being assigned to object cache, the **object-cache enable** command will prompt you to reboot the device, since the disk partitioning only takes effect on the next reboot. The configuration is then saved, and the object cache does not have to be re-enabled on the next reboot.

**Note**

To ensure success of the **object-cache enable** command, verify the following two conditions:

- Disk assignments have been made to object cache *before* you use this command.

- Use this command *before* you use the **accelerator smb** global configuration command.

To enable a specified application accelerator object cache, use the **accelerator ao-name object-cache enable** global configuration command.



Note

To ensure that each application accelerator object cache and the global object cache function successfully, note these guidelines:

- Each application accelerator object cache can be enabled or disabled independent of whether or not the global object cache is enabled or disabled.
- You must disable all individual application accelerator object caches *before* you use the **no object-cache enable** global configuration command to disable the global object cache.
- The **object-cache enable** global configuration command does not automatically enable individual application accelerator object caches.
- You can enable or disable an individual application accelerator object cache whether or not the associated application accelerator is enabled or disabled.

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 SMB print accelerator, use the **show statistics accelerator smb** EXEC command.

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

- [Configuring HTTP Acceleration](#)
- [Configuring MAPI Acceleration](#)
- [Configuring Encrypted MAPI Acceleration](#)
- [Configuring SMB Acceleration](#)
- [Configuring ICA Acceleration](#)
- [Configuring SSL Acceleration](#)
- [Configuring SMB Acceleration](#)

Configuring DRE Settings

To enable DRE settings, check the **Data Redundancy Elimination** check box in the Enabled Features window .

To configure the DRE auto bypass and load monitor settings, follow these steps:

- Step 1 From the WAAS Central Manager menu, choose **Devices > device-name** (or **Device Groups > device-group-name**).

- Step 2** Choose **Configure > Acceleration > DRE Settings**.
The DRE Settings window appears.
- Step 3** Check the **Enable DRE auto bypass** check box to generate an alarm and automatically DRE bypass application traffic.
- Step 4** Check the **Enable DRE Load Monitor** check box to enable load report.
- The **disk latency maximum** can be set from 1-1000; the default value is 5.
 - The **DRE load threshold** can be set from 50-99; the default value is 95.
- Step 5** Click **Submit**.
The changes are saved to the device or device group.
-

To enable DRE auto bypass from the CLI, use the **dre auto-bypass enable** global configuration command.

To enable DRE load monitor from the CLI, use the **dre load-monitor report** global configuration command.

Configuring HTTP Acceleration

The HTTP application accelerator accelerates HTTP traffic. To optimize HTTPS, you must enable both SSL and HTTP and also have protocol chaining enabled.

The default Web optimization policy is defined to send traffic to the HTTP accelerator. The Web optimization policy uses the HTTP class map, 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 class map.

To enable the HTTP accelerator, check the **HTTP Accelerator** check box in the Enabled Features window .

To configure the HTTP acceleration settings, follow these steps:

-
- Step 1** From the WAAS Central Manager menu, choose **Devices > device-name** (or **Device Groups > device-group-name**).
- Step 2** Choose **Configure > Acceleration > HTTP/HTTPS Settings**.
The HTTP Acceleration Settings window appears ([Figure 12-1](#)).



Note For WAAS Express, the HTTP acceleration settings are the same, but the fields are laid out differently in the HTTP/HTTPS Settings window.

Figure 12-1 HTTP Acceleration Settings Window

The screenshot shows the 'HTTP/HTTPS Settings' window in the Cisco WAAS configuration interface. The breadcrumb trail is: Devices > WAE-231-03 > Configure > Acceleration > HTTP/HTTPS Settings. The current settings are 'None (Using Factory Defaults)'. The 'Metadata Cache Settings' section includes the following options:

- ☒ Enable HTTP Metadata Cache
- ☒ Enable HTTPS Metadata Cache
- Maximum age of Cache entry: 86400 (seconds) (5-2592000)
- Minimum age of Cache entry: 60 (seconds) (5-86400)
- ☒ Enable local HTTP 301 Redirect messages
- ☒ Enable local HTTP 401 Authentication-required messages
- ☒ Enable local HTTP 304 Not-Modified messages

Below these settings is a 'File Extension Filters' section with an empty text box and a help icon. The 'Sharepoint Settings' section has an unchecked 'Enable Pre-fetch Optimization' checkbox. The 'Server Compression Settings' section has an unchecked 'Suppress server compression for HTTP and HTTPS' checkbox. The 'DRE Hints Settings' section has a checked 'Enable DRE Hints for HTTP and HTTPS' checkbox. At the bottom are 'Submit' and 'Reset' buttons. The status bar at the bottom right shows 'Alarms 0 0 5 0' and the IP address '346124'.

- Step 3** Check the **Enable HTTP metadatacache caching** check box to enable the WAE to cache HTTP header (metadata) information. The default setting is checked.
- This check 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 [About HTTP Metadata Caching](#).
- Step 4** 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 checked.
- For details on HTTP metadata caching, see [About HTTP Metadata Caching](#).
- Step 5** 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 6** In the Minimum age of a Cache entry field, enter the minimum number of seconds for which 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 7** 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 8** 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 9** 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 10 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.

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

Step 11 Check the **Enable Pre-fetch Optimization** check box to allow the edge WAAS device to prefetch data. This setting is not enabled by default.

This optimization benefits Web browser-based Microsoft Office applications when they access Microsoft Office documents (MS Word and Excel only) hosted on a Microsoft SharePoint Server 2010. For viewing Word documents, the client must have Microsoft Silverlight installed.

By checking this check box, you are telling the edge WAAS device to prefetch the subsequent pages of the documents from the SharePoint server before the client actually requests them, and serve them from the cache when the request from the client arrives. You can now seamlessly scroll through the document without having to wait for the content to load.



Note SharePoint prefetch optimization works with view in browser mode only.

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 checked.

By checking this check 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 enabled 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-metadataacache EXEC** command.

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

To enable or disable specific HTTP accelerator features for specific clients or IP subnets, use the HTTP accelerator subnet feature. For more details, see [Using an HTTP Accelerator Subnet](#).

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 containing over 255 characters
- 301 and 401 responses with cookie headers
- Use of HEAD method
- 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.

Using an HTTP Accelerator Subnet

The HTTP accelerator subnet feature allows you to selectively enable or disable specific HTTP optimization features for specific IP subnets by using ACLs. This feature can be applied to the following HTTP optimizations: HTTP metadata caching, HTTPS metadata caching, DRE hints, and suppress server compression.

To define IP subnets, use the **ip access-list** global configuration command. Refer to this command in [Cisco Wide Area Application Services Command Reference](#) for more information on configuring subnets. You can use both standard and extended ACLs.

To configure a subnet for an HTTP accelerator feature, follow these steps:

-
- Step 1** Enable global configuration for all the HTTP accelerator features that you want to use.
- Step 2** Create an IP access list to use for a subnet of traffic:
- ```
WAE(config)# ip access-list extended md_acl
WAE(config-ext-nacl)# permit ip 1.1.1.0 0.0.0.255 any
WAE(config-ext-nacl)# permit ip 2.2.2.0 0.0.0.255 3.3.3.0 0.0.0.255
WAE(config-ext-nacl)# exit
```
- Step 3** Associate the ACL with a specific HTTP accelerator feature. Refer to the **accelerator http** global configuration command in [Cisco Wide Area Application Services Command Reference](#) for information on associating an ACL with an HTTP accelerator feature:
- ```
WAE(config)# accelerator http metadatacache access-list md_acl
```

In this example, the HTTP metadata cache feature applies to all the connections that match the conditions specified in the extended access-list md_acl.

In the following example, the HTTP suppress-server-encoding feature applies to all the connections that match the conditions specified in the standard access-list 10:

```
WAE(config)# ip access-list standard 10
WAE(config-std-nacl)# permit 1.1.1.0 0.0.0.255
WAE(config-std-nacl)# exit
WAE(config)# accelerator http suppress-server-encoding accesslist 10
```

For the features (DRE hints and HTTPS metadata cache in this example) that do not have an ACL associated with them, global configuration is used and the features are applicable to all the connections.

Configuring MAPI Acceleration

The MAPI application accelerator accelerates Microsoft Outlook Exchange traffic that uses the Messaging Application Programming Interface (MAPI) protocol.

- For WAAS Version 5.3.x and later, Microsoft Outlook 2000–2013 clients are supported.
- For WAAS Version 5.2.x and earlier, 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) 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 optimization 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 optimization policy that accelerates MAPI traffic with a class map 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 section.

**Note**

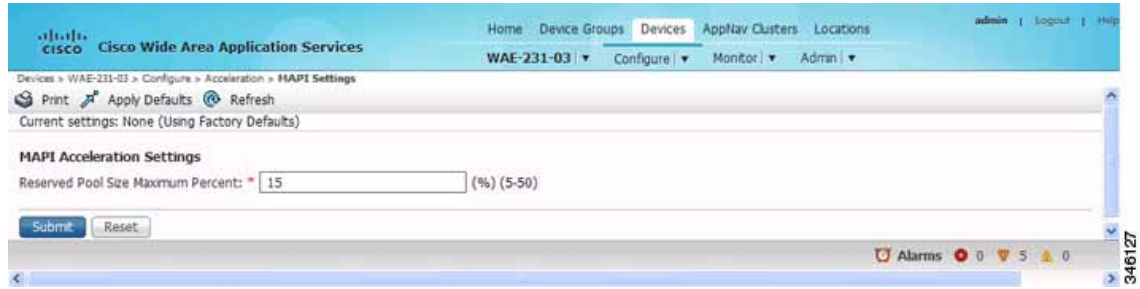
When you enable MAPI acceleration, Encrypted MAPI acceleration is enabled by default.

To configure MAPI acceleration settings, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).

Step 2 Choose **Configure** > **Acceleration** > **MAPI Settings**.

The MAPI Acceleration Settings window appears ([Figure 12-2](#)).

Figure 12-2 *MAPI Acceleration Settings Window*

- Step 3** In the Reserved Pool Size Maximum Percent field, enter the maximum percent of connections in order 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 to 50 percent. The default is 15 percent, which reserves 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 three connections per AG. For deployments that see 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 remain unused when the device is not under TFO overload. Reserved connections are released when the AG is terminated.

- Step 4** Click **Submit**.

The changes are saved to the device or device group.

Configuring Encrypted MAPI Acceleration

The Encrypted MAPI acceleration feature provides WAN optimization for secure MAPI application protocols using Microsoft Kerberos security protocol and Microsoft Windows Active Directory identity for authentication of clients or servers or both in the domain.



Note

You must enable MAPI acceleration first for Encrypted MAPI acceleration to be enabled. Encrypted MAPI acceleration is enabled by default.

This section contains the following topics:

- [Workflow for Configuring Encrypted MAPI](#)
- [Configuring Encrypted MAPI Settings](#)
- [Configuring a Machine Account Identity](#)
- [Creating and Configuring a User Account](#)
- [Configuring Microsoft Active Directory](#)
- [Managing Domain Identities and Encrypted MAPI State](#)

Workflow for Configuring Encrypted MAPI

To configure Encrypted MAPI traffic acceleration, complete the tasks listed in [Table 12-1](#). These tasks must be performed on both data center and branch WAEs unless specified as Not Required or Optional.

Table 12-1 *Tasks for Configuring Encrypted MAPI*

Task	Additional Information and Instructions
1. Configure DNS Settings.	To configure DNS settings, see Configuring the DNS Server in Chapter 6, “Configuring Network Settings.”
2. Configure NTP Settings.	To synchronize the time with Active Directory, see the Configuring NTP Settings in Chapter 10, “Configuring Other System Settings.”
3. Verify WAE devices are registered and online with the WAAS Central Manager.	To verify WAE devices are registered and online with the WAAS Central Manager, see Devices Window in Chapter 15, “Monitoring and Troubleshooting Your WAAS System.”
4. Configure SSL Peering Service.	To configure SSL Peering Service, see Configuring SSL Peering Service .
5. Verify WAN Secure mode is enabled.	To verify WAN Secure mode is enabled, use the show accelerator wansecure EXEC command.
6. Configure windows domain settings and perform domain join. (The domain join function automatically creates the machine account in Active Directory.)	To configure Windows Domain Server Authentication settings, see Configuring Windows Domain Server Authentication Settings in Chapter 7, “Configuring Administrative Login Authentication, Authorization, and Accounting.” Note that performing a domain join of the WAE is not required on branch WAE devices.
7. Configure domain identities (for machine account and optional user accounts).	To configure a machine account identity, see Configuring a Machine Account Identity . (Optional) To create a user account and configure a user account identity, see Creating and Configuring a User Account . Note that configuring domain identities is not required on branch WAE devices.
8. Enable Windows Domain Encrypted Service.	To enable the Windows Domain Encrypted Service, navigate to the Configure > Security > Windows Domain > Encrypted Services page and check the Enable Encrypted Service check box.
9. Enable Encrypted MAPI Traffic Optimization.	To enable Encrypted MAPI Traffic, see Enabling and Disabling the Global Optimization Features .

Configuring Encrypted MAPI Settings

To configure encrypted MAPI settings, follow these steps:

- Step 1** Configure DNS settings.

The WAAS DNS server must be a part of the DNS system of Windows Active Directory domains to resolve DNS queries for traffic encryption.

For more information about configuring DNS settings, see [Configuring the DNS Server](#) in Chapter 6, “Configuring Network Settings.”

Step 2 Configure NTP settings to synchronize the time with the Active Directory.

The WAAS device has to be in synchronization with the Active Directory for Encrypted MAPI acceleration. The WAAS NTP server must share time synchronization with the Active Directory Domain Controllers’ domains for which traffic encryption is required. Out-of-sync time will cause Encrypted MAPI acceleration to fail.

For more information about synchronizing time with the Active Directory, see [Configuring NTP Settings](#) in Chapter 10, “Configuring Other System Settings.”

Step 3 Verify if WAE devices are registered and are online with the WAAS Central Manager.

For more information about verifying that WAE devices are registered and are online with the WAAS Central Manager, see the [Devices Window](#) in Chapter 15, “Monitoring and Troubleshooting Your WAAS Network.”

Step 4 Configure the SSL Peering Service.



Note The SSL accelerator must be enabled and in running state.

For more information about configuring the SSL Peering Service, see [Configuring SSL Peering Service](#).

Step 5 Verify if WAN Secure mode is enabled.

The default mode is Auto. You can verify the state of WAN Secure mode using the following EXEC command:

show accelerator wansecure

If necessary, you can change the state of WAN Secure using the following global configuration command:

accelerator mapi wansecure-mode {always | auto | none}

Step 6 (Optional on data center WAEs if only user accounts are used for domain identity configuration in Step 7.) Configure Windows domain settings and perform a domain join. (A domain join automatically creates the machine account in Active Directory.)



Note Performing a domain join of the WAE is not required on branch WAE devices.

To configure Windows Domain Server Authentication settings, see [Configuring Windows Domain Server Authentication Settings](#) in Chapter 7, “Configuring Administrative Login Authentication, Authorization, and Accounting.”



Note Kerberos and Windows NT LAN Manager (NTLM) authentication are used for Encrypted MAPI acceleration. For WAAS 5.3.1, encrypted NTLM traffic is supported for EMAPI, and the WAE device optimizes NTLM traffic for domains configured with NTLM authentication.

Step 7 Configure domain identities. (Not required for branch WAEs.)

You must have at least one account, either user or machine, that is configured with a domain identity. Each device can support up to five domain identities, one machine account identity and four user account identities. This allows a WAAS device to accelerate up to five domain trees. You must configure a domain identity for each domain with an exchange server that has clients to be accelerated.

- a. Configure the machine account identity.

A machine account for the core device is automatically created during the join process in the Windows Domain Server authentication procedure in Step 6. If you are using a machine account, a machine account identity must be configured for this account.

Each device supports only one machine account identity.

To configure a machine account identity, see [Configuring a Machine Account Identity](#).

- b. Create and configure optional user accounts.

You can utilize up to four optional user accounts for additional security. Multiple user accounts provide greater security than having all of the core devices using a single user account. You must configure a user account identity for each user account, whether you are utilizing an existing user account or creating a new one.

To create a user account and configure a user account identity, see [Creating and Configuring a User Account](#).

Step 8 Enable Windows Domain Encrypted Service. (This is enabled by default.)

- a. From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- b. From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.
The Encrypted Services window appears.
- c. Check the **Enable Encrypted Service** check box.
- d. Click **Submit** to save your changes.

Step 9 Enable Encrypted MAPI Traffic Optimization.

In the Enabled Features window, check the **Encrypted MAPI Traffic Optimization** check box (the **MAPI Accelerator** check box must also be checked), and click **Submit**. (Encrypted MAPI traffic optimization is enabled by default.)

For more information on the Enabled Features window, see [Enabling and Disabling the Global Optimization Features](#).

Configuring a Machine Account Identity

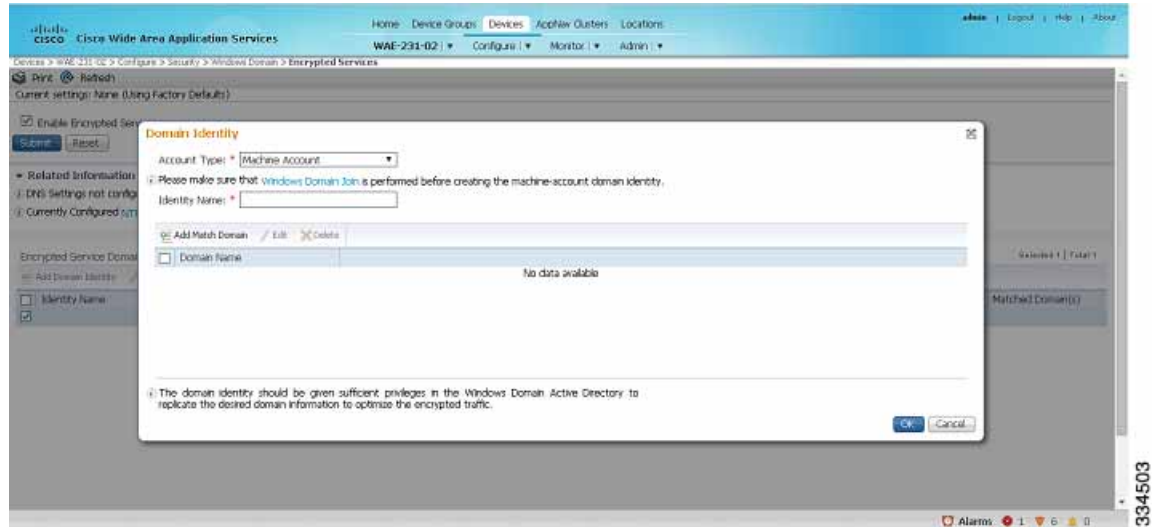
To configure an identity for a machine account, follow these steps:

- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.
The Encrypted Services window appears.
- Step 3** Click the **Add Domain Identity** button.
The Domain Identity dialog box appears ([Figure 12-3](#)).



Note Every WAAS device that has to be accelerated must have a domain identity.

Figure 12-3 Add Domain Identity—Machine Account



- a. In the Domain Identity dialog box that is displayed, choose **Machine Account** from the Account Type drop-down list.



Note Windows domain join must be completed before creating the machine account domain identity. For more information, see [Configuring Windows Domain Server Settings on a WAAS Device](#) in Chapter 7, “Configuring Administrative Login Authentication, Authorization, and Accounting.”

- b. Enter the identity name in the Identity Name field. Only alphanumeric characters are allowed. Space, ?, and | are not allowed. The length is not to exceed 32 characters.



Note The domain identity must have sufficient privileges in the Windows Domain Active Directory to replicate the desired domain information to optimize encrypted traffic. To configure privileges, see [Configuring Microsoft Active Directory](#).

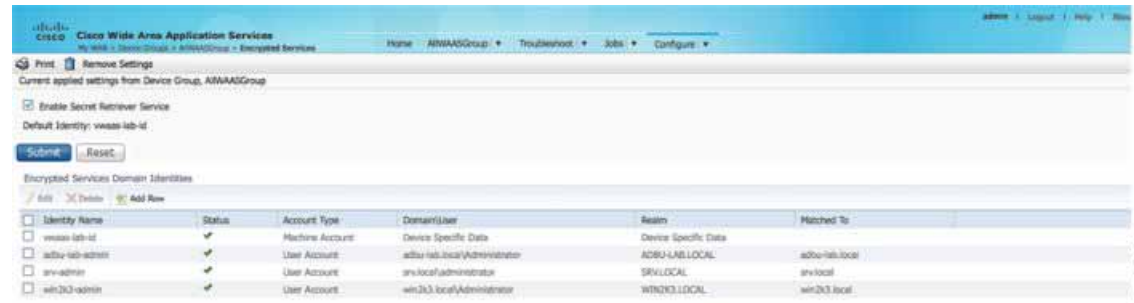
- Step 4** Click the **Add Match Domain** button to add the child domains of the domain (with which the device is registered) for which the Domain Identity should optimize the encrypted traffic. You can add up to 32 child domains. If you do not want the Domain Identity to optimize the traffic for any of the child domains, you can delete the selected match domain items.



Note This is available only on devices running WAAS Version 5.4 and above.

- Step 5** Click **OK**.

The domain identity appears in the Encrypted Services Domain Identities list ([Figure 12-4](#)).

Figure 12-4 Encrypted Services—Domain Identity

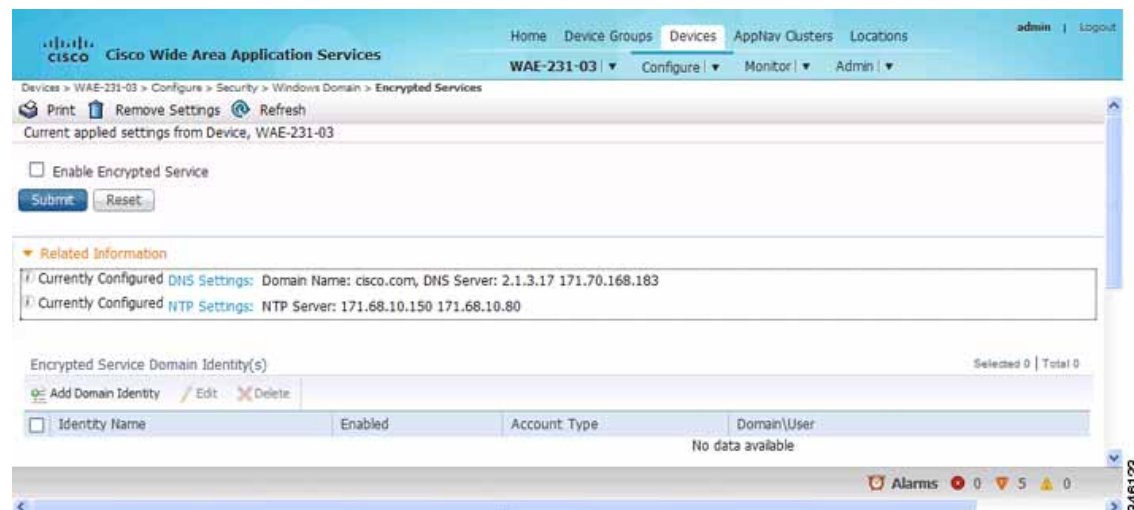
333672

To configure and verify Encrypted Services Domain Identities from the CLI, use the **windows-domain encrypted-service** global configuration command and the **show windows-domain encrypted-service EXEC** command.

Creating and Configuring a User Account

To create a user account and configure a user account identity, follow these steps:

- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**. The Encrypted Services window appears (Figure 12-5).

Figure 12-5 Encrypted Services

346123

- Step 3** Click **Add Domain Identity** to add a user account domain identity. The Domain Identity window appears (Figure 12-6).

Figure 12-6 Add Domain Identity—User Account

- a. Choose user account from the **Account Type** drop-down list.
- b. Enter the identity name in the Identity Name field. Only alphanumeric characters are allowed. Space, ?, and | are not allowed. The length is not to exceed 32 characters.
- c. Enter username and password.
- d. Enter the domain name.
- e. Enter the Kerberos realm.
- f. Click **Add Match Domain** to add the child domains of the selected domain, for which the Domain Identity should optimize the encrypted traffic. You can add up to 32 child domains. If you do not want the Domain Identity to optimize the traffic for any of the child domains, you can delete the selected match domain items.

**Note**

The domain identity must have sufficient privileges in the Windows Domain Active Directory to replicate the desired domain information to optimize encrypted traffic. For information about configuring privileges, see [Configuring Microsoft Active Directory](#).

Step 4 Click **OK**.

The domain identity appears in the Encrypted Services Domain Identities list.

**Note**

Secure store encryption is used for the user account domain identity password. If secure store cannot be opened, an alarm is raised indicating that the configuration updates could not be stored on the device. After secure store can be opened and the configuration updates are successfully stored on the device, the alarm is cleared.

To configure and verify Encrypted Services Domain Identities from the CLI, use the **windows-domain encrypted-service** global configuration command and the **show windows-domain encrypted-service EXEC** command.

Configuring Microsoft Active Directory

To grant Cisco WAAS permission to accelerate Microsoft Exchange-encrypted email sessions, follow these steps:

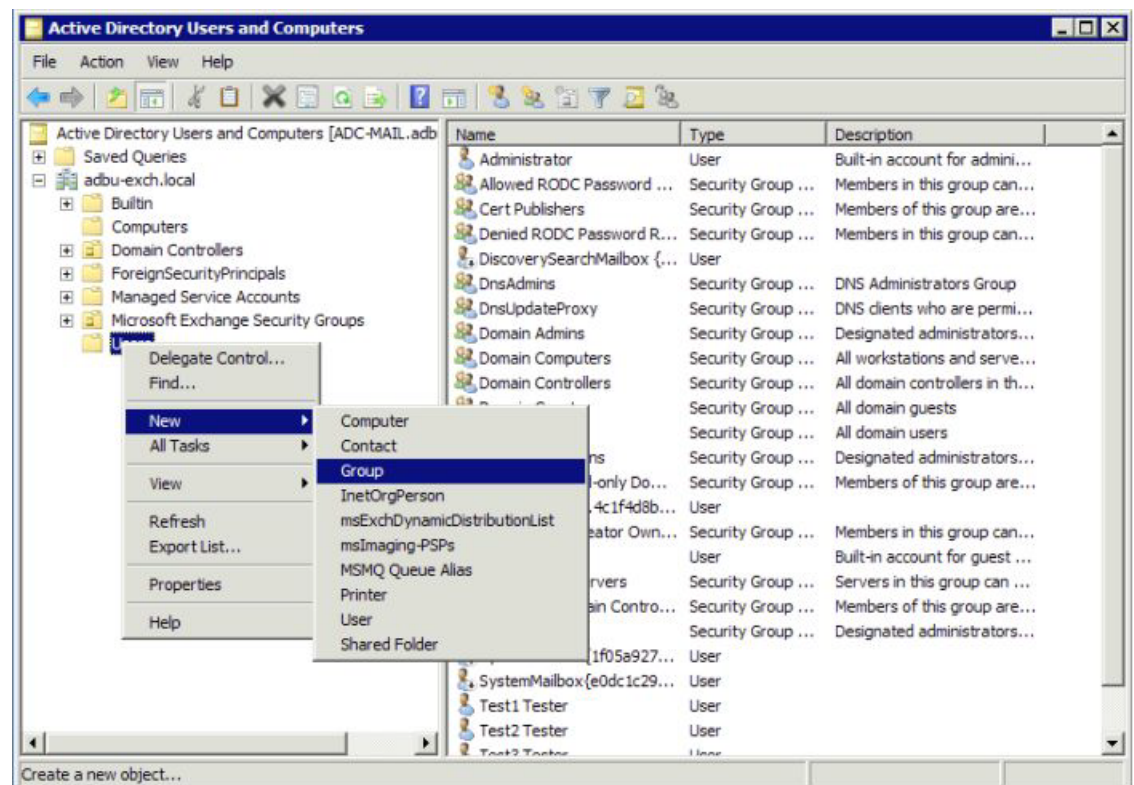
- Step 1** Using an account with Domain Administrator privileges, launch the **Active Directory Users and Computers** application.
- Step 2** Create a new group.



Note This group is for accounts that WAAS will use to optimize Exchange traffic. Normal users and computers should not be added to this group.

- a. Right-click the **Unit** to contain the new group and choose **New > Group** (Figure 12-7).

Figure 12-7 Active Directory—Add Group



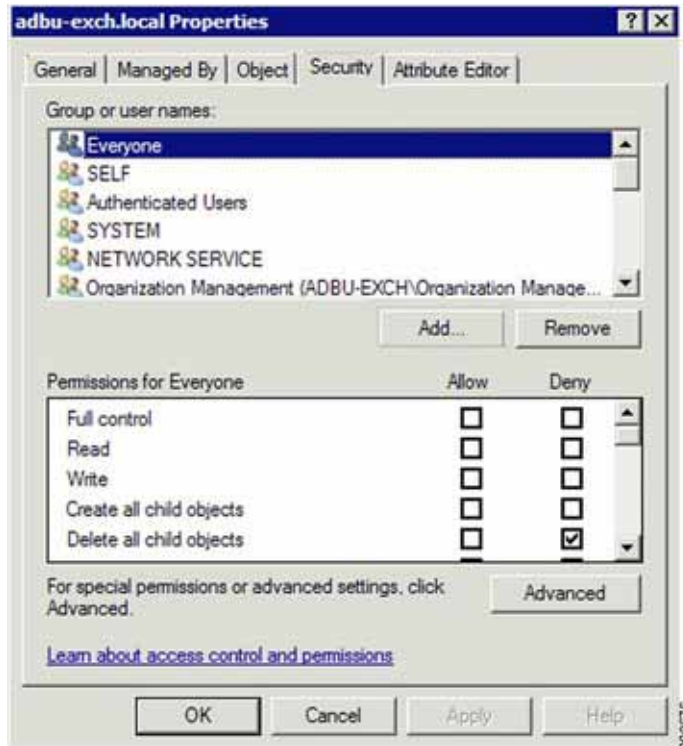
- b. Enter a name in the Group name field and select the following attributes:
- Group scope: Universal
 - Group type: Security
- c. Click **OK**.

- Step 3** Configure the permissions required by WAAS.

- a. In the Active Directory Users and Computers application window, choose **View > Advanced Features** from the menu bar.

- b. Right-click the root of the domain and choose **Properties**.
- c. Click the **Security** tab (Figure 12-8).

Figure 12-8 Active Directory—Security Tab



- d. Click **Add** in the Group or User Names section.
- e. Enter the name of the new group in the Enter the object names to select field.
- f. Click **OK** to add the new group to the list.
- g. Check the check box adjacent to the new group in the Group or user names list and set the following permissions to **Allow**:
 - Replicating Directory Changes
 - Replicating Directory Changes All
- h. Click **OK**.

Step 4 Add an account to the group.

User or workstation (computer) accounts must be added to the new group for WAAS Exchange Encrypted email optimization.

- a. Right-click on the account you want to add and select the **Member Of** tab.
- b. Click **Add**.
- c. Choose the new group you created and click **OK**.

Active Directory permissions configuration is complete.

Managing Domain Identities and Encrypted MAPI State

This section contains the following topics:

- [Editing an Existing Domain Identity](#)
- [Deleting an Existing Domain Identity](#)
- [Disabling Encrypted MAPI](#)
- [Encrypted MAPI Acceleration Statistics](#)

Editing an Existing Domain Identity

You can modify the attributes of an existing domain identity on a WAAS device, if needed.



Note

If the password for a user account has been changed in the Active Directory, you must edit the user account domain identity on the WAAS device to match the new Active Directory password.

The following restrictions apply:

- For a machine account identity, only the state of the domain identity (enabled or disabled) can be modified from a WAAS device.
- For a user account identity, only the state of the domain identity (enabled or disabled) and the password can be modified from a WAAS device.

To change the password for a user account domain identity on a WAAS device when the password for the account in the Active Directory has changed, follow these steps:

-
- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
 - Step 2** From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.
The Encrypted Services window appears.
 - Step 3** Select the user account domain identity to modify and click the **Edit** icon.
The Domain Identity window appears.
 - Step 4** Change the password in the Password field. The password should be the same as the password for the account in Active Directory.
 - Step 5** Click **OK**.
-

Deleting an Existing Domain Identity

To delete a domain identity on a WAAS device, follow these steps:

-
- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
 - Step 2** From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.
The Encrypted Services window appears.
 - Step 3** Select one or more domain identities to delete and click the **Delete** icon to remove the domain identity configured on the WAAS device.

A warning message appears if the domain identity is being used for optimizing encrypted traffic.

- Step 4** Click **OK** to accept or **Cancel** to abort the procedure.
-

Disabling Encrypted MAPI

To disable Encrypted MAPI, follow these steps:

-
- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** Disable Encrypted Service.
- From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.
The Encrypted Services window appears.
 - Uncheck the **Enable Encrypted Service** check box.
 - Click **Submit** to save your changes.
- Step 3** Disable Encrypted MAPI Traffic Optimization.
- From the menu, choose **Configure** > **Acceleration** > **Enabled Features**.
The Enabled Features window appears.
 - Uncheck the **Encrypted MAPI Traffic Optimization** check box.
 - Click **Submit** to save your changes.
-

Encrypted MAPI Acceleration Statistics

To view the statistics for Encrypted MAPI connections, see [Using Predefined Reports to Monitor WAAS](#) in Chapter 15, “Monitoring and Troubleshooting Your WAAS Network,” and see the MAPI acceleration reports.

Cisco WAAS MAPI RPC over HTTP

For WAAS v5.5.3, and for WAAS v6.1.1 and later, Cisco WAAS enables support for optimization of Microsoft Outlook and Microsoft Exchange traffic using Cisco WAAS MAPI RPC over HTTP and HTTPS protocol.

This section describes the following Cisco WAAS MAPI RPC over HTTP features:

- [Microsoft Outlook and Exchange Versions Supported for Cisco WAAS MAPI RPC over HTTP](#)
- [Optimizing MAPI RPC over HTTPS](#)
- [Cisco WAAS MAPI RPC over HTTP CLI Commands](#)
- [MAPI Acceleration Charts for Cisco WAAS MAPI RPC over HTTP](#)

Microsoft Outlook and Exchange Versions Supported for Cisco WAAS MAPI RPC over HTTP

Table 2 shows the clients and servers supporting WAAS MAPI RPC over HTTP:

Table 2 *Clients and Servers Supporting WAAS MAPI RPC over HTTP*

Clients Supported	Servers Supported
Outlook 2013 (for Windows 7 and Windows 8)	Exchange 2013 (for Windows Server 2012, 2012 R2, 2008 R2 [full installation])
Outlook 2010 (for Windows 7 and Windows 8)	Exchange 2010 (for Windows Server 2012, 2012 R2, 2008, and 2008 R2)
Outlook 2007 (for Windows Vista, Windows 7)	



Note

If HTTP-AO or SSL-AO is disabled, the MAPI RPC over HTTP optimization feature will not work.

Optimizing MAPI RPC over HTTPS

The WAAS software supports optimizing MAPI RPC over HTTPS, which allows the client and server to use the DCE/RPC protocol over an encrypted connection.

To support optimizing MAPI RPC over HTTPS, follow these steps:

- Step 1** Configure SSL acceleration. For more information on configuring SSL acceleration, see the [“Configuring SSL Acceleration”](#) section of the *Cisco Wide Area Application Services Configuration Guide*.
- Step 2** When you configure SSL acceleration, be sure to enable protocol chaining, by checking the **Enable protocol chaining** check box on the SSL Accelerated Services window.



Note

If protocol chaining is not enabled, the WAAS device will only optimize SSL traffic on the specified IP address and port.

Cisco WAAS MAPI RPC over HTTP CLI Commands

New CLI Commands for MAPI RPC over HTTP

The following CLI commands have been added for Cisco WAAS MAPI RPC over HTTP.

- show statistics accelerator mapi
- show statistics accelerator mapi rpc-http

CLI Commands Modified for MAPI RPC over HTTP

The following CLI commands have been modified for Cisco WAAS MAPI RPC over HTTP.

- show accelerator mapi
- [no] debug accelerator mapi rpc-http

MAPI Acceleration Charts for Cisco WAAS MAPI RPC over HTTP

The MAPI Acceleration report displays MAPI acceleration statistics. For WAAS Version 5.5.3 and above, the following MAPI acceleration charts are added or modified:

- MAPI: Handled Traffic Pattern—A new pie diagram that shows the three different types of traffic handled by the MAPI AO. For more information, see [MAPI: Handled Traffic Pattern](#) in Chapter 15, “Monitoring and Troubleshooting Your WAAS System.”
- MAPI: Connection Details—An existing chart for MAPI session connection statistics, MAPI: Connection Details now includes a new classification for optimized TCP and RPC-HTTP(S) MAPI connections. For more information, see [MAPI: Connection Details](#) in Chapter 15, “Monitoring and Troubleshooting Your WAAS System.”

Configuring SMB Acceleration

The SMB application accelerator handles optimizations of file server operations. These optimizations apply to SMBv1, SMBv2 and SMBv3. It can be configured to perform the following file server optimizations:

- SMB Print Optimization—A centralized print deployment reduces management overhead and increases cost savings. SMB Print Optimization optimizes print traffic by utilizing a centralized printer server, which resides in the data center. This removes the need for local print servers in the branches. The three most common uses for a centralized printer server are: to print from branch client to branch printer, to print from branch client to data center printer, and to print from data center client to branch printer.
- Read Ahead Optimization—The SMB accelerator performs a read-ahead optimization (SMBv1 only) on files that use the oplocks feature. When a client sends a read request for a file, it is likely that the accelerator may issue more read requests for the same file. To reduce the use of network bandwidth to perform these functions over the WAN on the file server, the SMB accelerator performs read-ahead optimization by proactively reading more file data than what has been initially requested by the client.
- Directory Listing Optimization—A significant portion of the traffic on the network is for retrieving directory listings. The SMB accelerator optimizes directory listings from the file server by prefetching. For directory prefetching, a request from the client is expanded to prefetch up to 64 KB of directory listing content. The SMB accelerator buffers the prefetched directory listing data until the client has requested all the data. If the directory listing size exceeds 64 KB, a subsequent request from the client is expanded by the SMB accelerator again to prefetch content up to 64 KB. This continues until all the entries of the directory are returned to the client.
- Directory Browsing Optimization - The SMB accelerator optimizes directory browsing by prefetching SMBv2 data from the file server and caching it in the RAM infrastructure of the WAE. When directory query requests are made by the client, the data is fetched from the cached data. To accommodate multiple client requests, locking mechanisms are in place while accessing parent directory and child files. Additionally, because the infrastructure has limited memory, new requests are cached only when memory is available.

- **Metadata Optimization**—The SMB accelerator optimizes fetching metadata from the file server through metadata prefetching. Additional metadata requests are tagged along with the client request and are sent to the file server to prefetch more information levels than what was requested by the client.
- **Named Pipe Optimization**—The SMB accelerator optimizes frequent requests from Windows Explorer to the file server to retrieve share, server, and workstation information. Each of these requests involves a sequence of operations that include opening and binding to the named pipe, making the RPC request, and closing the named pipe. Each operation incurs a round trip to the file server. To reduce the use of network bandwidth to perform these functions over the WAN on the file server, the SMB accelerator optimizes the traffic on the network by caching named pipe sessions and positive RPC responses.
- **Write Optimization**—The SMB accelerator performs write optimization by speeding up the write responses to the client by acknowledging the Write requests to the client whenever possible and, at the same time, streaming the Write requests over the WAN to the server.
- **Not-Found Metadata caching**—Applications sometimes send requests for directories and files that do not exist on file servers. For example, Windows Explorer accesses the Alternate Data Streams (ADS) of the file it finds. With negative Not-Found (NF) metadata caching, the full paths to those nonexistent directories and files are cached so that further requests for the same directories and files get local denies to save the round trips of sending these requests to the file servers.
- **DRE-LZ Hints**—The SMB accelerator provides DRE hints to improve system performance and resources utilization. At the connection level, the SMB accelerator uses the BEST_COMP latency sensitivity level for all connections, because it gives the best compression. At the message level, the SMB accelerator provides message-based DRE hints for each message to be transmitted over the WAN.
- **Microsoft Optimization**—The SMB accelerator optimizes file operations for Microsoft applications by identifying lock request sequences for file name patterns supported by Microsoft Office applications.
- **Invalid FID Optimization**—The SMB accelerator optimizes SMB2 and SMB3 clients by locally denying attempts to access files with invalid file handle values instead of sending such requests to the file servers.
- **Batch Close Optimization**—The SMB accelerator performs asynchronous file close optimizations on all SMB traffic.
- **Read Cache optimization**—The SMB accelerator optimizes read operations in SMB2 by caching read response data so that files can be served locally.
- **Write Optimization** —The SMB accelerator improves system performances by performing asynchronous write operations.
- **Signed Optimization** — The SMB accelerator provides L7 optimization of all SMB traffic. For more information, please refer to the additional details under Step 7 below.

To enable the SMB accelerator, check the **SMB Accelerator** check box in the Enabled Features window. To configure the SMB acceleration settings, follow these steps:

- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** Choose **Configure** > **Acceleration** > **SMB Settings**.
The SMB Settings window appears (Figure 12-9).

Figure 12-9 SMB Accelerator Configuration Window

Optimization Bypass Settings

Highest Dialect Optimized :

Highest Dialect Optimized Exceed Action :

Bypass File Name Pattern:

Object Cache Settings

☒ SMB Object Cache

SMB Sianina Optimization Settings

- Step 3** From the **Highest Dialect Optimized** drop-down list, choose the highest dialect to optimize. The available options are:
- NTLM 0.12 or NTLM 1.0
 - SMB 2.0
 - SMB 2.1
 - SMB 3.0
 - SMB 3.02
- Step 4** From the **Highest Dialect Optimized Exceed Action** drop-down list, choose the action for the dialects that are higher than the one chosen as the highest dialect to optimize:
- **Mute**—The dialects higher than the one chosen as the highest dialect to optimize are removed from the negotiation list. This is the default selection.



Note

The Mute option of SMB AO is deprecated in dialects 3.x and 2.0 of SMB; muting within these versions has been found to be unsuccessful in terms of optimization.

- **Handoff**—If the negotiated dialect is higher than the chosen highest dialect to optimize, the connection is handed off to the generic accelerator.

- Step 5** In the Bypass File Name Pattern field, enter the patterns for the file names that you want the SMB accelerator to bypass optimization for. The files whose names match the specified expressions are not optimized.
- Step 6** Check the SMB Object Cache check box if you want to enable disk caching for SMB traffic.
- Step 7** Check the **Signing Optimization** check box to enable optimization of signed SMB v2 and v3 traffic. This check box is checked by default.

An SMB connection request can originate from the Branch office to the Data Center or vice-versa. For every connection, the WAE near the requestor, takes the Edge WAE's role and WAE near the smb server takes the Core WAE's role.

The following prerequisites, at the Core and Edge WAE, are necessary to ensure that a signed connection is optimized:

- On the Core WAE, configure a valid user-identity with administrator privileges to enable secret-retrieval to fetch and cache the long term service key of the smb server using the global configuration command:

```
(config)#windows-domain encryption-service identity [identity] user-account name
[admin-username] domain <your.domain> realm [YOUR.DOMAIN] password
```

Verify the identity configuration by using the following EXEC Command.

```
sh windows-domain encryption-service identity detail
```

For Kerberos Authentication, ensure time synchronization between Client, Server, Core WAE and the Domain Controller.

If you want to verify if a connection is signed or not you can do so by looking into the **SMBv2 Negotiate** packet. The **Signing Required** field should be set to "True" in either the Negotiate Request or the Negotiate Response exchange.

These configurations are similar to the eAPI configuration. For more information, see step 6 of [Configuring Encrypted MAPI Settings](#).

- Verify that the WAN Secure mode is enabled. WAN Secure's secure connection enables the key to be transported to the Edge WAE.

The default recommended mode is Auto. You can verify the state of WAN Secure mode using the following EXEC command:

```
show accelerator wansecure
```

If necessary, you can change the state of WAN Secure using the following global configuration command:

```
accelerator smb wansecure-mode {always | auto | none}
```

- Verify if the WAE devices are registered and are online with the WAAS Central Manager.

- Step 8** Click the **SMBV1 Optimization Settings** tab to perform the following tasks:
- Check the **Meta Data Optimization** check box to enable metadata optimization. This check box is checked by default.

- Check the **Microsoft Office Optimization** check box to enable optimizations for all versions of Microsoft Office. The SMB accelerator does not perform read-ahead, write, and lock-ahead optimizations for Microsoft Office if this optimization is disabled. This check box is checked by default.
- Check the **Named Pipe Optimization** check box to enable named pipe optimization by caching named pipe sessions and positive RPS responses. This check box is checked by default.
- Check the **‘Not Found’ Cache Optimization** check box to enable caching pathnames of files not found. This check box is checked by default.
- Check the **Print Optimization** check box to enable SMB to configure a centralized print deployment. This check box is checked by default.
- Check the **Read Ahead Optimization** check box to enable the SMB to optimize the quantity of read-ahead data from the file. The SMB performs a read-ahead optimization only when the file is opened using the oplocks feature. This check box is checked by default.
- Check the **Write Optimization** check box to enable the write optimization by speeding up the write responses to the client. This check box is checked by default.

Click **SMBV2 Optimization Settings** tab to perform the following tasks:

- Check the **Batch Close Optimization** check box to enable asynchronous files close optimizations. This check box is checked by default.
- Check the **Invalid FID Optimization** check box to enable optimization of files with invalid file handle values. This check box is checked by default.
- Check the **SMBV2 Read Cache Optimization** check box to enable read response caching. This check box is checked by default.
- Check the **SMBV2 Write Optimization** check box to enable asynchronous write operations. This check box is checked by default.
- Check the **Directory Service Optimization** check box to enable optimization of directory browsing performance for SMB v2 traffic. The check box is checked by default. Directory service optimization is available only on devices or device groups running software image 6.1.1.

Click **SMBV3 Optimization Settings** tab to perform the following tasks:

- Check the **SMB v3 Batch Close Optimization** check box to enable asynchronous files close optimizations. This check box is checked by default.
- Check the **SMB v3 Invalid FID Optimization** check box to enable optimization of files with invalid file handle values. This check box is checked by default.
- Check the **SMB v3 Read Cache Optimization** check box to enable read response caching. This check box is checked by default.
- Check the **SMB v3 Write Optimization** check box to enable asynchronous write operations. This check box is checked by default.

Step 9 Click **Submit** to save the changes.

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

Configuring ICA Acceleration

The Independent Computing Architecture (ICA) application accelerator provides WAN optimization on a WAAS device for ICA traffic that is used to access a virtual desktop infrastructure (VDI). This is done through a process that is both automatic and transparent to the client and server.

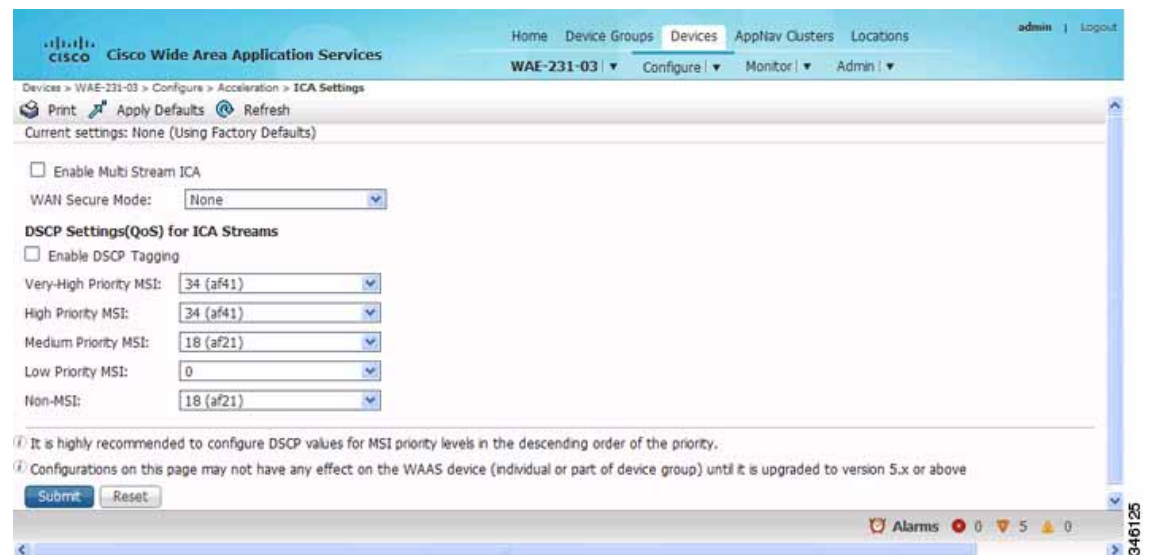
ICA acceleration is enabled on a WAAS device by default.

To enable the ICA accelerator, check the **ICA Accelerator** check box in the Enabled Features window (Figure 12-10).

To configure the ICA acceleration settings, follow these steps:

- Step 1** From the WAAS Central Manager menu, choose **Devices > device-name** (or **Device Groups > device-group-name**).
- Step 2** Choose **Configure > Acceleration > ICA Settings**.
The ICA Acceleration Configuration window appears.

Figure 12-10 ICA Acceleration Configuration Window



- Step 3** Check the **Enable Multi Stream ICA** check box to allow the client and server up to three additional TCP connections that optimize multistream ICA traffic.
- Step 4** From the **WAN Secure Mode** drop-down list, choose the mode. The options are:
 - **None**—Disables WAN Secure mode for ICA. This is the default.
 - **Always**—Enables WAN Secure mode for ICA.



Note The state of WAN Secure mode in both Branch WAE and Data Center WAE must match for connections to get optimized with the ICA accelerator.

- Step 5** In the DSCP Settings (QoS) under ICA Streams section, check the **Enable DSCP Tagging** check box to configure DSCP values for MSI priority levels. These values override the defaults. The valid range is from 0 to 63.



Note Configure DSCP values for MSI priority levels in the descending order of the priority.

- a. Very High-Priority MSI—Typically real-time traffic, such as audio. The default is af41.
- b. High-Priority MSI—Typically interactive traffic. The default is af41.
- c. Medium-Priority MSI—Typically bulk data. The default is af21.
- d. Low-Priority MSI—Typically background traffic, such as printing. The default is 0—best effort.
- e. Non-MSI—(the default is af21)



Note MSI priority configuration might not apply to devices earlier than WAAS Version 5.1.x.

Step 6 Click **Submit**.

The changes are saved to the device or device group.



Note Citrix ICA versions 7.x (XenApp and XenDesktop) contain changes affecting the optimization efficiency of WAAS compared to that achieved with Citrix ICA versions 6.x. To maximize the effectiveness of WAAS, the Citrix administrator should configure the following:

Adaptive Display: Disabled

Legacy Graphic Mode: Enabled

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

To verify the status of WAN Secure mode from the CLI, use the **show accelerator wansecure EXEC** command.

Configuring ICA over SSL

The WAAS software supports optimizing ICA over SSL. This allows the client and server to use the ICA protocol over an encrypted connection. To support optimizing ICA over SSL, you must perform the following steps:

- Configure ICA acceleration. See [Configuring ICA Acceleration](#).
- Configure SSL acceleration. See [Configuring SSL Acceleration](#).



Note When you are configuring SSL acceleration, be sure to enable protocol chaining. If protocol chaining is not enabled, the WAAS device will only optimize SSL traffic on the specified IP Address and Port.

Configuring SSL Acceleration

The SSL (Secure Sockets Layer) application accelerator optimizes traffic on 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**

On a WAAS Express device, only SSL cipher list, SSL certificate authorities, and SSL peering service configuration are supported.

**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 that goes 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. If a TLSv1.1 or TLSv1.2 client request is received, negotiation to downgrade to TLS v1.0 occurs. If refused by the client, the traffic is passed through.

[Table 12-3](#) provides an overview of the steps you must complete to set up and enable SSL acceleration.

Table 12-3 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 Preparing to Use SSL Acceleration .
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 Enabling Secure Store, Enterprise License, and SSL Acceleration .
3. Enable SSL application optimization.	Describes how to activate the SSL acceleration feature. For more information, see Enabling and Disabling the Global Optimization Features .
4. Configure SSL acceleration settings.	(Optional) Describes how to configure the basic setup of SSL acceleration. For more information, see Configuring SSL Global Settings .
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 Working with Cipher Lists .
6. Set up CA certificates.	(Optional) Describes how to select, import, and manage certificate authority (CA) certificates. For more information, see Working with Certificate Authorities .
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 Configuring SSL Management Services .
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 .
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 Using SSL -Accelerated Services .

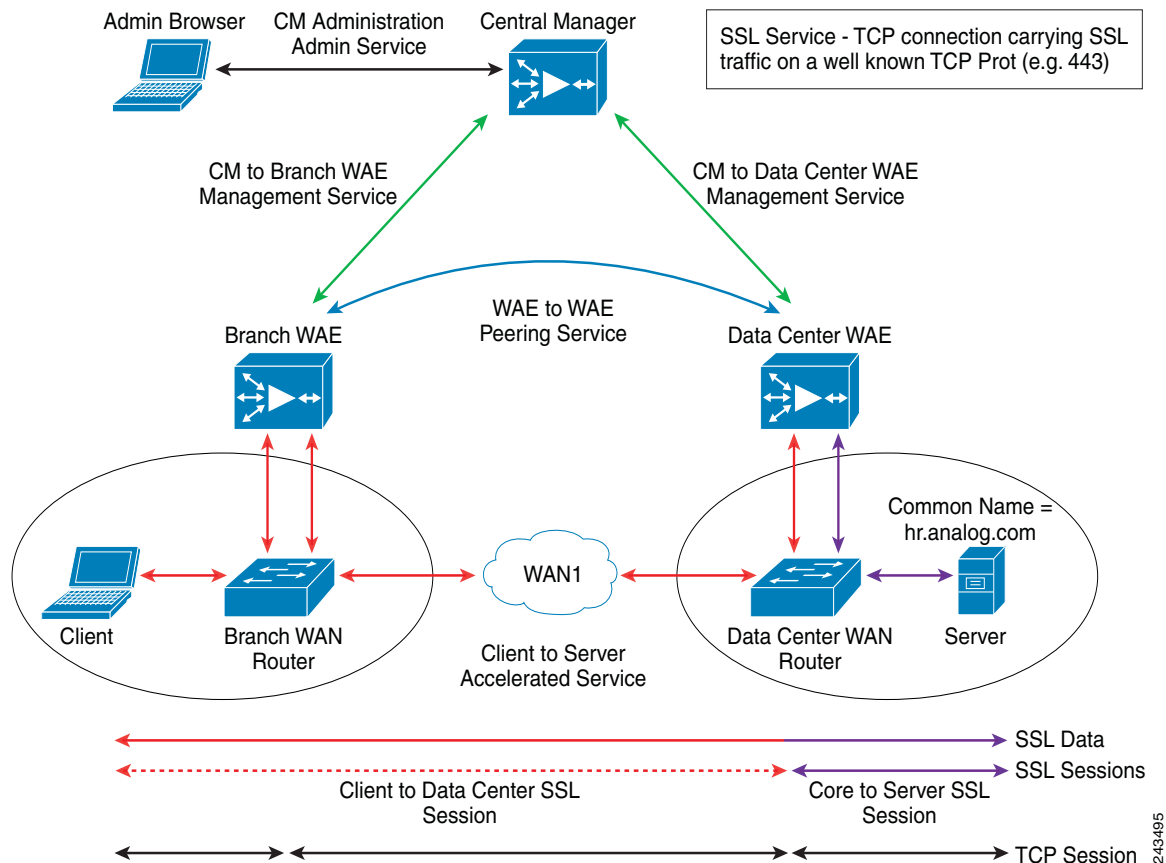
Preparing to Use SSL Acceleration

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 CA-signing information
- The cipher suites supported
- The SSL versions supported

Figure 12-11 shows how the WAAS software handles SSL application optimization.

Figure 12-11 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 should have its secure store initialized and unlocked or opened, but does not have 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, 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 [Configuring Secure Store Settings](#) in Chapter 10, “Configuring Other System Settings.”

Step 2 Enable the Enterprise license.

To enable the Enterprise license, see [Managing Software Licenses](#) in Chapter 10, “Configuring Other System Settings.”

Step 3 Enable SSL acceleration on devices.

To enable the SSL acceleration feature, see [Enabling and Disabling the Global Optimization Features](#).



Note

If the SSL accelerator is already running, you must wait for two datafeed poll cycles to be completed 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 SSL acceleration global settings, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).

Step 2 Choose **Configure** > **Security** > **SSL** > **Global Settings**.

The SSL Global Settings window appears ([Figure 12-12](#)).

Figure 12-12 SSL Global Settings Window

SSL Global Settings for WAE, wae84-07-psirt2-br-wae1

Current applied settings from WAE, wae84-07-psirt2-br-wae1

SSL version:

Revocation settings

Revocation check:

☐ Ignore OSCP failures

OCSP Responder URL:

Cipher List

CipherList:

CipherList Configured

CipherList Name:

	Priority	Cipher
<input type="checkbox"/>	1	dhe-rsa-with-aes-256-cbc-sha
<input type="checkbox"/>	1	rsa-with-aes-256-cbc-sha
<input type="checkbox"/>	1	dhe-rsa-with-aes-128-cbc-sha
<input type="checkbox"/>	1	rsa-with-aes-128-cbc-sha
<input type="checkbox"/>	1	dhe-rsa-with-3des-ede-cbc-sha
<input type="checkbox"/>	1	rsa-with-3des-ede-cbc-sha

Certificate and private key

[Generate self-signed certificate and private key](#)

[Import existing certificate and optionally private key](#)

[Export certificate and key](#)

[Generate certificate signing request](#)

Note: * - Required field

334/408

- Step 3** 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 the 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 4** From the SSL version drop-down list, 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 5** (Optional) Set the Online Certificate Status Protocol (OCSP) parameters for certificate revocation:
- From the OCSP Revocation check drop-down list, choose 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.
 - If the **Ignore OCSP failures** check box is enabled, the SSL accelerator will treat the OCSP revocation check as successful if it does not get a definite response from the OCSP responder.
- Step 6** From the Cipher List drop-down list, choose a list of cipher suites to be used for SSL acceleration. For more information, see [Working with Cipher Lists](#).
- Step 7** Choose a certificate/key pair method ([Figure 12-13](#)).

Figure 12-13 *Configuring Service Certificate and Private Key*

Server Certificate and private key
Generate self-signed certificate and private key
Import existing certificate and optionally private key
Export certificate and key
Generate certificate signing request
Optional Client Certificate and private key
Import existing client certificate and optionally 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 is used by the CA to generate a new certificate.



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

- Click **Import existing client certificate and optionally private key** to use the client configured certificate.

For information about service certificate and private key configuration, see [Configuring a Service Certificate and Private Key](#).

Step 8 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 ([Figure 12-14](#)), follow these steps:

Figure 12-14 Self-Signed Certificate and Private Key

Generate self-signed certificate and private key

☐ Mark private key as exportable

Key Size:*

Common Name:*

Organization:

Organization Unit:

Location:

State:

Country:

Email:

Expires in:*

243841

- 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 (Figure 12-15), follow these steps:



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

Figure 12-15 Importing Existing Certificate or Certificate Chain

Import existing certificate and optionally private key

☐ Mark private key as exportable

☒ Upload file in PKCS#12 format

☐ Upload file in PEM format

☐ Paste certificate and key in PEM-format

Passphrase to decrypt private key:

Upload:

243842

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

If the certificate and private key are already configured, you can update only the certificate. 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 CA, or to update an expiring certificate.

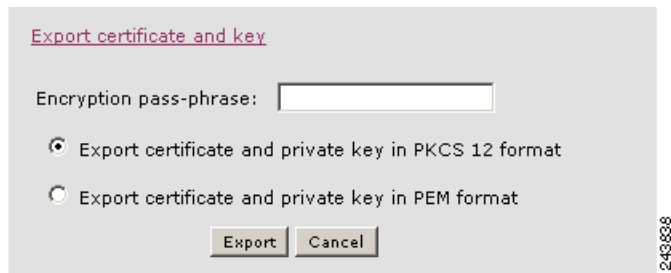
The Central Manager allows importing a certificate chain consisting of an end certificate that must be specified first, a chain of intermediate CA certificates that sign the end certificate or intermediate CA certificate, and end with a root CA.

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 (Figure 12-16), follow these steps:

Figure 12-16 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 the case of PEM format, the both certificate and private key are included in single PEM file.



Note

Central Manager will not allow the export of certificate and private key if the certificate and key were marked as nonexportable when they were generated or imported.

Step 4 To generate a certificate-signing request from a current certificate and private key (Figure 12-17), follow these steps:

Figure 12-17 Generate Certificate-Signing Request

Generate certificate signing request

Common Name: *

Organization:

Organization Unit:

Location:

State:

Country:

Email:

243840

- Step 5** To update the current certificate with one signed by the Certificate Authority:
- Generate PKCS#10 certificate signing request.
 - Send generated certificate signing request to Certificate Authority to generate and sign certificate.
 - 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.

- Step 6** To import an existing client certificate or certificate chain and, optionally, private key (Figure 12-18), follow these steps:

Figure 12-18 Import existing client certificate and optionally 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. To import existing client certificate 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 client 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.

- c. Enter a pass-phrase to decrypt the private key, or leave this field empty if the private key is not encrypted.
- d. Click **Choose File** to navigate to the client configured certificate and **Import Client Cert** to successfully import the above 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:

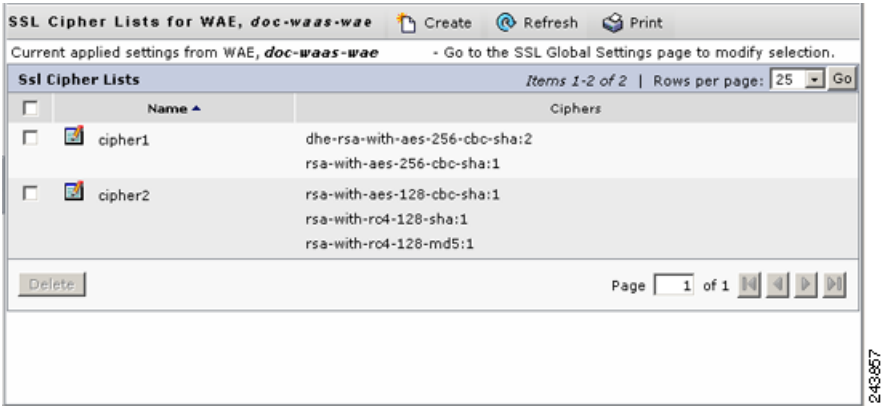
- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** Choose **Configure** > **Security** > **SSL** > **Cipher Lists**.

The SSL Cipher Lists window appears (Figure 12-19).



Note For a WAAS Express device, the SSL Cipher Lists window shows the same name and cipher fields, but in a slightly different format.

Figure 12-19 SSL Cipher Lists Window



Step 3 Click **Create** to add a new cipher list.

The Creating New SSL Cipher List window appears (Figure 12-20).



Note For a WAAS Express device, click **Add Cipher List** to add a new cipher list.

Figure 12-20 Creating New SSL Cipher List Window

Creating new Ssl Cipher List, Ssl Cipher List

Ssl Cipher List

CipherList Name:

Add New Cipher

Priority: Ciphers:

Cipher list Configured

<input type="checkbox"/>	Priority	Cipher
<input type="checkbox"/>	1	dhe-rsa-with-aes-256-cbc-sha

Note: * - Required Field

Step 4 Type a name for your cipher list in the Cipher List Name field.

Step 5 Click **Add Cipher** to add cipher suites to your cipher list.



Note For a WAAS Express device, select the ciphers you wish to add, skip to [Step 12](#).

Step 6 From the Ciphers drop-down list, choose the cipher suite that you want to add.



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

Step 7 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 8 Click **Add** to include the selected cipher suite on your cipher list, or click **Cancel** to leave the list as it is.

Step 9 Repeat [Step 5](#) through [Step 8](#) to add more cipher suites to your list as desired.

Step 10 (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 priorities assigned in this cipher list are only applicable if the cipher list is applied to SSL peering and management services.

- Step 11** (Optional) To remove a cipher suite from the list, check the cipher suite's box and then click **Delete**.
- Step 12** Click **Submit** when you are done configuring the cipher list.

**Note**

For a WAAS Express device, click **OK** to save the cipher list configuration.

SSL configuration changes will not be applied on the device until the security license has been enabled on the device.

Working with Certificate Authorities

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

To manage your CA certificates, follow these steps:

- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** Choose **Configure** > **Security** > **SSL** > **Certificate Authorities**.

The SSL CA Certificate List window appears ([Figure 12-21](#)).

**Note**

For a WAAS Express device, the SSL CA Certificate List window shows the same Name, Issued To, Issuer, and Expiry Date fields, but in a slightly different format.

There is also an **Aggregate Settings** field configurable as Yes or No. To finish the procedure for WAAS Express, skip to [Step 4](#).

Figure 12-21 SSL CA Certificate List Window



- Step 3** Add one of the preloaded CA certificates that is included with WAAS as follows:
- 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 4 Add your own CA certificate as follows:

- a. Click **Create**.

The Creating New CA Certificate window appears (Figure 12-22).



Note For a WAAS Express device, click **Add CA** to add your own CA certificate. Enter the name and the URL, and then click **Get CA Certificate**. After this, skip to [Step 6](#).

Figure 12-22 Creating New CA Certificate Window

- 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. From the **Revocation check** drop-down list, choose **Disable** 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 one of the following methods:
 - **Upload PEM File**
If you are uploading a file, it must be in a PEM format. Browse to the file that you want to use and click **Upload**.
 - **Paste PEM-encoded Certificate**
If you are pasting the CA certificate information, paste the text of the PEM format certificate into the Paste PEM-encoded certificate field.
 - **Get CA Certificate using SCEP**

This option automatically configures the certificate authority using Simple Certificate Enrollment Protocol (SCEP). If you are using the automated certificate enrollment procedure, enter the CA URL and click **Get Certificate**. The contents of the certificate are displayed in text and PEM formats.

To complete the automated certificate enrollment procedure, configure the SSL auto enrollment settings in [SSL Auto Enrollment](#).

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

Step 5 (Optional) To remove a CA from the list, select it and then click the **Delete** icon located in the toolbar.

Step 6 Click **Submit** after you are done configuring the CA certificate list.



Note For a WAAS Express device, click **OK** to save the CA certificate configuration.

SSL Auto Enrollment

The WAAS SSL acceleration feature allows you to enroll certificates automatically for a device (or device group) using SCEP. After the CA certificate is obtained, configure the SSL auto enrollment settings.



Note You must configure the CA authority before configuring auto enrollment settings.

To configure SSL auto enrollment settings, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices > device-name** (or **Device Groups > device-group-name**).

Step 2 Choose **Configure > Security > SSL > Auto Enrollment**.

The SSL Auto Enrollment Settings window appears ([Figure 12-23](#)).

Figure 12-23 SSL Auto Enrollment Settings Window

The screenshot displays the 'SSL Auto Enrollment Settings' window in the Cisco WAAS management interface. The breadcrumb trail at the top indicates the path: Home > Device Groups > Devices > ApplNav Clusters > Locators > wae-231-02 > Configure > Security > SSL > Auto Enrollment. The window title is 'SSL Auto Enrollment Settings'. Below the title, it states 'Current applied settings from WAE, wae-231-02' and provides a link to 'Go to the SSL Global Settings page to modify selection.' The settings are organized into several sections: 'CA settings' with fields for 'CA URL', 'CA' (a dropdown menu currently showing 'None'), and 'Challenge Password'; 'Certificate Signing Request' with fields for 'Common Name', 'Organization', 'Organization Unit', 'Location', 'State', 'Country', and 'Email-Id'; 'Key Size' with a dropdown menu set to '1024'; and an 'Enroll' section with an unchecked 'Enable Enroll' checkbox. At the bottom, there are two informational messages: 'Please visit the Machine Certificate section in the SSL Global Settings page and the Alerts page to check the enrollment status.' and 'Some or all configuration on this page may not have any effect on the WAE (individual or part of device group) until it is upgraded to version 5.0.1.x or above.' Below these messages are 'Submit' and 'Cancel' buttons.

Step 3 Configure the following CA settings:

- CA URL
- CA—Select the appropriate CA from the drop-down list
- Challenge Password



Note CA, CA URL, and Challenge Password are mandatory for enabling SSL auto enrollment.

Step 4 Configure the following Certificate Signing Request settings:

- Common Name
- Organization and Organization Unit
- Location, State, and Country
- Email-Id

Step 5 From the Key Size drop-down list, choose the key size. Valid values are 512, 768, 1024, 1536, or 2048.

Step 6 Check the **Enable Enroll** box.

Step 7 Click **Submit**.

You can then check the enrollment status in the Machine Certificate section on the SSL Global Settings page and on the Alerts page.

Configuring SSL Management Services

SSL management services are the SSL configuration parameters that affect secure communications between the Central Manager and the WAE devices (Figure 12-11). The certificate/key pairs used are unique for each WAAS device. Therefore, 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 menu, choose **Devices** > *device-name*.
- Step 2 Choose **Configure** > **Security** > **Management Service**.

The Management Services window appears (Figure 12-24).

Figure 12-24 SSL Management Services Window

Priority	Cipher
1	dhe-rsa-with-aes-256-cbc-sha
1	rsa-with-aes-256-cbc-sha
1	dhe-rsa-with-aes-128-cbc-sha
1	rsa-with-aes-128-cbc-sha
1	dhe-rsa-with-3des-ede-cbc-sha
1	rsa-with-3des-ede-cbc-sha

- Step 3 From the SSL version drop-down list, choose the type of SSL protocol to use. Choose **SSL3** for the SSL version 3 protocol, **TLS1** for the Transport Layer Security version 1 protocol, or **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 the primary Central Manager and the standby Central Manager and WAE devices.

Table 12-4 shows the cipher lists supported in Internet Explorer and Mozilla Firefox:

Table 12-4 *Cipher Lists Supported in Internet Explorer and Mozilla Firefox*

Cipher List Name	Internet Explorer	Firefox
dhe-rsa-with-aes-256-cbc-sha	Supported in IE8 and later	Supported
rsa-with-aes-256-cbc-sha	Supported in IE8 and later	Supported
dhe-rsa-with-aes-128-cbc-sha	Supported in IE8 and later	Supported
rsa-with-aes-128-cbc-sha	Supported in IE8 and later	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, but TLSv1 may not be enabled by default. Therefore, you must 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 you submit the changes. If this occurs, reload the page.

- Step 4** In the Cipher List pane, choose a list of cipher suites to be used for SSL acceleration. See [Working with Cipher Lists](#) for additional information.

Configuring SSL Admin Service

You can export the SSL CA signed certificate to enable trusted SSL communication between the WAAS Central Manager and the web browser. The default certificate for enabling SSL communication is the WAAS Central Manager self signed certificate. However, if you would like to use a different certificate, you need to configure it.

To configure the SSL certificate, follow these steps:

-
- Step 1** From the WAAS Central Manager menu, choose **Devices>CM>Configure> Security>SSL Admin Service**.
The default certificate is displayed.
- Step 2** Select the PKI operation
- 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.
The file that you import or export must be in either a PKCS12 format or a Privacy Enhanced Mail (PEM) format.
 - Click Generate Self-signed Certificate Key to have the Central Manager and WAAS device use a self-signed certificate/key pair for SSL.
- Step 3** Click Submit to register the certificate.
-

The Central Manager now uses the selected certificate for SSL communication.

Configuring SSL Peering Service

SSL peering service configuration parameters control the secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections ([Figure 12-11](#)). 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 menu, choose **Devices > device-name**.
- Step 2** Choose **Configure > Security > Peering Service**.
The Peering Service window appears ([Figure 12-25](#)).



Note For a WAAS Express device, the Peering Service window shows a subset of the fields in the standard Peering Service window in a slightly different format.

The cipher list **Priority** setting and the **Disable revocation check of peer certificates** options are not applicable to WAAS Express.

Figure 12-25 SSL Peering Service Window

Peer Services

Current applied settings from WAE, wae04-07-psirt2-br-wae1 - Go to the SSL Global Settings page to modify selection.

SSL version: Inherited

CipherList: Inherited [Create New](#)

CipherList Configured

CipherList Name: Inherited

	Priority	Cipher
<input type="checkbox"/>	1	dhe-rsa-with-aes-256-cbc-sha
<input type="checkbox"/>	1	rsa-with-aes-256-cbc-sha
<input type="checkbox"/>	1	dhe-rsa-with-aes-128-cbc-sha
<input type="checkbox"/>	1	rsa-with-aes-128-cbc-sha
<input type="checkbox"/>	1	dhe-rsa-with-3des-ede-cbc-sha
<input type="checkbox"/>	1	rsa-with-3des-ede-cbc-sha
<input type="checkbox"/>	+	...

Authentication

☐ Enable certificate verification

☐ Disable revocation check of peer certificates

Note: - Required Field

[Submit](#) [Cancel](#)

- Step 3** From the SSL Version drop-down list, 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, **TLS1** for the Transport Layer Security version 1 protocol, or **All** to use both SSL3 and TLS1 SSL protocols.



Note In a WAAS Express device, only SSL3 and TLS1 are supported for the SSL version.

- Step 4** To enable verification of peer certificates, check the **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 5** Check the **Disable revocation check for this service** check box to disable OCSP certificate revocation checking.



Note In a WAAS Express device, this option is not available.

- Step 6** 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.



Note In a WAAS Express device, the list of cipher suites to be used for SSL acceleration is shown in the Cipher List pane.

See [Working with Cipher Lists](#) for additional information.

- Step 7** Click **Submit**.

**Note**

In a WAAS Express device, SSL configuration changes will not be applied on the device until the security license has been enabled on the device.

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 menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** Choose **Configure** > **Acceleration** > **SSL Accelerated Services**.
- Step 3** To delete an accelerated service, select the service and click **Delete**.
- Step 4** Click **Create** to define a new accelerated service. A maximum of 512 accelerated services are allowed. The Basic SSL Accelerated Services Configuration window appears ([Figure 12-26](#)).

Figure 12-26 SSL-Accelerated Services—Basic Window

SSL Accelerated Service

Basic | Advanced

This service is bound to 'SSL' application policy. The optimization actions accelerating traffic matching this service are DRE, LZ and TFO.

Service Name:

In service: ☐

Client version rollback check: ☒

Enable protocol chaining: ☒

Match Server Name Indication: ☐ If enabled, the SSL setup message is parsed for destination hostname (in "Server Name Indication"), which is matched against SANs in the SSL certificate. Recommended for optimizing SaaS apps which typically have dynamic server domains.

Description:

Server addresses

Please specify the IP Address, Hostname or Domain of an accelerated server. Use 'Any' keyword to match any server IP Address. Note that hostname and domain server address types are only supported on devices using WAAS versions 4.2.X or later.

It is recommended to have maximum 32 server entries and up to 64 characters per entry. The combined length of all the server address/port entries should not exceed 2048 characters.

Server: Server Port:

Type	Address	Port

Server Certificate and private key

[Generate self-signed certificate and private key](#)

[Import existing certificate and optionally private key](#)

[Export certificate and key](#)

[Generate certificate signing request](#)

Optional Client Certificate and private key

[Import existing client certificate and optionally private key](#)

Note: * - Required Field

Alarms ● ● ● ● ●

- Step 5** Enter a name for the service in the Service Name field.
- Step 6** To enable this accelerated service, check the **In service** check box.
- Step 7** 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 8** To match subject alternative names, enable the **Match Server Name Indication** check box. For more information, see [Configuring SSL Acceleration for SaaS Applications](#).
- Step 9** To enable protocol chaining, check the **Enable protocol chaining** check box.
Enabling protocol chaining allows other protocols to be optimized over SSL.
- Step 10** (Optional) Type a description of the service in the Description field.
- Step 11** From the Server drop-down list, choose **IP Address**, **Hostname**, or **Domain** as the SSL service endpoint type.

- Step 12** Type the server IP address (or proxy IP address) , hostname, or domain of the accelerated server. Use the keyword **Any** to specify any server IP address.



Note 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 13** Enter the port associated with the service to be accelerated.
- Step 14** 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 15** To remove an IP address from the list, click **Delete**.
- Step 16** Choose a certificate and key pair method ([Figure 12-27](#)).

Figure 12-27 Configuring Service Certificate and Private Key

Server Certificate and private key
Generate self-signed certificate and private key
Import existing certificate and optionally private key
Export certificate and key
Generate certificate signing request
Optional Client Certificate and private key
Import existing client certificate and optionally 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.



Note In case of SaaS applications, the certificate should have the Subject Alternative Name (SAN) information.

- 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 is used by the CA to generate a new certificate.
The file that you import or export must be in either PKCS12 format or PEM format.
- Click **Import existing client certificate and optionally private key** to use the client configured certificate.

For service certificate and private key configuration steps, see [Configuring a Service Certificate and Private Key](#).

**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, and then wait 5 minutes and check the **In service** check box and click **Submit** to re-enable the service. Alternatively, in 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 the accelerated services by disabling and then re-enabling the SSL accelerator.

- Step 17** Click the **Advanced Settings** tab to configure SSL parameters for the service.
The Advanced SSL Accelerated Services Configuration window appears (Figure 12-28).

Figure 12-28 *SSL Accelerated Services—Advanced Window*

The screenshot shows the 'Advanced' configuration window for an SSL Accelerated Service. The 'SSL Settings' section has 'SSL version' set to 'Inherited' and 'CipherList' set to 'Inherited'. Below this is a table for 'Cipher list Configured' with columns for Priority and Cipher. The 'Authentication' section has checkboxes for 'Verify client certificate' and 'Verify server certificate', each with a sub-option to 'Disable revocation check'. The bottom of the window shows a 'Note: * - Required Field' and 'Submit' and 'Cancel' buttons.

Priority	Cipher
1	dhe-rsa-with-aes-256-cbc-sha
1	rsa-with-aes-256-cbc-sha
1	dhe-rsa-with-aes-128-cbc-sha
1	rsa-with-aes-128-cbc-sha
1	dhe-rsa-with-3des-ede-cbc-sha
1	rsa-with-3des-ede-cbc-sha

- Step 18** (Optional) From the SSL version drop-down list, 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, **TLS1** for the Transport Layer Security Version 1 protocol, or **All** to use both SSL3 and TLS1 SSL protocols.
- Step 19** (Optional) From the Cipher List drop-down list, 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 [Working with Cipher Lists](#).
- Step 20** (Optional) To set the OCSP parameters for certificate revocation, follow these steps:
- To enable the 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 21 Click **Submit** after you have finished configuring the SSL accelerated service.

Updating a Certificate/Key in a SSL Accelerated Service

If at some point you need to update a certificate or key in a SSL Accelerated Service, follow these steps:

- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** Choose **Configure** > **Acceleration** > **SSL Accelerated Services**.
- Step 3** Click **Edit SSL Accelerated Service** button in the **Name** column for the service in question.
- Step 4** Choose a certificate and key pair method ([Figure 12-27](#)) to either re-generate a self-signed certificate and private key or to import an updated certificate and/or key.
- Step 5** Depending on the chosen method fill out the required details, then click **Generate** or **Import** and next click **Submit**.



Note When you update a certificate for a SSL Accelerated Service and want it to be used by it, it is important to stop and start the configured SSL Accelerated Service. This step is required because the existing certificate and key are stored in memory on the accelerators. Updating the certificate/key via the steps described above is insufficient because it does not update the certificate/key in memory.
To ensure the updated certificate for the SSL Accelerated Service is used, make sure to follow the steps below as well.

- Step 6** Click the **Edit SSL Accelerated Service** button in the **Name** column for the service in question.
- Step 7** Remove the check mark for **In service**, then click **Submit**.
- Step 8** Click the **Edit SSL Accelerated Service** button in the **Name** column for the service in question for one last time.
- Step 9** Enable the check mark for **In service** then click **Submit**.

Configuring SSL Acceleration for SaaS Applications

SaaS applications are typically served from multiple SSL server farms, with multiple hosts spanning several data centers. For SSL services hosted in the enterprise data center, the IT administrator knows and controls the SSL server IP and can provide it to the data center WAAS. But for a SSL service that is hosted at a third-party SaaS provider in the cloud, the SSL server IP address is not controlled by the IT administrator because the cloud provider uses multiple Content Delivery Networks (CDNs) and data centers. Even for a single SaaS service, there might be multiple server IP addresses that can change dynamically. This leads to inadvertent errors due to namespace/certificate mismatch for SaaS applications.

To avoid these errors and to ensure that these applications are optimized, follow these steps to configure the SSL-accelerated services for SaaS applications:

Step 1 Create an SSL-accelerated service for a SaaS application using Step 1 through Step 8 outlined in [Using SSL -Accelerated Services](#).

Step 2 To match subject alternative names, check the **Match Server Name Indication** check box. Alternately, use the **match sni** command on the core WAAS device.

If enabled, the SSL accelerator parses the initial SSL connection setup message for the destination hostname (in the SSL protocol extension called Server Name Indication) and uses that to match it with the Subject Alternate Names list in the SSL certificate on the WAAS device.



Note We recommend this setting for optimizing cloud-based SaaS applications to avoid namespace/certificate mismatch errors that are caused due to the changing nature of the SaaS server domains and IP addresses.



Note Most modern browsers provide Server Name Indication (SNI) support. Ensure that you use a browser that supports SNI.



Note The Match Server Name Indication option is available only on devices running WAAS 5.3.5 or later.

Step 3 Use the keyword **Any** to specify the server IP address of the accelerated server.

Step 4 Direct all SSL traffic for SAAS applications to port 443.
The above configuration overrides any wildcard configuration.



Note If you have configured port 443 for traffic other than SaaS applications, you should review and reconfigure it appropriately.

Step 5 Click **Import Existing Certificate Key** to upload or paste a certificate/key pair. The certificate should be specifically used for the SaaS-accelerated service and should contain the Subject Alternate Names for the server domains that need to be optimized. Identify the server domains that need to be added for optimizing SaaS applications, by following the steps outlined in [Determining Server Domains Used by SaaS Applications](#).

**Note**

You must create a new certificate with the missing server domain names derived from the list at regular intervals to ensure that the connections are optimized.

- Step 6** Click **Submit** to complete configuring the SSL-accelerated service for the SaaS application.

Determining Server Domains Used by SaaS Applications

When you check the **Match Server Name Indication** check box, you can log in to the core WAAS device and use the **sh crypto ssl services accelerated-service service-name** command to view the list of server domain names that do not match the existing SSL certificate and hence are not optimized. If you want to optimize any of these server domain names, select and add them to your certificate by performing the following steps below.

The server domain names list contains a maximum of 128 server names.

- Step 1** Identify the relevant servers to be added. Use the **sh crypto ssl services accelerated-service service-name** to see additional details regarding the count and last seen information of the server name. If you need additional information to view the IP address and hostnames, use the **debug accelerator ssl sni** command to enable SNI debugs.
- Step 2** Log in to the Microsoft Management Console(MMC), OpenSSL, or any other available customer tool to create a new Certificate Signing Request (CSR) with the relevant server domain names of the SaaS applications in the subject alternative names extension of the certificate. Refer to the highlighted area in the example certificate below.

**Note**

When you add the SAN to the certificate, domain names should be separated by a comma. Note that a list of hostnames on a domain can be secured with a single certificate. For example, a.b.c.com and c.b.com can be added as *.b.c.com. However, for a new hostname on another domain, you have to make a new entry. For example, for b.c.com you have to add it as b.c.com or *.c.com. Additionally, you can also secure hostnames on different base domains in the same certificate, for example a.b.com and a.b.net.

Certificate:

Data:

```
Version: 3 (0x2)
Serial Number:
    ec:aa:9b:10:fa:9d:09:95
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=California, L=San Jose, O=Cisco
Systems Inc, OU=WAAS,
CN=Cisco_WAAS_CA/emailAddress=support@cisco.com
Validity
    Not Before: Jul 31 06:49:56 2013 GMT
    Not After : Aug 30 06:49:56 2013 GMT
Subject: C=US, ST=California, L=San Jose, O=Cisco
Systems Inc, OU=WAAS,
CN=Office365/emailAddress=support@cisco.com
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (1024 bit)
    Modulus:
        00:c6:85:0d:f9:df:4e:4f:c4:53:d5:3e:0f:c4:cb:
        53:42:34:34:7d:92:7f:ea:c1:75:0b:21:3f:5f:a1:
        be:34:f1:40:c3:32:52:a1:05:79:26:7b:a3:29:c5:
```



```

5e:9f:3f:92:6b:d1:b2:fd:bc:c9:2b:8b:e2:9f:1a:
91:83:9b:c8:7f:3f:d9:56:92:75:be:b6:ed:39:39:
2f:1a:2f:ba:39:1b:06:76:0a:17:b5:f0:ec:dd:4c:
fa:94:be:ea:7c:e0:4e:51:b4:d2:75:4d:8b:d9:6e:
de:34:10:c7:c5:e8:97:5f:f2:7f:97:1e:9a:e0:e2:
fc:b4:58:11:45:82:19:14:11
Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment
    X509v3 Subject Alternative Name:
        DNS:*.office365.com, DNS:*.outlook.com, DNS:*.aadcdn.microsoftonline-p.com,
        DNS:*.aspnetcdn.com, DNS:*.client.hip.live.com, DNS:*.hip.live.com,
        DNS:*.linkedinlabs.com, DNS:*.live.com, DNS:*.microsoft.com, DNS:*.microsoftonline-p.com,
        DNS:*.microsoftonline-p.net, DNS:*.microsoftonline.com, DNS:*.microsoftonlineimages.com,
        DNS:*.microsoftonlinesupport.net, DNS:*.msecnd.net, DNS:*.msocdn.com, DNS:*.office.net,
        DNS:*.office365.com, DNS:*.officeapps.live.com, DNS:*.officecdn.microsoft.com,
        DNS:*.onmicrosoft.com, DNS:*.outlook.com, DNS:*.res.outlook.com, DNS:*.sharepoint.com,
        DNS:*.sharepointonline.com, DNS:*.telemetry.microsoft.com,
        DNS:*.testexchangeconnectivity.com, DNS:*.vo.msecnd.net, DNS:*.webtrends.com

Signature Algorithm: sha1WithRSAEncryption
46:db:34:7f:c0:8e:13:81:67:0b:3c:8d:15:3a:ee:1f:c7:cf:
d1:6b:de:00:2a:35:9b:13:d6:bf:79:43:ce:31:c6:f9:de:f7:
20:1f:0e:86:9e:d4:91:01:57:a2:7b:fe:91:00:de:cf:58:90:
85:97:49:b3:11:4c:e9:05:d0:a1:a7:73:7e:50:64:8f:80:f4:
ec:fa:a7:bb:7a:c2:df:5e:c5:e3:a8:52:c4:31:4e:8e:53:36:
59:e9:0f:27:82:71:4e:3b:79:a4:c9:4f:18:7e:06:7a:0c:34:
0a:cf:3c:3e:73:73:5a:52:7d:03:a0:75:50:5a:d4:a5:8b:a9:
ea:96

```

Step 3 Submit the certificate to the Enterprise CA.

Step 4 Import the signed certificate from the Enterprise CA to the Trusted Root Certification Authorities store.\



Note The Enterprise root CA should be present in browser as trusted root CA.

Step 5 Uncheck the **In service** checkbox and click **Submit** to disable the accelerated service.

Step 6 Upload the new certificate and re-enable the service.

Akamai Connect and WAAS

The Akamai Connect feature is an HTTP/HTTPS object cache component that is added to Cisco WAAS. It is integrated into the existing WAAS software stack and is leveraged via the HTTP Application Optimizer.

Akamai Connect helps reduce latency for HTTP/HTTPS traffic for business and web applications, and can improve performance for many applications, including Point of Sale (POS), HD video, digital signage, and in-store order processing. It provides significant and measurable WAN data offload, and is compatible with existing WAAS functions such as DRE (deduplication), LZ (compression), TFO (Transport Flow Optimization), and SSL acceleration (secure/encrypted) for first and second pass acceleration.

This section contains the following topics:

- [Terms Used with Akamai Connect and WAAS](#)
- [Benefits of Adding Akamai Connect to WAAS](#)
- [Considerations for Using Akamai Connect with WAAS](#)
- [Caching Types](#)
- [Akamai Connected Cache](#)
- [OTT Caching](#)
- [Supported WAAS Platforms for Akamai Caching](#)
- [Workflow: Using Akamai Connect](#)
- [Registering, Activating, Enabling Akamai Connect](#)
- [Enabling Akamai Connected Cache](#)
- [Enabling OTT Caching](#)
- [Using HTTP Proxy for Connections to the Akamai Network](#)
- [Setting Caching Policies](#)
- [Setting Cisco Cloud Web Security User Policy](#)
- [Configuring Cache Prepositioning](#)

Terms Used with Akamai Connect and WAAS

The following terms are used with Akamai Connect and WAAS:

- **Akamai Connect** - Akamai Connect is an HTTP/S object cache component added to Cisco WAAS, integrated into the existing WAAS software stack and leveraged via the HTTP Application Optimizer. WAAS with Akamai Connect helps to reduce latency for HTTP/S traffic for business and web applications.
- **Akamai Connected Cache** - Akamai Connected Cache is a component of Akamai Connect, which allows the Cache Engine (CE) to cache content that is delivered by an Edge server on the Akamai Intelligent Platform.

Industry-wide, the terms *mode*, *profile*, and *policy* are sometimes used interchangeably to describe caching types and processes. This document uses these terms as follows:

- **Mode**—The version of transparent caching (Basic, Standard, Advanced, or Bypass).
- **Profile**—The set of host rules and caching types applied as a group, and which follows the CE order of precedence.
- **Policy**—The set of rules and the conditions of caching, applied either individually or as a group, to a device or device group.

Benefits of Adding Akamai Connect to WAAS

The following are some of the benefits of adding Akamai Connect to WAAS:

- Intelligent transparent object caching (by integrating Akamai's cache).
- Seamless integration of Akamai Connect in WAAS software and configuration (with WAAS Central Manager and WAAS CLI).

- Integration with Akamai's Edge Grid Network, which provides low-latency Content Delivery Network transfers (via Akamai Connected Cache).
- Significant and measurable WAN data offload.
- Cache prepositioning (warming) for websites that you specify.
- Hostname rules for cache control of specific websites or domains.
- First and second pass acceleration, because Akamai Connect works with WAAS middle-mile capabilities (including DRE, LZ, TFO, and SSL acceleration)
- Dual-sided or single-sided network deployment, described in [Dual-Sided or Single-Sided Network Deployment](#).

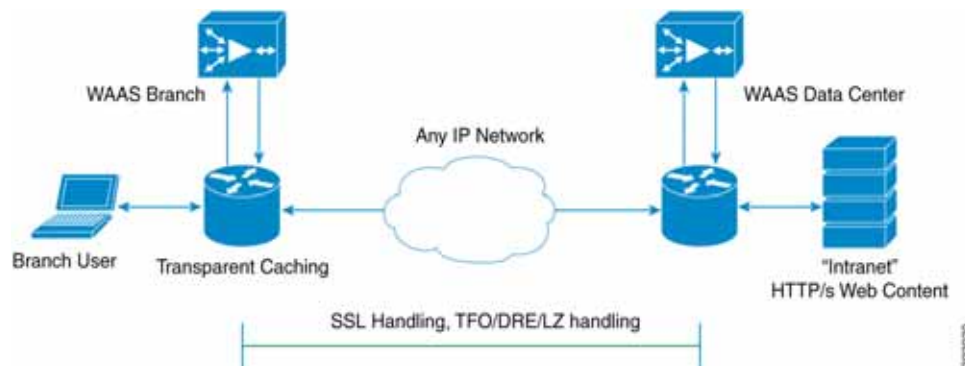
Dual-Sided or Single-Sided Network Deployment

Akamai Connect can be deployed in either a dual-sided or single-sided deployment scenario.

Dual-sided deployment ([Figure 12-29](#)) provides the benefits of existing WAAS technology plus Akamai caching for HTTP and HTTPS traffic.

- Transparent caching of customer-owned, Intranet web resources
- Caching in branch only.
- Includes prepositioning (for non-SSL content).

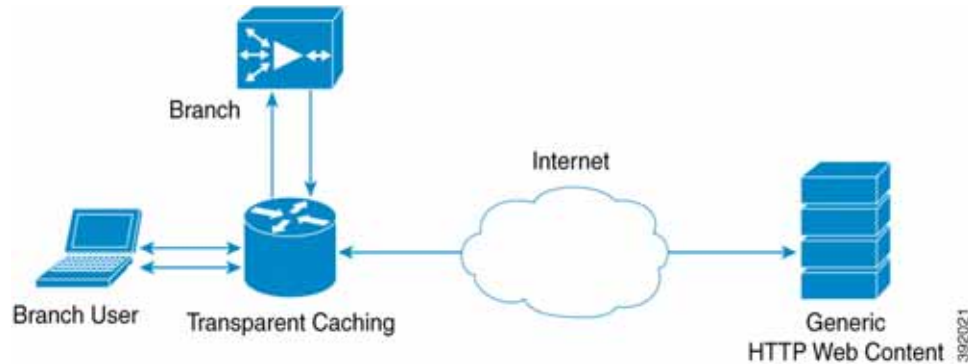
Figure 12-29 Dual-sided Deployment



Single-sided deployment ([Figure 12-30](#)) provides the benefits of HTTP object caching.

- Generic web resources that utilize proxy-specific HTTP cache-control headers.
- Caching in branch only.
- Includes prepositioning (for non-SSL content).
- Single-sided deployment is on by default with transparent caching in Standard mode.

Figure 12-30 Single-sided Deployment



Considerations for Using Akamai Connect with WAAS

The following are some considerations for using Akamai Connect with WAAS:

- You cannot view the contents of the cache, and cannot pin content to make it remain in the cache, for example, for prepositioned content.
- There is no separate cache for HTTPS content. However, data is stored differently for the same site if both HTTP and HTTPS are accessing. (The way the sites are stored in the cache is based on the URL, and this will change between HTTP and HTTPS.)

The CE has no explicit integration with AppNav. The AppNav status is based on the HTTP application accelerator.



Note

The terms *mode*, *profile*, and *policy* are sometimes used interchangeably to describe caching types and processes. This document uses these terms as follows:

Mode—The version of transparent caching (Basic, Standard, Advanced, or Bypass).

Profile—The set of host rules and caching types applied as a group, and which follows the CE order of precedence.

Policy—The set of rules and the conditions of caching, applied either singly or as a group, to device or device group.

Caching Types

WAAS supports transparent caching, Akamai Connected Cache, and Over-the-Top (OTT) caching.

Caching Types: Order of Precedence

When there are multiple caching modes and policies in use, the CE applies an order of precedence in the execution of these. A rule that is higher in the order of precedence is executed first, and any other rules that are applied to that domain or digital property is ignored. The order of precedence is:

1. Transparent caching rules

2. OTT/Akamai Connected Cache
3. Default Transparent policy

For example, if test.com is an Akamai Connected Cache property, but an Advanced mode cache rule is set for this site, then Advanced mode will take precedence and Akamai Connected Cache will be skipped.

**Note**

When cache prepositioning is turned on, it has the same priority as any other caching type.

**Note**

Akamai Connect determines cache type based on most exact hostname match followed by cache priorities. www.host.com is more exact than *.host.com. In this scenario, if a lower-priority cache, such as Akamai Connected Cache (Order of Precedence #2), has a more exact match than a higher priority cache, such as transparent (Order of Precedence #1), the caching will occur with the more exact match and lower-priority cache.

Transparent Caching

Transparent caching (which conforms to the RFC-2616 standard) delivers content from an origin server to the client without any modification. Transparent caching sends a request from a client to a server along with the associated authentication. No changes are made by proxy servers to either the headers or the returned packets along the way, although there are some headers that mark proxy actions that can be altered without the meaning of the cache control headers being altered.

There are four types of transparent caching modes: Basic, Standard, Advanced, and Bypass.

There are two modes in which transparent caching can operate: single-sided mode and dual-sided mode.

**Note**

When accessing transparent caching via HTTPS, the default caching mode is Basic mode. This ensures that no sensitive content is accidentally cached (in Basic mode, only content that you explicitly mark is cached). If you want content cached in a different mode with HTTPS, create a host rule that matches the HTTPS server location. For more information on creating a host rule, see [Setting Caching Policies](#).

Basic Mode

In Basic mode, the CE works in strict RFC-2616 behavior, and therefore, only caches responses that are marked explicitly as cacheable with Cache-Control Headers or that have an Expire header - to service and accelerate traffic from a datacenter to a branch office over any type of IP network. Caching is only in the branch or local router, and content can be cached from the Internet regardless of the location of the original source.

Standard Mode (Default)

In Standard mode (default), the CE also follows RFC-2616 behavior for cache control headers, but with the following differences from Basic mode:

- In Standard mode, the CE does not honor client cache override behavior, for example, must-revalidate and proxy-revalidate.
- If cache-control or expire headers are not present, and Last Modified Time appears, the CE performs a heuristic based on the Last Modified Time and stores objects for 10 percent of their apparent age, up to a maximum of one day.

**Caution**

A properly configured website will work with Standard mode, but login pages, cookie setting pages, or dynamic content not properly marked as cacheable may break. We recommend that you test the website; this is especially important for a newly-created website or one that does not have many users.

Advanced Mode

In Advanced mode, the CE caches media types more aggressively, and caches all object types for longer times (when there is no explicit expiration time). Most of the benefits of Advanced mode over Standard mode occur if the website has not already marked cacheable media content properly. Advanced mode is best suited for media-rich Intranet sites.

If cache-control or expire headers are not present and Last Modified Time appears, the CE performs a heuristic based on the Last Modified Time and stores objects for 20 percent of their apparent age, up to a maximum of one day.

For certain media file types, listed in [Table 12-5](#), Advanced Mode will cache these for a full day if the media type is not specified as uncacheable or the media type has no obvious age in the request. For all other media types, the system caches the object for a minimum of one hour to a maximum of seven days - regardless of whether the Last Modified Time is present.

Table 12-5 *Advanced Mode: Media types that may be cached for a full day*

Advanced Mode: Media types that may be cached for a full day

(if not specified as uncacheable or has no obvious age in the request)

3g2	3gp	aac	aif	aiff	asf	asx	au	avi	bin	bmp
cab	carb	cct	cdf	class	css	dcr	doc	docx	dtd	dv
dvd	dvr	dvr-ms	exe	flv	gcf	gff	gif	grv	html	hqx
ico	ini	jpeg	jpg	js	mlv	m4a	midi	mov	mp3	mp4
mpeg	mpg	mpv	nv	pct	pdf	png	ppc	ppt	pptx	pws
qt	swa	swf	tif	txt	vbs	w32	wav	wbmp	wma	wml
wmlc	wmls	wmlsc	wmv	xsd	xsl	xls	xlsx	zip		

**Caution**

A properly configured website will work in Advanced mode, but Advanced mode may break the presentation of certain web pages if there are even minor caching misconfigurations. We recommend that you test the performance of this caching mode for your applications before you bring the CE into production. When testing, pay particular attention to dynamic URLs and to content that requires authentication to be presented to a client.

Bypass Mode

In Bypass mode, the CE turns off caching for one or more configured sites. When Transparent Bypass mode is set for a particular hostname, the caching for the hostname specified in a rule is suppressed.

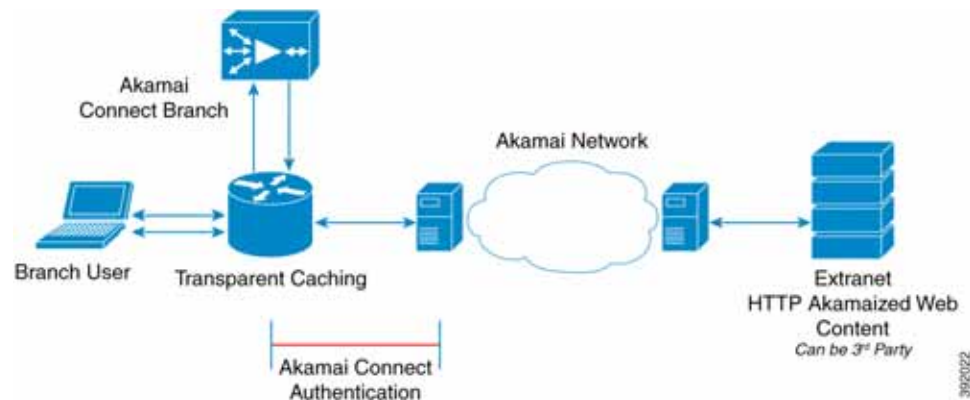
Bypass mode is useful when you want to turn off Akamai Connected Cache or OTT caching for a site or for a part of a site.

For example, if you have servers of the type `images#.bar.com`, you can configure a bypass rule so that only `images2.bar.com` is excluded from caching. All other `images#.bar.com` servers will continue to be cached under the existing rules.

Akamai Connected Cache

Akamai Connected Cache (Figure 12-31) allows the CE to cache content that is delivered by an Edge server on the Akamai Intelligent Platform. This is content that is served by the worldwide Akamai Content Delivery Network (CDN); it is typically not cacheable by enterprise cache engines, but can be cached in Akamai CE based on interactions with network edge elements that are serving it.

Figure 12-31 Akamai Connected Cache



Akamai Connected Cache Features

The following is a list of Akamai Connected Cache features:

- Object caching is done on the client-side WAAS device only.
- Prepositioning can be leveraged to cache HTTP websites delivered via the Akamai Intelligent Platform.
- During the enabling/registration of HTTP object cache, each WAE CE contacts the Akamai network to obtain credentials.
- The WAAS/Akamai CE determines which sites can be “Akamaized” by Akamai Connected Cache from the HTTP headers in the first reply. The CE and the Akamai Edge Server then exchange credentials and agree that Akamai Connected Cache can occur. This is done again via HTTP headers in HTTP request and responses.
- The Akamai Edge Servers can provide objects it is handling, the object that will not change, to allow WAEs with Akamai CE and the correct credentials to cache these objects. Users or other caches without valid credentials will not be allowed to cache.
- The Akamai Edge Server provides additional headers to allow the WAAS/Akamai CE to cache the objects for the objects it handles. The CE forwards this back to the corresponding client. The headers passed between the CE and the client are similar to what the client or enterprise proxy server would see if the WAE was not in the path.

Akamai Connected Cache Requirements

Akamai Connected Cache is enabled by default when you check the **Enable Akamai Connect** check box at the Akamai Connect **Cache Settings** tab (**Configure > Caching > Akamai Connect**).

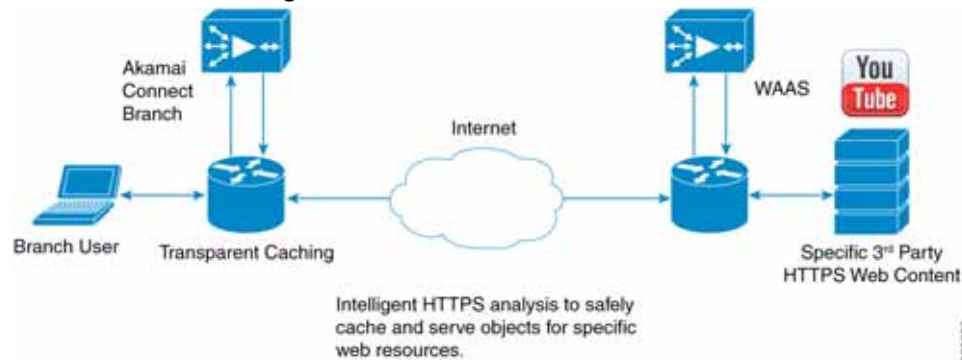
Akamai Connected Cache requires registration and an authentication key to operate. For how to disable/enable Akamai Connected Cache see [Enabling Akamai Connected Cache](#).

OTT Caching

Over-the-Top (OTT) caching caches dynamic content by examining the URL related to a session and a site to determine if the object is identical to the one previously stored in the CE cache. OTT is used for streamed content, particularly video content, and for sites that use dynamic URLs based on session or authentication methods.

OTT is a caching feature that Akamai has engineered to allow WAAS to cache and serve some popular sites that are normally not cacheable. This caching feature requires special metadata that is created and distributed by Akamai. OTT uses metadata logic to determine a unique cache key per video; this allows dynamic URLs to be cached.

Figure 12-32 OTT Caching



This list highlights how OTT functions with WAAS:

- Currently, the CE uses only OTT for one site, YouTube.
- Since YouTube is delivered via HTTPS, you need to follow the same process as you do for SAAS optimization. For more information, see [Configuring SSL Acceleration for SaaS Applications](#). The domains that must be matched are *.youtube.com, *.ytimg.com, *.googlevideo.com, and *.ggpht.com.
- OTT is disabled by default, but enabled after HTTP application accelerator object cache is enabled. For how to enable or disable OTT, see [Enabling OTT Caching](#).

The following is a workflow of the OTT feature with WAAS and Akamai Connect:

1. During the registration process the WAE CE provides metadata for YouTube.
2. A client goes to the YouTube site. (Note that the one client request actually requests the video in chunks, even with a dynamic ID. Each chunk not only contains a part of a video, but has an associated audio/video quality, such as 360p, 480p, or 720p.
3. The Akamai CE uses metadata logic to determine a unique cache key per dynamic ID. The CE stores this for one day, even though YouTube usually expires the dynamic ID in approximately six hours.

- Each time the video is played, the request reaches out to the origin server and fetches the dynamic ID. It then compares this with the dynamic ID and cache key pair in the cache.

If the dynamic ID associated with the video has changed, the video will be served from the origin, and this will result in a miss. A new cache key is generated for that ID and is then stored.

If a match is found, the video is served out of cache.

Supported WAAS Platforms for Akamai Caching

The flow of allocated resources to the CE is controlled by the WAAS Central Manager, but the overall resource pool and the amount of resources that can be allocated to the cache engine is controlled by the hardware platform, and the number of supported connections and users that the router is designed to service.

Table 12-6 shows the WAAS platforms supporting Akamai caching:

Table 12-6 Supported WAAS Platforms for Akamai Caching

Appliance	SM	vWAAS	ISR-WAAS
WAVE-294	SM-700	vWAAS-200	ISR-WAAS-750 (ISR-4451, ISR-4431, ISR-4351, ISR-4331)
WAVE-594	SM-900	vWAAS-750	ISR-WAAS-1300 (ISR-4451, ISR-4431)
WAVE-694	SM-710	vWAAS-1300	ISR-WAAS-2500 (ISR-4451)
—	SM-910	vWAAS-2500	—
—	—	vWAAS-6000	—



Note

If you are upgrading from a version earlier than vWAAS Version 5.4, you will need a third disk and possibly more memory added. For more information, see the [Akamai Connect and vWAAS](#) section of the *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*.

Workflow: Using Akamai Connect

- Before you register Akamai Connect, confirm that your WAAS configuration has all relevant components to work with Akamai Connect, as described in [Confirming Your WAAS Configuration for Akamai Connect](#).
- Enable Akamai Connect, as described in [Enabling Akamai Connect](#).
- Register and activate Akamai Connect, as described in [Activating the Akamai Connect License](#).
- Enable Akamai Connected Cache, as described in [Enabling Akamai Connected Cache](#).
- (Optional) Enable Over the Top caching, as described in [Enabling OTT Caching](#).

6. If needed, set up HTTP proxy for connections to the Akamai Network (using the WAAS CM as proxy or configuring external HTTP proxy), as described in [Using HTTP Proxy for Connections to the Akamai Network](#).
7. If needed, de-register and re-register a WAAS device, as described in [Deregistering and Reregistering a WAAS Device](#).
8. If needed, replace an expired Akamai Connect license, as described in [Replacing an Inactive or Expired Akamai Connect License](#).
9. Set caching policies (one policy for all sites or individual policies for specific sites), as described in [Setting Caching Policies](#).
10. (Optional) Set Cisco Cloud Web Security user policy, as described in [Setting Cisco Cloud Web Security User Policy](#).
11. Configure cache prepositioning, as described in [Configuring Cache Prepositioning](#).
12. View cache prepositioning task status, as described in [Viewing Cache Prepositioning Task Status](#).
13. (Optional) Copy cache prepositioning tasks, as described in [Copying Cache Prepositioning Tasks](#).
14. View Akamai Connected Cache statistics, including response time savings, throughput summary, HTTP bandwidth savings, top sites, and cache statistics (hits), as described in [Akamai Connected Cache Charts](#) in Chapter 15, “Monitoring and Troubleshooting Your WAAS Network.”

Registering, Activating, Enabling Akamai Connect

This section describes how to register, activate and enable Akamai Connect, as well as how to de-register and re-register a WAAS device, and replace an inactive or expired Akamai Connect license.

Confirming Your WAAS Configuration for Akamai Connect

Before you begin the registration process to activate Akamai Connect, confirm that your WAAS configuration has the following:

- The WAAS CM and WAAS appliances are updated to software version 5.5.1.
- A verified NTP service that is within 30 seconds of the NTP standard server (NTP.org). For how to configure the NTP server, see [Configuring an NTP Server](#) in Chapter 10, “Configuring Other System Settings.”
- A working public DNS server configured on the WAAS devices and the WAAS CM. For how to configure the DNS server, see [Configuring the DNS Server](#) in Chapter 6, “Configuring Network Settings.”
- The ability for the WAAS CM to reach Akamai’s Luna system via HTTPS on port 443. (The custom hostname is in your activation file.)
- The ability for WAAS devices to make a connection to the Akamai Management Gateway (AMG) to get the authentication key. The WAAS device configured for Akamai Connect needs the correct network connectivity to access the AMG every day to get correct credentials and updated metadata. WAAS will make an HTTPS connection on port 443 to the AMG to get this information.

If the WAAS devices cannot go direct to the Internet, you can configure them to use the WAAS CM as a proxy. For more information, see

**Note**

The Akamai Connected Cache feature will stop functioning if WAAS loses communication with the AMG for more than 48 hours.

Enabling Akamai Connect

The Akamai Connect screen has two tabs:

- **Cache Settings**, for [Enabling Akamai Connect](#)
- **Cache Prepositioning**, for [Configuring Cache Prepositioning](#)

To enable Akamai Connect, follow these steps. For more information on Akamai Connect, see [Akamai Connect and WAAS](#).

Step 1 From the WAAS Central Manager menu, from either the Device Groups or Devices tab, choose **Configure > Caching > Akamai Connect**.

The Akamai Connect window appears, with two tabs: Cache Settings and Cache Prepositioning.

Step 2 Choose the **Cache Settings** tab.

**Note**

If you are configuring the Akamai Connect feature for a device group, the device group should have only devices that support Akamai Connect. For more information, see [Supported WAAS Platforms for Akamai Caching](#).

Step 3 Check the **Enable Akamai Connect** check box to turn on the Akamai Connect CE. When the EULA (End-User License Agreement) appears, click **Accept**.

When you create settings for the first time, either at the device or the group level, the Akamai license upload file is displayed, and you can select the license file supplied and click **Submit**. For more information on activating the Akamai Connect license, see [Activating the Akamai Connect License](#).

**Note**

Turning on the CE starts active caching in Standard mode. If you want Advanced or Bypass mode, you must specify it. This step is described in [Setting Caching Policies](#).

Step 4 Continue to **Edit Settings** and/or **Advanced Cached Settings**.

**Note**

To edit any settings, including advanced settings and cache preposition, the Akamai Connect feature must remain enabled.

Activating the Akamai Connect License

Before you begin the registration process to activate Akamai Connect, confirm the readiness of your WAAS configuration, as described in [Confirming Your WAAS Configuration for Akamai Connect](#).

To receive and activate the Akamai Connect activation file, follow these steps:

-
- Step 1** Purchase a license for Akamai Connect from your Cisco account representative or reseller.
- Step 2** The account representative or reseller enters the order into the Cisco Commerce Workspace (CCW) system. The order *must* specify an email address for eDelivery of the Activation file.
- Step 3** CCW contacts the Akamai Luna Portal to request a license or licenses for the number and type of Akamai licenses entered.
- Step 4** Akamai generates and sends the license(s) to the CCW system in the form of a single activation file.
- Step 5** The CCW system sends an email, with the activation file attached, to the email address specified in the order. The order of priority for selecting the email address in a CCW order is::
- Priority1: eDelivery email address
 - Priority2: end customer email address
 - Priority3: shipping contact email address



Note If you do not provide an email address in your order, you will not receive an activation file.

- Step 6** Enable Akamai Caching on each WAE. There are two paths available to reach the Akamai Connect screen. You can use either one to enable Akamai Connect to use any of the transparent caching methods, Akamai Connected Cache, or OTT. If this is the first time you are navigating to the Akamai Connect screen, you will be prompted to provide the activation file for licensing.
- From the WAAS CM choose **Device/Device Group > Configure > Caching > Akamai Connect**.
 - OR
 - From the WAAS CM choose **Home > Admin > Licenses > Akamai Connect**. This path can be used later to add more licenses, if needed.

The Akamai Connect screen is displayed.

- Step 7** At the **Upload Akamai Connect License file** field, click **Browse**, highlight the activation file and click **OK**.
- Step 8** Click **Upload**. The authentication data in the activation file is transmitted to the Akamai Luna portal.
- Step 9** After the device message is sent to the Luna portal:
- The Luna portal sends the Entitlement Code to the WAAS Central Manager and the Akamai Management Gateway (AMG).
 - The WAAS Central Manager sends the Entitlement Code to WAAS.
 - The AMG rolls out the Entitlement Code to Edge Servers on the Akamai Grid Network.

The Entitlement Code is maintained on Luna, on the AMG, and on the WAAS device. WAAS connects to the AMG using a proxy/DNS server that can resolve the address **amg.terra.akamai.com**.

- Step 10** The list titled **Status of devices with Akamai Connect feature configured** displays the following types of status for one, some, or all devices.
- Akamai Device Status - ActivationInProgress, Active
 - Operational Status - Disconnected, Connected, or Running
 - Connectivity to Akamai - Activating, Activated, or Connected

The device registration, operational status, and connectivity to Akamai proceed through a set of status indicators for the three status categories: Akamai Device Status/Operational Status/Connectivity to Akamai:

- **ActivationInProgress /Disconnected /Activating**
- **ActivationInProgress /Connected /Activating**
- **Active /Connected /Activated**
- **Active /Connected /Connected**



Note

The activation process for WAAS devices may take between 15-60 minutes to complete, and for this time period, the **Connectivity to Akamai** status displays as **Activating**. During this time, device(s) may not be able to communicate with the Akamai Network, because they are not recognized by the AMG's until the activation process is complete, and the **Connectivity to Akamai** status displays as **Connected**.

Step 11 For the last steps in the registration process, Luna sends the Connected Cache credentials to the AMG and to the Edge Servers on the Akamai Grid network. The AMG forwards Connected Cache credentials on to WAAS. With the Connected Cache credentials on both WAAS and the Edge Servers, the Connected Cache is enabled, and caching requests can be served by the Edge servers. This authenticated connection can then service requests for Connected Cache and OTT caching from the Akamai Grid network Edge Servers.

Step 12 The registration of each WAE begins. The WAAS CM provides information to the Akamai Luna Portal for each device that will be running Akamai Connect.



Note

Connected Operational Status can take several minutes to complete. Rollout of the activation to the Edge servers can take up to 45 minutes to complete. A device may take from a few minutes to up to two hours to show an **Active** Activation Status, depending on when the request was made, traffic conditions, and other variables.

Step 13 Each WAE that has been sent the entitlement code will try to make an SSL connection to the AMG using **amg.terra.akamai.com**. The Luna Portal will push out the Akamai Connected Cache credentials to the AMG and Akamai Grid Network (to the Akamai Edge Servers).

- The AMG will push the Akamai Connected Cache credentials out to each of the WAEs that are configured for Akamai Connected Cache. If OTT is enabled, the OTT metadata needed to help cache YouTube objects is also processed at this time.
- The Akamai Connected Cache credentials are sent by the WAE CE when going to the origin server. If the WAE CE has valid credentials according to the Akamai Edge Server, the Akamai Edge Server then provides objects to the WAE CE that are not normally cacheable to other devices.

Step 14 The WAE CE will request new credentials daily and will be good for two days. The connections are always established from WAE or WAAS CM over TCP 443 to the AMG.

- For security, firewalls are usually deployed by performing statefull inspection on traffic from within the company to the outside. They are also configured to block unknown traffic from the outside to the inside. Since connection should not initiate from AMG to any WAAS CM or WAE at any time, there should not be an issue. If there is, then a hole will need to be made to allow the WAAS CM or WAE to speak to any device on port 443.

**Note**

The Devices listing on the **All Devices** screen includes a column titled **Akamai Connect**, which shows the status of each device: Active, Not Supported, Connected, Disconnected.

- Step 15** As needed, configure HTTP proxy or external HTTP proxy, as described in [Using HTTP Proxy for Connections to the Akamai Network](#).

Deregistering and Reregistering a WAAS Device

When you deregister a WAAS device from the WAAS CM, the WAAS CM will trigger the removal of the device record on the Akamai side, thereby invalidating the entitlement key used by the CE to talk to AMG devices. On the WAAS side, the CE will continue operating in transparent cache mode.

When you reregister a WAAS device with the WAAS CM, one of two things will happen:

- The WAAS CM will auto-assign the device to device groups (that are so marked). If any of these device groups have Akamai Connect/HTTP cache settings, the WAAS CM will trigger registration with Akamai.
- If no device group is configured with Akamai Connect/HTTP cache settings, the registration is done individually.

After the device is registered, it will get a new entitlement key.

Replacing an Inactive or Expired Akamai Connect License

If your license has become inactive or expired, follow these steps to replace your license:

- Step 1** When a license is inactive or expired, a notification is displayed in one of two WAAS CM screens:
- At the **Home > Admin > Licenses > Akamai Connect** screen: “Akamai Connect License is Inactive. Please remove current license and import valid license.”
 - At the **Home > Monitor > Troubleshoot > Akamai Diagnostics** screen: “Akamai Connect License is Inactive. Please remove existing license and import new one using Akamai License page.”
- Step 2** Remove the inactive or expired license.
- Step 3** To upload a new license file, at the **Home > Admin > Licenses > Akamai Connect** screen, click Choose File to browse to the new license file and click **Upload**.
- Step 4** If you import an expired license, you will see the message: “Unable to communicate to Akamai server (Error: License is inactive or expired). See Central Manager log file for detailed error information.”
- Step 5** To obtain a new license, contact your Cisco account representative or reseller.

Enabling Akamai Connected Cache

You can configure Akamai Connected Cache CE settings at the **device group level** (to apply a configuration to all registered devices) or the **device level** (to apply a configuration to a particular registered device).

To enable Akamai Connected Cache, follow these steps. For more information on Akamai Connected Cache, see [Akamai Connected Cache](#).

-
- Step 1** To enable Akamai caching, check the **Akamai Connected Cache** check box. The default is enabled. When you enable Akamai connected cache, it is enabled for all suitable Akamaized content.
- Step 2** Click **Submit**.
- Step 3** After you enable Akamai Connected Cache, you can set a caching policy for all sites, or an individual caching policy for specific sites, as described in [Setting Caching Policies](#).
- Step 4** After you enable Akamai Connected Cache, you can configure cache prepositioning, as described in [Configuring Cache Prepositioning](#).
-

Enabling OTT Caching

To enable OTT caching, follow these steps. For more information on OTT caching, see [OTT Caching](#).

-
- Step 1** To enable Over the Top (OTT) caching, check the **Over the Top Cache** check box. In the initial release, OTT caching applies only to YouTube.
- Step 2** Click **Submit** or continue to Advanced Cache Settings. For more information on Advanced Cache Settings, see [Advanced Mode](#).
-

Using HTTP Proxy for Connections to the Akamai Network

When using Akamai Connect, the WAAS CM and WAAS device(s) must be able to communicate with the Akamai Network: with the Akamai Luna API servers to provision entries for WAAS devices, and with the Akamai AMG devices for Akamai Connected Cache and OTT features.

However, some WAAS deployments may disallow outgoing connections to the Internet for the WAAS CM or WAAS device(s). For these deployments, the WAAS device(s) may use an HTTP proxy to contact the Akamai Network.

You can set up the following proxy configurations:

- No HTTP proxy use
- [Using the WAAS CM as HTTP Proxy](#)
- [Configuring External HTTP Proxy](#)

For these three proxy configurations, WAAS supports five deployment scenarios:

Deployment Scenario	Deployment Connections	WAAS CM to Luna API Servers	WAAS HTTP CE to Akamai AMG
No HTTP proxy use	Direct/ Direct	Direct	Direct
WAAS CM as HTTP proxy	Direct/ WAAS CM as proxy	Direct	WAAS CM as HTTP proxy
External HTTP proxy	Direct/ External HTTP proxy	Direct	External HTTP proxy

Deployment Scenario	Deployment Connections	WAAS CM to Luna API Servers	WAAS HTTP CE to Akamai AMG
External HTTP proxy	External HTTP proxy/ Direct	External HTTP proxy	Direct
External HTTP proxy	External HTTP proxy/ External HTTP proxy	External HTTP proxy	External HTTP proxy

The following considerations apply to all HTTP proxy deployments:

- You configure HTTP proxy from the WAAS CM; there are no CLI commands for HTTP proxy. Configuring HTTP proxy settings does not require restart of the WAAS CM.
- HTTP Proxy must support HTTP Connect method for tunneling HTTPS connections.
- Configuring the HTTP proxy setting does not require restart of the WAAS CM.



Note

WAAS v5.5.1 does not support HTTP proxy user authentication. It is recommended that you restrict access to proxy using IP address ACLs.

Using the WAAS CM as HTTP Proxy

Note the following considerations when using the WAAS CM as a proxy to the Akamai network:

- When using Akamai Connected Cache, each WAAS CE device is communicating with the Akamai network. Some WAAS deployments may disallow WAE devices to establish outgoing connections to the Internet (i.e., private networks). In this case, the WAE device may use the WAAS CM device(s) as proxy for all connections to the Akamai network.
- You may still have to allow a hole for the WAAS CM to make communications on TCP port 443 outbound.
- There is no option for the WAAS CM to use a proxy device to get to the Internet.
- All connections are made from the WAAS CE device or WAAS CM out to the Akamai network; never from the Akamai network to the WAAS CE device or WAAS CM.
- You configure this feature from the WAAS CM only, not the CLI.

To use the WAAS CM as HTTP proxy, follow these steps:

- Step 1** From Devices or Device Groups, navigate to **Configure > Caching > Akamai Connect**.
- Step 2** Choose the **Cache Settings** tab.
- Step 3** Check the **Use HTTP proxy for connections to Akamai network** check box.
- Step 4** At the **HTTP Proxy:** dropdown list, select **Central Manager as HTTP Proxy**.
- Step 5** Click **Submit**.

Configuring External HTTP Proxy

When using the Akamai Connected Cache, WAAS devices are communicating with the Akamai Network. Some deployments may disallow outgoing connections to the Internet for WAAS devices. For these deployments, WAAS devices can use an HTTP proxy to contact the Akamai Network. For more information on HTTP proxy, see [Using HTTP Proxy for Connections to the Akamai Network](#).



Note

HTTP proxy must support HTTP CONNECT for tunneling HTTPS connections.

To configure external HTTP proxy, follow these steps:

- Step 1** From Devices or Device Groups, navigate to **Configure > Caching > Akamai Connect**.
- Step 2** Check the **Use HTTP proxy for connections to Akamai network** check box.
- Step 3** At the **HTTP Proxy:** dropdown list, select **External HTTP Proxy**.
- Step 4** Specify a Proxy Host and a Proxy Port:
 - Proxy Host field - Enter a hostname or address.
 - Proxy Port - Enter a value between 1-65,555.



Note

If the WAAS CM is already using an external HTTP proxy, there is no option displayed to use the WAAS CM as proxy; these fields will display the currently configured HTTP proxy.

- Step 5** Click **Submit**.

Setting Caching Policies

For how to set one caching policy for all sites, or set individual caching policies for a specific site., follow these steps:

- Step 1** From Devices or Device Groups, navigate to **Configure > Caching > Akamai Connect**.
- Step 2** Choose the **Cache Settings** tab.
- Step 3** In the **Advanced Cache Settings** section, at the **Default Transparent Caching Policy** drop-down list, choose a caching policy:
 - Basic
 - Standard (default)
 - Advanced
 - Bypass
- Step 4** *To set a default caching policy for all sites*, choose a caching policy and click **Submit**. To enable transparent caching for a specific site, see Step 5.
- Step 5** *To enable transparent caching for a specific site*, change the **Default Transparent Caching Policy** to **Bypass**.

- Step 6** At the **Site Specific Transparent Caching Policy** section, click **Add Hostname/IP**. The **Site Caching Policy Task** dialog box opens.
- In the **Hostname/IP** field, specify the hostname of the site to be configured. The hostname can be a specific server, or a domain name that contains a wildcard, such as *.cisco.com.
 - At the **Transparent Caching Policy** drop-down list, select the cache policy for this site: Basic, Standard, Advanced, or Bypass.
 - Click **OK**. The new hostname/IP is added as a line item to the Site Specific Transparent Caching Policy table.



Note The policy you set for a specific site takes precedence over the default caching policy set for all sites.

You can configure up to 512 hostnames for each site-specific transparent caching policy.

- Step 7** Configure Cisco Cloud Web Security (CWS) user policy. For more information see [Setting Cisco Cloud Web Security User Policy](#).
- Step 8** Configure HTTP Proxy:
- To configure WAAS CM as HTTP proxy, see [Using the WAAS CM as HTTP Proxy](#)
 - To configure external HTTP proxy, see [Configuring External HTTP Proxy](#).

Setting Cisco Cloud Web Security User Policy

The Cisco Cloud Web Security feature provides content scanning of HTTP and secure HTTP/S traffic and malware protection service to web traffic. CWS servers scan web traffic content and either allow or block the traffic based on configured policies. Servers use credentials such as private IP addresses, user names, and user groups to identify and authenticate users and redirect the traffic for content scanning.

Traffic is transparently proxied by an ASA or ISR to cloud-based CWS servers (called towers), where the web traffic is scanned and if deemed acceptable is provided to the origin server. All traffic coming back is through the CWS tower.

Note the following considerations when using the Cisco CWS option:

- CWS can be used only when one WAAS device is present in the path.
- When you enable CWS, the Akamai CE always adds an “if modified since” header to the request so that the response needs to go remote to the origin server (in this case, the Scansafe tower) - so all requests get scanned and no security is bypassed. If a 304 Not Modified is returned, then the Akamai CE provides the object from the cache. If a 200 Okay is returned, then the object is fetched from the origin server.
- CWS does not work with Akamai Connected Cache, because the Akamai Connected Cache credentials passed by the WAE CE to the Akamai Edge Server associates an IP address to the credentials. The CWS tower would change the source IP address from the client to its own when going out to the origin server, negating any benefit from Connected Cache.
- CWS is only designed for single-sided flows.
- If preposition is enabled and is possible that the flow may be redirected to a CWS tower, follow these recommendations:

- (Preferred choice) configure a white-list on the ISR or CWS tower to bypass the WAE IP address.
- On the CWS tower, configure a user or group that the WAE will fall into for authentication and allow it access to all sites on which the preposition is occurring.

To enforce the Cisco CWS user policy, follow these steps:

-
- Step 1** Navigate to **Configure > Caching > Akamai Connect > Cache Settings** tab.
- Step 2** At the Advanced Settings section, check the **Cisco Cloud Web Security present** check box.
- Step 3** Click **Submit**.
-

Configuring Cache Prepositioning

Cache prepositioning, also known as cache warming, allows you to specify a policy to prefetch and cache content at a specified time. For example, prepositioning content with a URL inside the branch office during non-peak hours can help to improve performance during peak hours, by significantly offloading WAN links.

Cache prepositioning runs at the same priority as other caching types, for example, Akamai Connected Cache or OTT.



Note

In order for HTTPS content to be prepositioned, you must define an SSL accelerated service; otherwise, any HTTPS requests encountered in the job will fail, although the preposition task will continue and any objects available via HTTP will be retrieved. For more information on defining an SSL accelerated service, see [Configuring SSL Acceleration](#).

When a scheduled fetch operation begins or is complete, it is added to the Cache Preposition Status table.


Here is a workflow of how to configure cache prepositioning at the **Cache Prepositioning** tab (**Configure > Caching > Akamai Connect**):

- Enable DRE for preposition connections (optional).
- Create a new cache preposition task: specify task name, base URLs for prepositioning, include/exclude types, download rate, and recursion depth.
- Specify the task's recursion delay time and recursion hostnames.
- Create a schedule for the cache preposition task: specify schedule name, frequency (yearly, monthly, weekly, daily), and start time.
- View cache preposition task status information, including start/end time, byte/object count, refresh bytes/count, store bytes/count, and uncacheable bytes/count.

To configure a cache preposition task, follow these steps:

-
- Step 1** From Devices or Device Groups, navigate to **Configure > Caching > Akamai Connect**. The Akamai Connect window appears with two tabs: Cache Settings and Cache Prepositioning.
- Step 2** Choose the **Cache Prepositioning** tab. At this tab, you can add, edit, or delete cache prepositioning tasks, as well as monitor cache preposition task status.

- Step 3** (Optional) Check the **Preposition with DRE** check box to enable DRE for preposition connections. The default is disabled, to prevent negative impact to the DRE byte cache for data that will be stored at the object level.
- Step 4** Click **Add Cache Preposition Task**.
The Cache Prepositioning Task dialog box opens.
- Step 5** Specify the following:

Field	Description
Name	<p>The name of the preposition task. Preposition task name is an alphanumeric identifier up to 47 characters. Special characters like ‘,/ \, {, }, (,), ?, ”, <, >, [,], &, *,’ are not allowed.</p> <p>Note the following when specifying a task:</p> <ul style="list-style-type: none"> You can configure up to 10 URLs per task. You can configure up to 10 schedules per task. You can configure up to 50 tasks per device or device group.
URLs	<p>The base URLs for prepositioning. The maximum length for the URL is 900 characters. Characters that are not allowed in the URL are space, double quotes (“). ASCII characters are allowed in the range of ASCII 33 through ASCII 125.</p> <ul style="list-style-type: none"> Use a space to separate multiple URLs. You can configure up to 10 URLs per task.
Include Types	The object types to include in caching, such as .jsp or .asp, each separated by a comma. The list of object name patterns to be included has a total pattern field limit of 47 characters.
Exclude Types	The object types to exclude from caching, such as .jsp or .asp, each separated by a comma. The list of object name patterns to be excluded has a total pattern field limit of 47 characters.
Download Rate	The maximum download rate, in KBps. Select any value between 0 to 10,000,000 KBps. The default is 20 KBps. A selection of 0 indicates unlimited, or no enforced rate limiting.
Recursion Depth	<p>The depth of the link level at which the content is retrieved. Recursion depth is active only if you check the Recursive Task check box. Select 1, 2, 3, 5, 8, 13, or 21 from the drop-down list, or enter any custom value between 1 to 1000. The default is 1.</p> <div>  <p>Note A greater number of specified levels of links means a greater amount of data stored in the cache, sometimes exponentially more. If the amount of requested prefetched data becomes larger than the cache, the newly requested data will flush all previously stored data, and may slow down other operations that attempt to use the cache.</p> </div>

Field	Description
Duration	<p>The maximum amount of time, in minutes, a preposition task can run before it is halted. The default is no set duration. To set a duration time, select from a range of 1 to 2,147,483,647 minutes.</p> <p>Setting the duration of a task is especially useful to:</p> <ul style="list-style-type: none"> • Ensure that preposition tasks do not overlap with each other. • Ensure that preposition tasks do not overlap with times of higher user traffic.
Enable Task	<p>Check the Enable Task check box to enable the specified preposition task to run. For the task to run, you must specify at least one URL and one schedule (described in Step 5).</p>

Step 6 At the **Advanced Settings** section of the **Cache Prepositioning Task** dialog box, you can specify recursion delay time and recursion hostnames:

Field	Description
Recursion Delay Time	<p>The delay time, in seconds, between requests during recursive download. This simulates user wait time. Recursive delay time is necessary because some servers use the lack of time between requests to detect and restrict web spiders.</p> <ul style="list-style-type: none"> • Enter a value between 0 to 600 seconds. The default is 2 seconds. • A value of zero provides the best performance when there are no web spider restrictions.
Recursion Domains	<p>The list of server domain suffixes for which recursive spidering is permitted. If the list is empty, then spidering is only permitted within the same domain as the specified URL.</p> <p>You can configure up to ten servers:</p> <ul style="list-style-type: none"> • The server name is up to 255 characters. • Server names are separated by comma or space.

Step 7 In the **Cache Prepositioning Schedule** section, click **Add Schedule**.

The Cache Prepositioning Schedule dialog box opens

Step 8 Specify the following:

Field	Description
Schedule Name	<p>The name of the schedule for this preposition task. Schedule name is an alphanumeric identifier up to 256 characters. The Schedule Name allows you to provide your own representation of a schedule. For example, for a schedule that occurs each Monday, Wednesday, and Friday at 10:30 a.m. can be named as Weekly MWF 10:30AM or Every Week - MON-WED-FRI at 10:30AM.</p>
Frequency	<p>The specified time for prepositioning: yearly, daily, weekly, or monthly days. If you choose monthly days, a calendar with check boxes opens for you to check one, some, or all the days in a month for this schedule.</p>
Start Time (HH:MM)	<p>From the two drop-down lists, choose the hour and minute at which the task schedule should start.</p>

Step 9 In the Cache Prepositioning Schedule dialog box, click **OK**.

Step 10 In the Cache Prepositioning Task dialog box, click **OK**.

Step 11 Click **Submit**.

The new cache prepositioning task is added as a line item to the Cache Prepositioning listing table.

Viewing Cache Prepositioning Task Status

Two tables are provided in the Cache Prepositioning section to show the status of a cache prepositioning task. To view the status of a cache preposition task you have configured, select the task from the first table, the Cache Preposition Listing table. The second table, the Cache Prepositioning Status table, displays information on the selected task.

- For an individual device, the cache prepositioning status table shows the selected task status for the current device.
- For a device group, the cache prepositioning status table shows the status of the selected cache preposition task, for all devices under that device group.

The following types of information are displayed for the selected task:

Field	Description
Device Name	The name of the selected device.
Start Time	The date, hour, and minute for the task schedule to start.
End Time	The date, hour, and minute for the task schedule to end.
Byte Count	The total number of bytes in cache during the most recent preposition task run.
Object Count	The total count of objects in cache during the most recent preposition task run.
Refresh Bytes	The number of bytes refreshed in cache during the most recent preposition task run.
Refresh Count	The count of objects refreshed in cache during the most recent preposition task run.
Store Bytes	The number of unmodified bytes for objects found in cache during the most recent task run.
Store Count	The count of unmodified objects found in cache during the most recent task run.
Uncacheable Bytes	The number of bytes of uncacheable objects encountered during the most recent task run.
Uncacheable Count	The count of uncacheable objects encountered during the most recent task run.
Status	The status of the task, such as Scheduled, Complete, or Error.
Error	If the task status is "Error," an error message describing the task status is displayed.

Copying Cache Prepositioning Tasks

You can copy cache prepositioning tasks that have a device or device group enabled with Akamai Connect, with WAAS running v5.5.1 or 5.4.1. Use the following methods to copy cache prepositioning tasks:

- Device to device
- Device to device group

- Device group to device
- Device group to device group

**Note**

Cache Preposition Tasks and WAAS versions: You can also use the **Copy Tasks** feature to copy a cache preposition task between WAAS Version 5.5.1 devices and device groups and WAAS versions earlier than Version 5.5.1 devices and device groups.

To copy a cache preposition task, follow these steps:

Step 1 Navigate to **Configure > Caching > Akamai Connect > Cache Prepositioning** tab > **Cache Prepositioning** section.

Step 2 Click the **Copy Tasks** button.

The **Cache Prepositioning Task** dialog box opens.

Step 3 At the **From** drop-down list, select a device or device group as the source.

Step 4 At the next drop-down list, select a device or device group as the destination.

**Note**

If you try to copy a task with the same name between device and device groups, the following error message is displayed: **One or more preposition tasks with the same name already exists in the destination device/DG.**

Step 5 At the **Existing Cache Prepositioning Tasks** table, select one, some or all of the preposition tasks to be copied.

Step 6 Click **OK**.

The selected cache prepositioning tasks are copied from the source to the destination.

Cisco Support for Microsoft Windows Update

Cisco support for Microsoft Windows Update enables caching of objects used in Windows OS and application updates. Cisco support for Microsoft Windows Update is enabled by default, and enabled only for specific sites.

This section contains the following topics:

- [Benefits of Cisco Support for Microsoft Windows Update](#)
- [Viewing Statistics for Cisco Support for Microsoft Windows Update](#)
- [Cisco Support for Microsoft Windows Update and Akamai Cache Engine](#)

Benefits of Cisco Support for Microsoft Windows Update

The Microsoft OS and application updates are managed by update clients such as Microsoft Update. Microsoft Update downloads the updates via HTTP, often in combination with BITS (Background Intelligent Transfer Service) to help facilitate the downloads. Clients use HTTP range request to fetch updates.

The objects that comprise the updates, such as .cab files, are typically cacheable, so that HTTP object cache is a significant benefit for this process.

For example, for Windows 7 and 8 OS updates—via direct Internet or WSUS (Windows Server Update Services), versions 2012 and 2012R2—more than 98% of the update files, such as .cab, .exe, and .psf files, are served from cache on subsequent updates. Cisco support for Microsoft Windows Update reduces the volume of WAN offload bytes and reduces response time for subsequent Windows updates.

Viewing Statistics for Cisco Support for Microsoft Windows Update

There are two ways to view data generated by Cisco support for Microsoft Windows Update:

- The [Top Sites](#) report, described in Chapter 15, “Monitoring and Troubleshooting Your WAAS Network” provides information including WAN response time and WAN offload bytes.
- For WAAS Version 6.1.1, the cache engine access log file has two new fields for Microsoft Windows Update statistics:
 - rm-w (range miss, wait)—The main transaction, a cache miss, which waited for the sub-transaction to fetch the needed bytes.
 - rm-f (range miss, full)—The sub-transaction, a cache write of the entire document.

Example 1:

Example 1 contains two log lines, the main transaction and sub-transaction, when a range is requested on an object that is not in cache:

```
ws8-rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
08/28/2015 12:22:29.663 (f1=27520) 300 13.164 0.000 446 - - 34912 172.25.30.4

191.234.4.50 2905 h - - rm-w 206 GET
http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/secu/2013/07/wind
ows8-rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -

08/28/2015 12:24:31.448 (f1=27520) 300 134.949 0.000 355 344 3591542 568 172.25.30.4
191.234.4.50 2f25 m-s - - rm-f 200 GET
http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/secu/2013/07/wind
ows8-rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
```

Example 2:

Example 2 shows a cache hit when a range is requested on an object that is either completely in cache, or in the process of being downloaded. If it is in the process of being downloaded, then the main transaction has latched onto a sub-transaction like the one shown in Example 1.

```
08/28/2015 03:34:36.906 (f1=26032) 300 0.000 50.373 346 - - 13169 172.25.30.4
8.254.217.62 2905 h - - - 206 GET
http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/secu/2013/07/wind
ows8-rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
```

Cisco Support for Microsoft Windows Update and Akamai Cache Engine

Cisco support for Microsoft Windows Update enables Akamai Cache Engine to support Windows Update caching in two ways:

- Download and cache full objects even when ranges within objects that not in cache are requested.
- Future range requests on the objects can be served out of cache.

There is a limit, set by OTT metadata during the Akamai Connect registration process, from the start of the object—the number of bytes or the percent of file length—where the download functionality is triggered. A request of a size above the set limit does not initiate a full object download, and the request is forwarded to the origin as is.



Caution

Cisco Support for Microsoft Windows update is enabled by default, and enabled only for specific sites. The enabled sites are updated via OTT metadata.

If you want to disable Cisco Support for Microsoft Windows Update, you must disable OTT caching. To do this, uncheck the **Over the Top Cache** check box. However, note that unchecking the **Over the Top Cache** check box disables *all* OTT functionality, both global and custom OTT configurations.

For more information on the Akamai Connect registration process, see [Activating the Akamai Connect License](#).

Creating a New Traffic Optimization Policy

[Table 12-7](#) provides an overview of the steps that you must complete to create a new traffic optimization policy.

Table 12-7 Checklist for Creating a New Optimization Policy

Task	Additional Information and Instructions
1. Prepare for creating an optimization policy.	Provides the tasks you need to complete before creating a new optimization policy on your WAAS devices. For more information, see Preparing to Create an Optimization Policy .
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. For more information, see Creating an Application Definition .
3. Create an optimization 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: <ul style="list-style-type: none"> • Create application class maps 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 Creating an Optimization Policy .

Preparing to Create an Optimization Policy

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

- Review the list of optimization 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 Optimization Policy.”](#)

- 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 optimization policy. We recommend that you create optimization policies on device groups so that the policy is consistent across multiple WAAS devices.

Creating an Application Definition

The first step in creating an optimization 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. 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 menu, choose **Configure > Acceleration > Applications**.
The Applications window appears, which displays a list of all the applications on your WAAS system. It also lists the device or device group from which it gets the settings.
- Step 2** From this window, perform the following tasks:
- Select an application and click the **Edit** icon in the task bar to modify the definition, or click the **Delete** icon in the task bar to delete.
 - Determine if your WAAS system is collecting statistics on an application. The Enable Statistics column displays Yes if statistics are being collected for the application.
 - Create a new application, as described in the steps that follow.
- Step 3** Click the **Add Application** icon in the taskbar.
The Application window appears.
- Step 4** Enter a name for this application.
The name cannot contain spaces and special characters.
- Step 5** (Optional) Enter a comment in the **Comments** field.
The comment you enter appears in the Applications window.
- Step 6** 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 check box.



Note If you are collecting statistics for an application, and decide to disable statistics collection, and then reenable statistics collection at a later time, the historical data is retained, but a gap in data will exist for the period when statistics collection was disabled. An application cannot be deleted if there is an optimization policy using it. However, if you delete an application that you had collected statistics for, and then later recreate the application, the historical data for the application is lost. Only data collected since the re-creation of the application is displayed.



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

Step 7 Click **OK**.

The application definition is saved and is displayed in the application list.

Creating an Optimization Policy

After you create an application definition, create an optimization policy that determines the action a WAAS device takes on the specified traffic. For example, you can create an optimization 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 optimization policies on your WAAS system.

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

To create an optimization policy, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).

Step 2 Choose **Configure** > **Acceleration** > **Optimization Policies**.

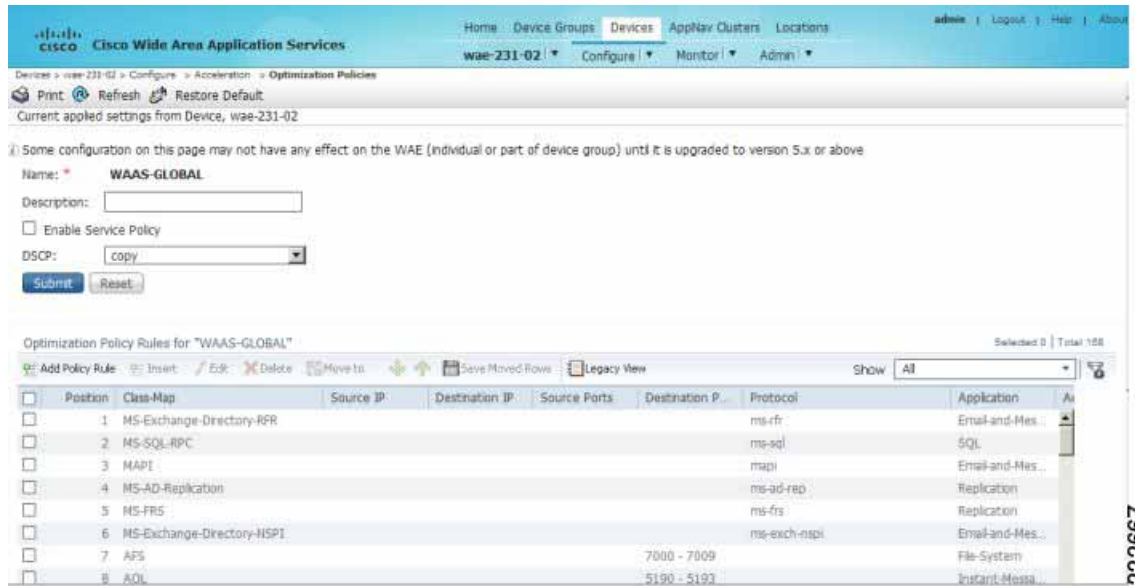
The Optimization Policies window appears ([Figure 12-33](#)).



Note In a WAAS Express device, the Optimization Policies window shows a subset of the fields in the standard Optimization Policies window.

Enable Service Policy option, DSCP option, and the Protocol column in the list of policy rules are not applicable to WAAS Express.

Figure 12-33 Optimization Policies Window



This window displays information about all the optimization policies that reside on the selected device or device group and the position of each policy. 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 [Modifying the Position of an Optimization Policy](#). This window also displays the class map, source and destination IP addresses, source and destination ports, protocol, application, action, and accelerates assigned to each policy.



Note If there are WAAS Version 4.x devices, you can click the **Legacy View** taskbar icon to view the policies as they appear in a WAAS Version 4.x device.

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

- Configure a description, configure the Enable Service Policy setting, and configure the DSCP setting. This DSCP setting field configures DSCP settings at the device (or device group) level.



Note The device will only use this policy setting to determine what optimizations are performed if Enable Service Policy is set.

- Select one or more optimization policies that you want to delete, and click the **Delete** icon to delete the selected policies.
- Select an optimization policy and click the **Edit** icon to modify the checked policy.
- Restore predefined policies and class maps. For more information, see [Restoring Optimization Policies and Class Maps](#).
- Create an optimization policy, as described in the steps that follow.

Step 3 Click the **Add Policy Rule** icon in the taskbar to create a new optimization policy.

The Optimization Policy Rule pop-up window appears ([Figure 12-34](#)).

Figure 12-34 Add Optimization Policy Rule Window

- Step 4** From the Class-Map Name drop-down list, select an existing class map for this policy, or click **Create New** to create a new class map for this policy. For information on creating a new class map, see [Creating an Optimization Class Map](#).
- Step 5** From the Action drop-down list, choose the action that your WAAS device should take on the defined traffic. [Table 12-8](#) describes each action.



Note For a WAAS Express device, only a subset of actions are available: Passthrough, TFO Only, TFO with LZ, TFO with DRE, and TFO with DRE and LZ.

Table 12-8 Action Descriptions

Action ¹	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 feature, see Transport Flow Optimization in Chapter 1, “Introduction to WAAS.”
TFO with DRE (Adaptive Cache)	Applies both TFO and DRE with adaptive caching to matching traffic.
TFO with DRE (Unidirectional Cache)	Applies both TFO and DRE with unidirectional caching to matching traffic.
TFO with DRE (Bidirectional Cache)	Applies both TFO and DRE with bidirectional caching to matching traffic.
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 (Adaptive Cache) and LZ	Applies TFO, DRE with adaptive caching, and LZ compression to matching traffic.

Table 12-8 *Action Descriptions (continued)*

Action ¹	Description
TFO with DRE (Unidirectional Cache) and LZ	Applies TFO, DRE with unidirectional caching, and LZ compression to matching traffic.
TFO with DRE (Bidirectional Cache) and LZ	Applies TFO, DRE with bidirectional caching, and LZ compression to matching traffic.

1. When configuring a device running a WAAS version prior to 4.4.1, options that include Unidirectional or Adaptive caching are not shown in the Action list.

**Note**

When ICA acceleration is enabled, all the connections are processed with the DRE mode as unidirectional, and acceleration type is shown as TIDL (TCP optimization, ICA acceleration, DRE, and LZ).

**Note**

When configuring optimization policies on a device group, if the device group contains devices running a WAAS version prior to 4.4.1 and you are configuring an action that includes Unidirectional or Adaptive caching, the caching mode is converted to bidirectional. Similarly, when devices running a WAAS version prior to 4.4.1 join a device group that is configured with optimization policies that use Unidirectional or Adaptive caching, the caching mode is converted to bidirectional. In such cases, we recommend that you upgrade all the devices to the same software version or create different device groups for devices with incompatible versions.

Step 6 From the Accelerate drop-down list, choose one of the following additional acceleration actions that your WAAS device should take on the defined traffic:

- **None**—No additional acceleration is done.
- **MS PortMapper**—Accelerate using the Microsoft Endpoint Port Mapper (EPM).
- **SMB Adaptor**—Accelerate using the SMB Accelerators.
- **HTTP Adaptor**—Accelerate using the HTTP Accelerator.
- **MAPI Adaptor**—Accelerate using the MAPI Accelerator.
- **ICA Adaptor**—Accelerate using the ICA Accelerator.

**Note**

For a WAAS Express device, HTTP Express is available as an accelerator.

Step 7 Specify the application that you want to associate with this policy by performing either of the following:

- From the Application drop-down list, choose an existing application such as the one that you created, as described in [Creating an Application Definition](#). This list displays all the predefined and new applications on your WAAS system.
- Click **New Application** to create an application. You can specify the application name and enable statistics collection. After specifying the application details, click **OK** to save the new application and return to the Optimization Policy window. The new application is automatically assigned to this device or device group.

- Step 8** (Optional) Choose a value from the DSCP Marking drop-down list. 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.



Note In a WAAS Express device, the DSCP Marking drop-down list is not shown.

For the DSCP marking value, you can choose to use the global default values (see [Defining Default DSCP Marking Values](#)) or select one of the other defined values. You can choose copy, which copies the DSCP value from the incoming packet and uses it for the outgoing packet.

- Step 9** Click **OK**.

The new policy appears in the Optimization Policies window ([Figure 12-33](#)).

Creating an Optimization Class Map

You can create an optimization class map in two ways:

- In the device context, choose **Configure > Acceleration > Optimization Class-Map**, and then click the **Add Class-Map** taskbar icon.
- While adding or editing a policy rule, as described in [Creating an Optimization Policy](#), click **Create New** next to the Class-Map Name drop-down list.

The Optimization Class-Map pane is displayed for both of these methods.

To define an optimization class map for an optimization policy, follow these steps:

- Step 1** Enter a name for this application class map. The name cannot contain spaces or special characters.



Note You must create a unique class map name across all types. For example, you cannot use the same name for an optimization class map and an AppNav class map.



Note In WAAS Express, the class map name cannot contain the following prefixes (case sensitive): class, optimize, passthrough, application, accelerate, tfo, dre, lz, or sequence-interval. Existing class map names containing any of these prefixes must be changed manually.

- Step 2** (Optional) Enter a description.

- Step 3** From the Type drop-down list, choose the class map type. Choose **Application Affinity** unless you want to match all the TCP traffic, in which case you should choose **Any TCP Traffic**.

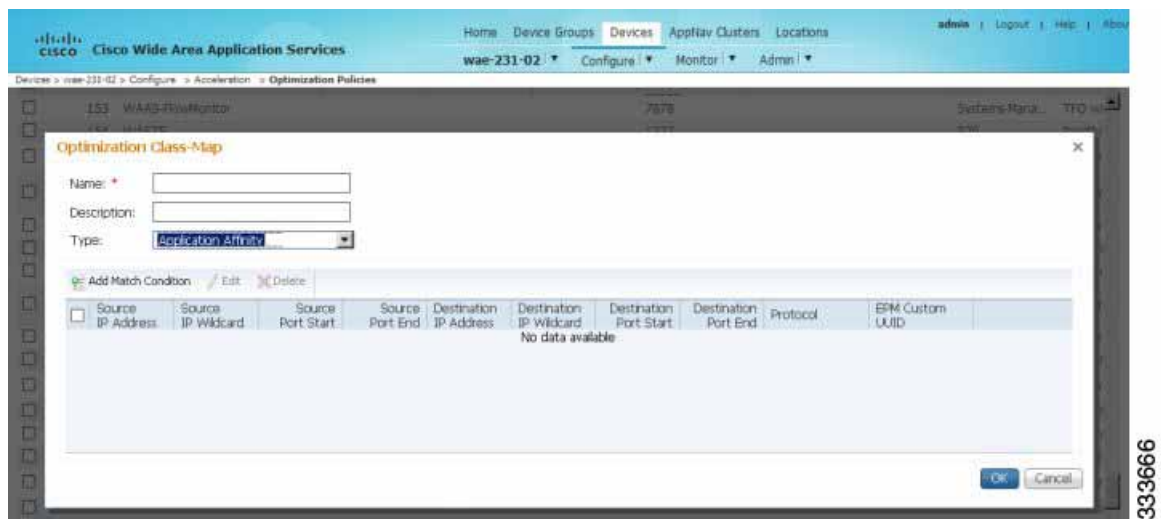
Once you have chosen the type, you can enter the match conditions.

- Step 4** Click the **Add Match Condition** icon to enter the conditions (Figure 12-35).



Note For a WAAS Express device, Protocol and EPM Custom UUID settings are not applicable.

Figure 12-35 Adding a New Match Condition Window



- Step 5** 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 the 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 in dotted decimal notation, such as 0.0.0.255 for /24.

To match traffic that uses dynamic port allocation, choose the corresponding application identifier from the Protocol drop-down list. For example, to match Microsoft Exchange Server traffic that uses the MAPI protocol, choose **mapi**. To enter a custom EPM UUID, choose **epm-uuid** and enter the UUID in the EPM Custom UUID field.



Note If you try to create a class map with an EMP UUID match condition that is already being used, that class map is removed and an error message is displayed stating that a class map already exists with the same EPM UUID match condition.

- Step 6** Add additional match conditions, as needed. If any one of the conditions is matched, the class is considered as matched.
- Step 7** Click **OK** to save the class map.

Managing Application Acceleration

This section contains the following topics:

- [Modifying the Accelerator Load Indicator and CPU Load-Monitoring Threshold](#)
- [Viewing a List of Applications](#)
- [Viewing a Policy Report](#)
- [Viewing a Class Map Report](#)
- [Restoring Optimization Policies and Class Maps](#)
- [Monitoring Applications and Class Maps](#)
- [Defining Default DSCP Marking Values](#)
- [Modifying the Position of an Optimization Policy](#)
- [Modifying the Acceleration TCP Settings](#)

Modifying the Accelerator Load Indicator and CPU Load-Monitoring Threshold

High CPU utilization can adversely affect current optimized connections. To avoid CPU overload, you can enable CPU load monitoring and set the load monitoring threshold. When the average CPU utilization on the device exceeds the set threshold for 2 minutes, the device stops accepting new connections and passes new connections, if any, through. When the average CPU utilization falls below the threshold for 2 minutes, the device resumes accepting optimized connections.

This section contains the procedures for modifying the accelerator load threshold and CPU load monitoring.



Note

When a CPU overload condition occurs, the polling interval is reduced to an interval of 2 seconds. Although the average CPU utilization may fall below the threshold during this time and the overload condition cleared, the CPU alarm may still be present. The CPU alarm is only cleared when the overload condition does not reappear in the next 2-minute-interval poll.

To modify the accelerator load indicator threshold and cpu load monitoring for a WAE device, follow these steps:

- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** Choose **Configure** > **Acceleration** > **Accelerator Threshold**.
The Accelerator Threshold window appears.
- Step 3** To enable CPU Load Monitoring, check the **Enable** check box. (The default is enabled.)
- Step 4** In the **Accelerator Load Indicator Threshold** field, enter a percent value between 80 and 100. The default is 95.
- Step 5** In the **CPU Load Higher Monitoring Threshold** field, enter a percent value between 1 and 100. The default is 98.
- Step 6** In the **CPU Load Lower Monitoring Threshold** field, enter a percent value between 1 and 100. The default is 90.
- Step 7** In the **Window Size** field enter a value between 1 to 16. The default value is 4.

- Step 8** In the **Sampling Intervals Avg Time** field enter a value between 1 and 120. The default is 10.
- Step 9** In the **Overloaded State Time** field, enter a value between 1 to 120. The default value is 10.
- Step 10** Click **Submit**.
If the device group has the 6.x software image, you can configure additional settings to monitor the cpu load for the device group.
- Step 11** To enable CPU Load Monitoring, check the **Enable** check box. (The default is enabled.)
- Step 12** To enable softirq monitoring, check the **Enable softirq Monitoring** checkbox.
- Step 13** In the **Accelerator Load Indicator Threshold** field, enter a percent value between 80 and 100. The default is 95.
- Step 14** In the **CPU Load Monitoring Threshold** field, enter a percent value between 80 and 100. The default is 95.
- Step 15** In the **CPU Load Higher Monitoring Threshold** field, enter a percent value between 1 and 100. The default is 98.
- Step 16** In the **CPU Load Lower Monitoring Threshold** field, enter a percent value between 1 and 100. The default is 90.
- Step 17** In the **Window Size** field enter a value between 1 to 16. The default value is 4.
- Step 18** In the **Sampling Intervals Avg Time** field enter a value between 1 and 120. The default is 10.
- Step 19** In the **Overloaded State Time** field, enter a value between 1 to 120. The default value is 10.
- Step 20** Click **Submit**.
-

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 menu, choose **Devices > device-name** (or **Device Groups > device-group-name**).
- Step 2** Choose **Configure > Acceleration > Optimization Policies**.
The Optimization Policies window appears.
- Step 3** Click the Application column header to sort the column by application name so that you can locate a specific application more easily.



Note If there are WAAS Version 4.x devices, click the **Legacy View** taskbar icon to view the policies as they appear in a WAAS Version 4.x device.

To edit an optimization policy, check the box next to the application and click the **Edit** taskbar icon.

If you determine that one or more policies are not needed, check the check box next to each of these applications and click the **Delete** taskbar icon.

If you determine that a new policy is needed, click the **Add Policy Rule** taskbar icon (see [Creating an Optimization Policy](#)).

Viewing a Policy Report

To view a report of a policy residing on each WAE device or device group, follow these steps:

- Step 1** From the WAAS Central Manager menu, choose **Configure > Acceleration > Optimization Policy Report** (Figure 12-36).

The Policy Report for Devices tab appears. This report lists each device (or device group) and the overall policy count on the device (or device group) referencing this application. It includes both active policies (those in use by the device or device group), and backup policies (those not in use by the device when the device gets its configuration from a device group). When the device is deassigned from the device group, the backup policies are applied back to the device and become active again.

An application cannot be deleted unless the No. of Policies field is 0.

Figure 12-36 Optimization Policy Report

Name	Type	Active Settings From
WAE-231-03	AppNav Controller	AWAASGroup (DeviceGroup)
wae-231-02	Application Accelerator	wae-231-02 (Device)

- Step 2** Click the **Policy Report for Device-Groups** tab to view the number of devices per device group and the number of active policies in the device group.
- Step 3** To see the optimization policies that are defined on a particular device or group, click the corresponding device or device group. The policies are displayed in the Optimization Policies window.

For information about viewing a class map report, see [Viewing a Class Map Report](#).

Viewing a Class Map Report

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

- Step 1** From the WAAS Central Manager menu, choose **Configure > Acceleration > Optimization Policy Report**.
- The Policy Report for Devices tab appears.
- Step 2** Click the **Class-Map Report** tab to view a report of the devices and device groups on which the class map is configured.
- Step 3** Select the class map and click the **View** icon to see the devices or device groups on which the class maps reside.

Restoring Optimization Policies and Class Maps

The WAAS system allows you to restore the predefined policies and class maps that shipped with the WAAS system. For a list of the predefined policies, see [Appendix A, “Predefined Optimization Policy.”](#)

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 class maps, follow these steps:

-
- | | |
|--------|--|
| Step 1 | From the WAAS Central Manager menu, choose Devices > <i>device-name</i> (or Device Groups > <i>device-group-name</i>). |
| Step 2 | Choose Configure > Acceleration > Optimization Policies .
The Optimization Policies window appears. |
| Step 3 | Click the Restore Default taskbar icon to restore over 150 policies and class maps 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 and Class Maps

After you create an optimization 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](#).

To monitor a class map, from the WAAS Central Manager menu, choose **Configure** > **Acceleration** > **Monitor Classmaps**. Select the class map on which to enable statistics and click the **Enable** button.

The WAAS Central Manager GUI can display statistics for up to 25 applications and 25 class maps. An error message is displayed if you try to enable more than 25 statistics for either. However, you can use the WAAS CLI to view statistics for all the applications that have policies on a specific WAAS device. For more information, refer to the [Cisco Wide Area Application Services Command Reference](#).

You can use the TCP Summary report to monitor a specific application. For more information, see the [Transmission Control Protocol \(TCP\) Summary Report](#) in Chapter 15, “Monitoring and Troubleshooting Your WAAS Network.”

Most charts can be configured to display Class Map data by clicking the **chart Edit** icon and choosing the **Classifier** series.

Defining Default DSCP Marking Values

According to policies that you define in an application definition and an optimization 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 for each device (or device group) in the Optimization Policies page for that device (or device group). This value applies to the traffic if a lower level value is not defined.
- **Policy**—You can define the DSCP value in an optimization policy. This value applies only to traffic that matches the class maps defined in the policy and overrides the application or global DSCP value.

This section contains the following topic:

- [Defining the Default DSCP Marking Value](#)

Defining the Default DSCP Marking Value

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

-
- | | |
|---------------|---|
| Step 1 | From the WAAS Central Manager menu, choose Devices > <i>device-name</i> (or Device Groups > <i>device-group-name</i>). |
| Step 2 | Choose Configure > Acceleration > Optimization Policies .
The Optimization Policies window appears. |
| Step 3 | Choose a value from the DSCP drop-down list. The default setting is copy, which copies the DSCP value from the incoming packet and uses it for the outgoing packet. |
| Step 4 | Click OK to save the settings. |
-

Modifying the Position of an Optimization Policy

Each optimization 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.

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 optimization 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 15, “Monitoring and Troubleshooting Your WAAS Network.”](#)

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

-
- | | |
|---------------|---|
| Step 1 | From the WAAS Central Manager menu, choose Devices > <i>device-name</i> (or Device Groups > <i>device-group-name</i>). |
|---------------|---|

Step 2 Choose **Configure > Acceleration > Optimization Policies**.

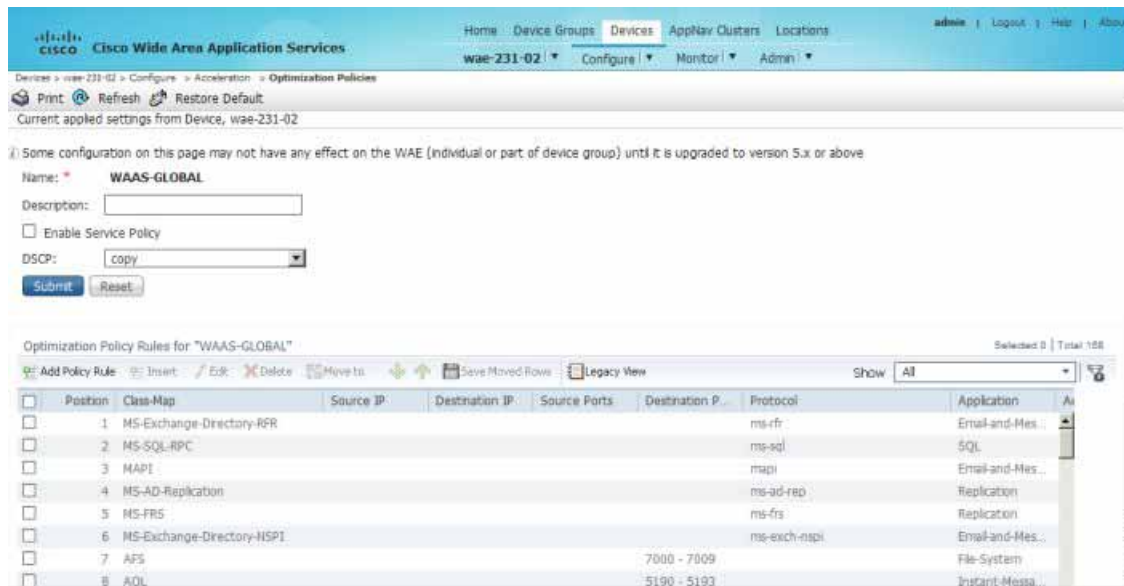
The Optimization Policies window appears (Figure 12-37).



Note For a WAAS Express device, all policies are grouped under the waas_global category.

For a list of predefined policies, see [Appendix A, “Predefined Optimization Policy.”](#)

Figure 12-37 Optimization Policies Window

**Step 3** Modify the position of the optimization policy in any of the following ways:

- Select the policy you want to move and use the up and down arrow () icons in the taskbar to move that policy higher or lower in the list.
- Select the policy you want to move and click **Move To** to specify the exact position.
- Select the policy and drag and drop it into the desired position



Note The **Save Moved Rows** icon must be clicked to save the new policy positions.

You can also create a new optimization policy at a particular position by selecting the policy above the location and then clicking **Insert**.

If a device goes through all the policies in the list without making a match, the WAAS device passes through the traffic unoptimized.



Note For a WAAS Express device, the class default policy should be last. This policy cannot be modified or deleted.

Step 4 Click the **Save Moved Rows** icon to save changes, if any, that you made to policy positions.

- Step 5** If you determine that a policy is not needed, follow these steps to delete the policy:
- Select the policy you want to delete.
 - Click the **Delete** icon in the taskbar.



Note A default policy that maps to a default class map matching any traffic cannot be deleted.

- Step 6** If you determine that a new policy is needed, click the **Add Policy** taskbar icon to create the policy (see [Creating an Optimization Policy](#)).

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 [Calculating the TCP Buffers for High BDP Links](#).

If you want to adjust the default TCP adaptive buffering settings for your WAE device, see [Modifying the TCP Adaptive Buffering Settings](#).

To modify the acceleration TCP settings, follow these steps:

- Step 1** From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).
- Step 2** Choose **Configure** > **Acceleration** > **TCP Settings**. The Acceleration TCP Settings window appears.
- Step 3** Check the **Send TCP Keepalive** check box. (By default, this check box is 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.
- Step 4** Modify the TCP acceleration settings, as needed. See [Table 12-9](#) for a description of these settings.
- For information on how to calculate these settings for high BDP links, see [Calculating the TCP Buffers for High BDP Links](#).

Table 12-9 TCP Settings

TCP Setting	Description
Optimized Side	
Maximum Segment Size	Maximum packet size allowed between a 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 a 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 a WAAS device. The default is 1432 bytes.
Send Buffer Size	Allowed TCP sending buffers size (in kilobytes) for TCP packets sent from a 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 5 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 **Set High BDP recommended values**. For more information about calculating TCP buffers for high BDP links, see [Calculating the TCP Buffers for High BDP Links](#).

Step 6 Click **Submit**.

**Note**

If the original and optimized maximum segment sizes are set to their default values and you configure a jumbo MTU setting, the segment sizes are changed to the jumbo MTU setting minus 68 bytes. If you have configured custom maximum segment sizes, their values are not changed if you configure a jumbo MTU. For more information on jumbo MTU, see the [Configuring a Jumbo MTU](#) in Chapter 6, “Configuring Network Settings.”

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-512—Default BDP is 32 KB
- WAE-612—Default BDP is 512 KB
- WAE-674—Default BDP is 2048 KB
- WAE-7341—Default BDP is 2048 KB
- WAE-7371—Default BDP is 2048 KB
- All WAVE platforms—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:

$$\text{BDP [Kbytes]} = (\text{link BW [Kbytes/sec]} * \text{Round-trip latency [Sec]})$$

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

$$\text{MaxBDP} = \text{Max (BDP(link 1),...,BDP(link N))}$$

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.

After 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 fields for the optimized connection on the Acceleration TCP Settings window.



Note

These manually configured buffer sizes are applicable 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 [Modifying the TCP Adaptive Buffering Settings](#).

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 menu, choose **Devices > device-name** (or **Device Groups > device-group-name**).
- Step 2** Choose **Configure > Acceleration > TCP Adaptive Buffering Settings**.
The TCP Adaptive Buffering Settings window appears.
- Step 3** To enable TCP adaptive buffering, check the **Enable** check box. (By default, this is enabled.)
- Step 4** In the Send Buffer Size and Receive Buffer Size fields, enter the maximum size, in kilobytes, of the send and receive buffers.
- Step 5** 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.