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 Cisco 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, and Cisco Virtual WAAS (vWAAS) instances.

This chapter contains the following sections:

About Application Acceleration

The Cisco WAAS software comes with more than 150 predefined optimization policies that determine the type of application traffic your Cisco 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 elements shown in the following table:

Table 1: Optimization Policy Elements

Optmization Policy Element	Description
Application Definition	Identifies general information about a specific application, such as the application name and whether the Cisco WAAS Central Manager collects statistics about this application.

Optmization Policy Element	Description
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 800 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 Cisco 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 Cisco 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 Cisco WAAS Central Manager are globally applied to all the Cisco WAAS devices that register with the Cisco WAAS Central Manager, regardless of the device group membership configuration.

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

- Layer 4 optimizations that include Transport Flow Optimization (TFO), Data Redundancy Elimination (DRE), and Lempel-Ziv (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 specified optimization policy, for Cisco WAAS Version 4.4.1 and later, the DRE feature can use different caching modes, shown in the following table.

Table 2: DRE Caching Modes

DRE Caching Mode	Description
Bidirectional	The peer Cisco 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. For Cisco WAAS versions earlier than Cisco WAAS Version 4.4.1, bidirectional mode is the only supported caching mode.

DRE Caching Mode	Description
Unidirectional	The peer Cisco 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 Cisco 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

This section contains the following topics:

About 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 Cisco WAAS optimization techniques to the traffic that it intercepts.

In addition, the global optimization features include each of the following application accelerators:

- Microsoft End Port Mapper (EPM)
- HyperText Transfer Protocol (HTTP)
- Independent Computing Architecture (ICA)
- Messaging Application Programming Interface (MAPI)
- Server Message Block (SMB)
- Secure Sockets Layer (SSL)
- SSL Interposer

By default, all of the application accelerators are enabled except SMB, SSL Interposer and Encrypted MAPI.

Note The application accelerators require specific types of licenses to operate: a Transport license for TFO, DRE, and LZ optimization, and an Enterprise license for all other application accelerators. For more information on installing and managing licenses, see the chapter "Configuring Other System Settings".

Procedure for Enabling and Disabling the Global Optimization Features

Before you begin

- You must enable the accelerator on both of the peer Cisco WAEs at either end of a WAN link for all application accelerators to operate, except for single-sided SMART-SSL acceleration.
- In the case of single-sided SMART-SSL acceleration, you do not need a peer Cisco WAE to exist or for both Cisco WAEs to have the SSL Interposer accelerator enabled.

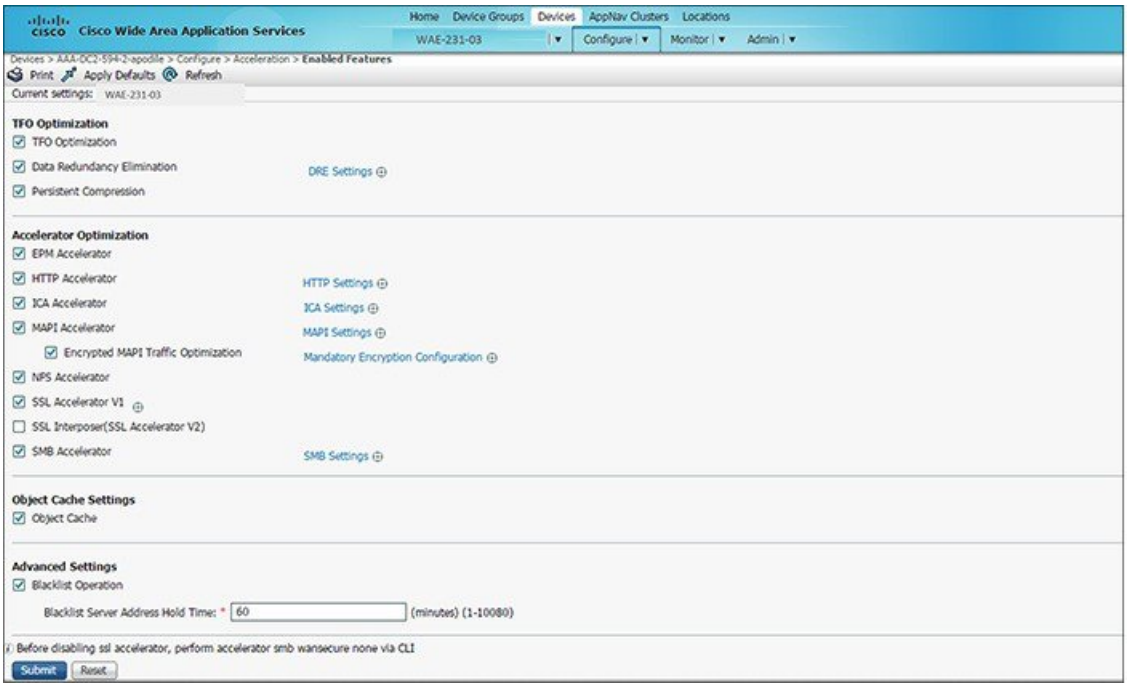
Procedure

Step 1 From the Cisco 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.

Figure 1: Enabled Features Window



For Cisco WAAS Express Devices:

- On Cisco WAAS Express devices, only a subset of the standard features are available. On Cisco 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 Cisco ISR-WAAS devices and one for all other kinds of Cisco WAEs.

- Not all of the properties in the standard Cisco WAAS device are available in the Cisco WAAS Express version of the application accelerators, including SMART-SSL acceleration.

- For Cisco WAAS Express, the following Express versions of application accelerators are supported:
  - HTTP accelerator express (see Configuring HTTP Acceleration)
  - SSL accelerator express (see Configuring SSL Acceleration)
- For a Cisco WAAS device running Cisco WAAS Version 6.x and a Cisco WAAS Express peer device running Cisco IOS Release 15.6(3)M, 15.6(2)T1 or later, TLS1 is supported, but SSL3 is removed. Before upgrading Cisco WAAS Express to one of these Cisco IOS releases, configure TLS1 in the Cisco WAAS Express Device Group:
  a. Navigate to **Device Groups** > *DeviceGroupName* > **Configure** > **Enabled Features**.
  b. Select the **SSL Accelerator Express Peering Service**.
  c. From the **SSL Version:** dropdown list, choose **TLS1**.
  d. Click **Submit**.
  e. Upgrade the Cisco WAAS Express.
- For information on upgrading and interoperability, see the Release Note for Cisco Wide Area Application Services.
- If you try to enable DRE on a Cisco 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 Cisco 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 the chapter "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, on page 9.
- 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 Procedure for Configuring HTTP Acceleration, on page 10.
- 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 Procedure for Configuring ICA Acceleration, on page 35.
- 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 About MAPI Acceleration.

  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 For Encrypted MAPI acceleration to be enabled, you must *first* enable MAPI acceleration.

- 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, on page 37. For Cisco Version 6.2.1 and later, you can accelerate Microsoft Office 365 traffic. For more information, see Configuring Microsoft Office 365 for Cisco WAAS.
- If you check the **SSL Interposer (SSL Accelerator V2)** check box, you must configure additional settings to enable SMART-SSL acceleration. By default, the SSL Interposer is by default SMART SSL will be enabled on a fresh installation, that is, on new OVA deployments, ENCS platforms, 5.5.7 to 6.4.1 upgrades. It will be disabled when you upgrade the devices from Cisco WAAS Software Version 6.2.3 to 6.4.1. For more information, see Configuring SMART-SSL Acceleration.

  Both SSL accelerator and SMART-SSL can co-exist on a device.

Step 4 To enable the object cache, at the **Object Cache Settings** pane, check the **Object Cache** check box.

Cisco 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.

Note Object Cache is not supported on Cisco vWAAS-200 and Cisco vWAAS-150 platforms.

- To enable an individual application accelerator object cache: Controls to enable and disable an individual object cache are displayed in that application accelerator's **Advanced Settings** screen.
- To ensure that the object cache and individual application accelerator object cache work successfully, consider 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 At the **Advanced Settings** pane, uncheck the **Blacklist Operation** check box if you want to disable it.

The **blacklist operation** feature allows a Cisco WAE to better handle situations in which TCP setup packets that have options are blocked or not returned to the Cisco 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 Cisco 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.

Cisco WAAS is able to accelerate traffic between Cisco branch WAEs and Cisco data center WAEs in situations where optioned TCP packets are dropped. We recommend that you leave the **blacklist operation** feature enabled.

Step 6 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.

Configuring Optimization and Acceleration from the Cisco WAAS CLI

This section contains the following topics:

Global Configuration Commands Used to Configure Optimization and Acceleration

The following table shows the Cisco WAAS CLI global configuration commands used to configure optimization and acceleration.

Table 3: Cisco WAAS CLI Commands Used to Configure Optimization and Acceleration

Command Mode	Command	Optimization or Acceleration Configuration Task
Global Configuration	**tfo optimize**	Configure TFO optimization, DRE, and persistent compression.
	accelerator epm	Configure EPM acceleration.
	accelerator http	Configure HTTP acceleration.
	accelerator ica	Configure ICA acceleration.
	accelerator mapi	Configure MAPI acceleration.
	accelerator smb	Configure SMB acceleration.
	accelerator ssl	Configure SSL acceleration.
	object-cache enable	Configure global object cache.
	accelerator *ao-name* **object-cache enable**	Enable a specified application accelerator object cache.
	auto-discovery	Configure the Blacklist Operation feature.
EXEC	**show accelerator**	Display the status of the application accelerators.
	show statistics accelerator	Display statistics for the application accelerators.
	show statistics accelerator smb	Display statistics for the SMB print accelerator.

Optimization and Acceleration Configuration Guidelines

Consider the following guidelines for configuring optimization and acceleration:

- 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.
- To ensure success of the **object-cache enable** global configuration command, verify the following two conditions:
  - Disk assignments have been made to object cache *before* you run this command.
  - Run this command *before* you run the **accelerator smb** global configuration command.
- 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.

- Before you run the **no object-cache enable** global configuration command to disable the global object cache, you must disable *all* individual application accelerator object caches.
- 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.

Configuring Individual Features and Application Accelerators

This section contains the following topics:

Configuring DRE Settings

Before you begin

Data Redundancy Elimination (DRE) is one of the critical technologies used to identify redundant data patterns in application traffic, replacing them with signatures that Cisco WAAS devices transfer across the WAN to regenerate the original data. The result is optimal usage of WAN bandwidth and improved end-user response time.

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

Procedure

Step 1 From the Cisco 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 To generate an alarm and automatically DRE bypass application traffic, check the **Enable DRE auto bypass** check box.

Note If you do not enable DRE auto bypass, the **Device Status** alarm displays yellow and the traffic gets bypassed without forwarding to the Service Node (SN). We recommend that you do not disable DRE through the configuration. Instead, configure individual policies to bypass DRE functionality.

Step 4 To enable load report, check the **Enable DRE Load Monitor** check box.

- The disk latency maximum can be set from **1** to **1000**; the default value is **5**.
- The DRE load threshold can be set from **50** to **99**; the default value is **95**.

Step 5 Click **Submit**.

The changes are saved to the device or device group.

Step 6 To use the Cisco WAAS CLI to enable DRE settings:

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

Configuring HTTP Acceleration

This section contains the following topics:

Procedure for Configuring HTTP Acceleration

Before you begin

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.

Procedure

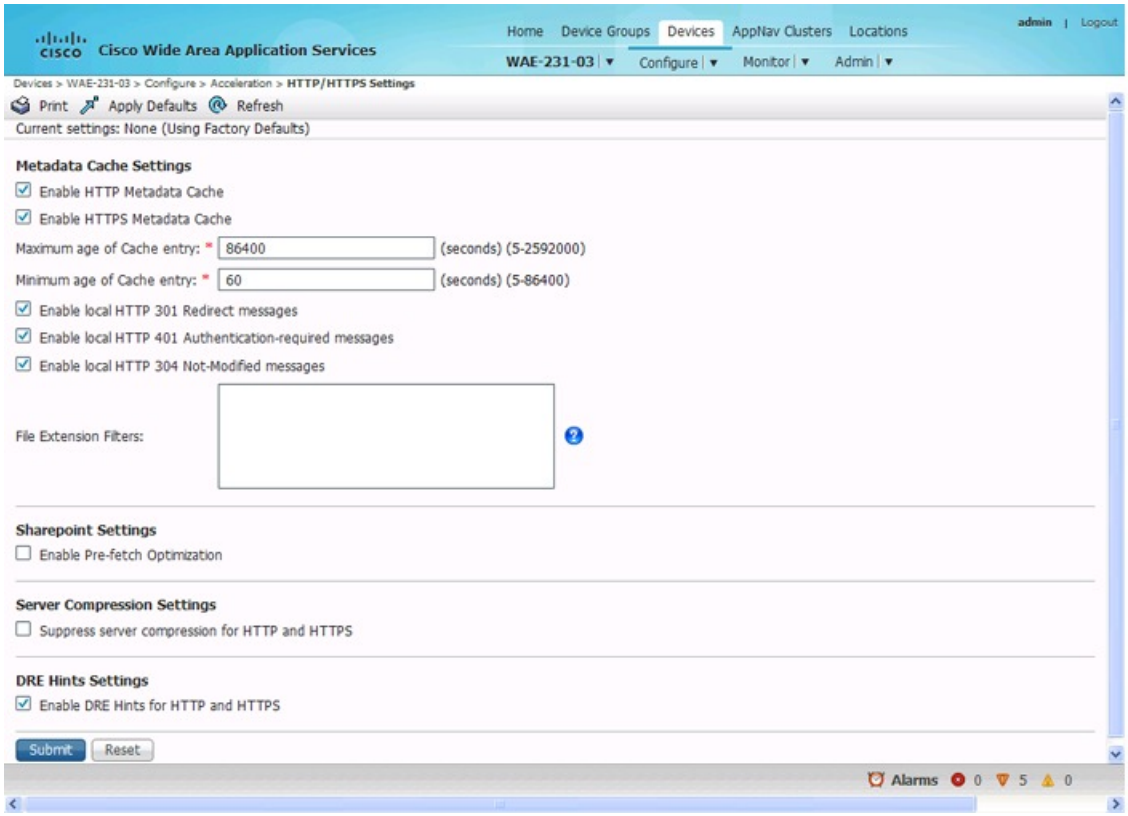
Step 1 To enable the HTTP accelerator: at the **Accelerator Optimization** pane of the **Enabled Features** window, check the **HTTP Accelerator** check box.

Step 2 From the Cisco WAAS Central Manager menu, choose **Devices >** *device-name* or **Device Groups >** *device-group-name*.

Step 3 Choose **Configure > Acceleration > HTTP/HTTPS Settings**.

The **HTTP/HTTPS Acceleration Settings** window appears.

Figure 2: HTTP/HTTPS Settings Window



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

Step 4 Configure the metadata cache settings. At the **Metadata Cache Settings** pane:

a) To enable the Cisco WAE to cache each HTTP header (metadata) information, check the **Enable HTTP metadatacache caching** check box. The default setting is checked.

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

For more information, see HTTP Metadata Caching.

b) To enable the Cisco WAE to cache HTTPS header (metadata) information (HTTP as payload in SSL traffic), check the **Enable HTTPS metadatacache caching** check box. The default setting is checked.

For more information, see HTTP Metadata Caching.

c) 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 **86,400 seconds (24 hours)**. Valid time periods range from 5–2,592,000 seconds (30 days).

d) 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 86,400 seconds (24 hours).

e) To enable the Cisco WAE to cache and to locally serve HTTP 301 messages, check the **Enable local HTTP 301 redirect messages** check box. The default setting is checked.

f) To enable the Cisco WAE to cache and locally serve HTTP 401 messages, check the **Enable local HTTP 401 Authentication-required messages** check box. The default setting is checked.

g) To enable the Cisco WAE to cache HTTP 200 and HTTP 304 messages and locally serve HTTP 304 messages, check the **Enable local HTTP 304 Not-Modified messages** check box. The default setting is checked.

h) 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 of the window. 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 5 To allow the Cisco WAAS Edge WAE to prefetch data, at the **Sharepoint Settings** pane, check the **Enable Pre-fetch Optimization** check box. The default for this setting is unchecked.

- The prefetch optimization benefits the Web browser-based Microsoft Office applications when they access Microsoft Office Word and Microsoft Office Excel documents that are hosted on a Microsoft SharePoint Server 2010. To view Microsoft Word documents, you must have Microsoft Silverlight installed on your system.
- By checking the Enable Pre-fetch Optimization check box, you are directing the Cisco WAAS Edge WAE 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 6 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 7 To configure the Cisco WAE to suppress server compression between the client and the server, at the **Server Compression Settings** pane, check the **Suppress server compression for HTTP and HTTPS** check box. The default setting is checked.

- By checking the **Suppress server compression for HTTP and HTTPS** check box, you are directing the Cisco WAE to remove the Accept-Encoding value from HTTP and HTTPS request headers, which prevents the web server from compressing HTTP and HTTPS data that it sends to the client. This allows the Cisco WAE to apply its own compression to the HTTP and HTTPS data, which typically results in more optimum compression than that of 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 8 To send DRE hints to the DRE module for improved DRE performance, at the **DRE Hints Settings** pane, check the **Enable DRE Hints for HTTP and HTTPS** check box. The DRE hint feature is enabled by default.

Step 9 Click **Submit**.

The changes are saved to the device or device group.

What to do next

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

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

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

To enable or disable specific HTTP accelerator features for specific clients or IP subnets, run the HTTP accelerator subnet feature. For more details, see Using an HTTP Accelerator Subnet, on page 13.

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

Using an HTTP Accelerator Subnet

Before you begin

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 the *Cisco Wide Area Application Services Command Reference* for more information on configuring subnets. You can use both standard and extended ACLs.

Procedure

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. For more information on associating an ACL with an HTTP accelerator feature, see the **accelerator http** global configuration command in the *Cisco Wide Area Application Services Command Reference*:

```
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**.

What to do next

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

This section contains the following topics:

About MAPI Acceleration

Consider the following MAPI acceleration features and guidelines:

- The MAPI application accelerator accelerates Microsoft Outlook Exchange traffic that uses the Messaging Application Programming Interface (MAPI) protocol.
  - For Cisco WAAS Version 5.3.x and later, Microsoft Outlook 2000 to 2013 clients are supported.
  - For Cisco WAAS Version 5.2.x and earlier, Microsoft Outlook 2000 to 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.
- Microsoft Outlook 2007 and 2010 have encryption enabled by default. You must disable encryption to benefit from the MAPI application accelerator.
- MAPI accelerator and the EPM 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 Microsoft Outlook administrator has configured Microsoft 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 Microsoft Outlook.

- If the Cisco 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.
- When you enable MAPI acceleration, Encrypted MAPI acceleration is enabled by default. For more information on Encrypted MAPI acceleration, see Configuring Encrypted MAPI Acceleration.

Configuring MAPI Acceleration Using the Cisco WAAS Central Manager

Procedure

Step 1 To enable the MAPI accelerator, choose **Configure** > **Acceleration** > **Enabled Features** window.

The **Enabled Features** window appears.

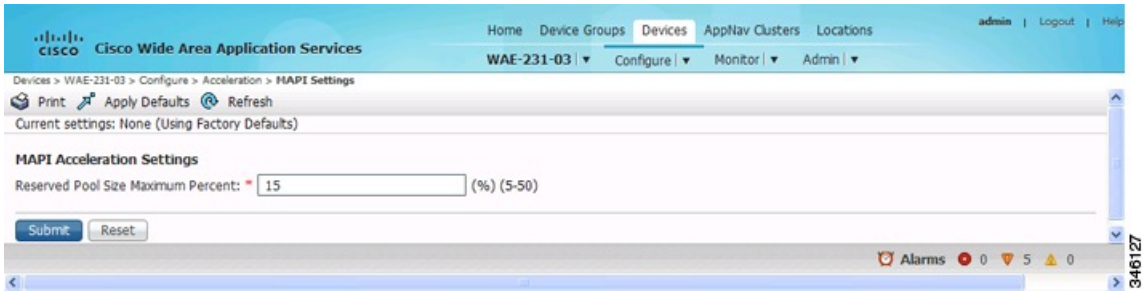
a) At the **Accelerator Optimization** pane, check the **MAPI Accelerator** check box.
b) Click **Submit**.

Step 2 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 3 Choose **Configure** > **Acceleration** > **MAPI Settings**.

The **MAPI Acceleration Settings** window appears.

Figure 3: MAPI Acceleration Settings Window



Step 4 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.

- The maximum percent of connections 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 optimized by the MAPI accelerator.
- The client maintains at least one association group per server to which it connects, with an average of about three connections per association group. For deployments that see a greater average number of

connections per association group, 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 association group is terminated.

Step 5 Click **Submit**.

The changes are saved to the device or device group.

Configuring Encrypted MAPI Acceleration

This section contains the following topics:

About 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.

Consider the following guidelines and terms for encrypted MAPI acceleration:

- You must enable MAPI acceleration first for Encrypted MAPI acceleration to be enabled. Encrypted MAPI acceleration is enabled by default.
- The following terms are used with Microsoft Windows Active Directory and Cisco Encrypted MAPI acceleration:
  - **Microsoft Active Directory**: A set of directory-based and identity-based services developed by Microsoft for Windows domain networks. The Microsoft Active Directory Domain Services (DS) domain controller stores information about domain users and devices
  - **User Identity**: An Active Directory user account. The Microsoft Active Directory employs the user identity to authenticate the user, and to grant appropriate access to domain resources.
  - **Machine Account Identity**: A computer (machine) account used to authenticate the user's computer access to Microsoft Active Directory Domain Services. Each Windows Active Directory computer has a unique machine (computer) account.

Workflow for Configuring Encrypted MAPI

To configure Encrypted MAPI traffic acceleration, complete the tasks listed in the following table. These tasks must be performed on both data center and branch WAEs unless specified as **Not Required** or **Optional**.

Table 4: Workflow for Configuring Encrypted MAPI

Step	Task	Additional Information and Instructions
1.	Configure DNS Settings.	To configure DNS settings, see Configuring the DNS Server in the chapter "Configuring Network Settings."

Step	Task	Additional Information and Instructions
2.	Configure NTP Settings.	To synchronize the time with Active Directory, see Configuring NTP Settings in the chapter "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 Cisco WAAS Central Manager, see Devices Window in the chapter "Monitoring Your Cisco WAAS System."
4.	Configure SSL Peering Service.	To configure SSL Peering Service, see Configuring SSL Peering Service, on page 54.
5.	Verify WAN Secure mode is enabled.	To verify WAN Secure mode is enabled, run the **show accelerator wansecure** EXEC command.
6.	(Optional) 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 the chapter "Configuring Administrative Login Authentication, Authorization, and Accounting." • Performing a domain join of the Cisco WAE is not required on Cisco branch WAE devices. • It is sufficient to create any one identity account, either machine or user. Domain-join is required only for machine account used as an identity account.
7.	Configure domain identities (for machine account and optional user accounts).	To configure a machine account identity, see Configuring a Machine Account Identity, on page 20. (Optional) To create a user account and configure a user account identity, see Creating and Configuring a User Account, on page 21. 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** window 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, on page 3.

Configuring Encrypted MAPI Settings

Procedure

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, see Configuring the DNS Server in the chapter "Configuring Network Settings."

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

The Cisco WAAS device has to be in synchronization with the Active Directory for Encrypted MAPI acceleration. The Cisco WAAS NTP server must share time synchronization with the Active Directory Domain Controllers' domains for which traffic encryption is required.

Note Out-of-sync time will cause Encrypted MAPI acceleration to fail.

For more information, see Configuring NTP Settings in the chapter "Configuring Other System Settings."

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

For more information, see Devices Window in the chapter "Monitoring Your Cisco WAAS Network."

Step 4 Configure the SSL Peering Service.

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

For more information, see Configuring SSL Peering Service, on page 54.

Step 5 Verify that **WAN Secure mode** is enabled.

The default mode is **Auto**.

- To verify the state of WAN Secure mode, run the following EXEC command:

  show accelerator wansecure

- To change the state of WAN Secure mode, run 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 Microsoft Windows domain settings and perform a **domain join**. (A **domain join** automatically creates the machine account in Active Directory.)

- It is sufficient to create any one identity account, either machine or user.
- **Domain join** is required only for machine account used as an identity account.

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

For more information, see Configuring Windows Domain Server Authentication Settings in the chapter "Configuring Administrative Login Authentication, Authorization, and Accounting."

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

Step 7 Configure domain identities. This is not required for branch WAEs.

- As highlighted in Step 6, 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 Cisco 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.

For more information, see Configuring a Machine Account Identity, on page 20.

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.

For more information, see Creating and Configuring a User Account, on page 21.

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

a) From the the Cisco 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) To save your changes, click **Submit**.

Step 9 Enable Encrypted MAPI Traffic Optimization.

a) Choose **Configure > Acceleration > Enabled Features**.

The **Enabled Features** window appears.

b) In the **Enabled Features** window, check the **Encrypted MAPI Traffic Optimization** check box.

c) In the **Enabled Features** window, check the **MAPI Accelerator** check box.

Note To enable Encypted MAPI, you must also check the MAPI Accelerator check box. (Encrypted MAPI traffic optimization is enabled by default.)

d) Click **Submit**.

For more information, see Enabling and Disabling the Global Optimization Features, on page 3.

Configuring a Machine Account Identity

Procedure

Step 1 From the Cisco 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**.

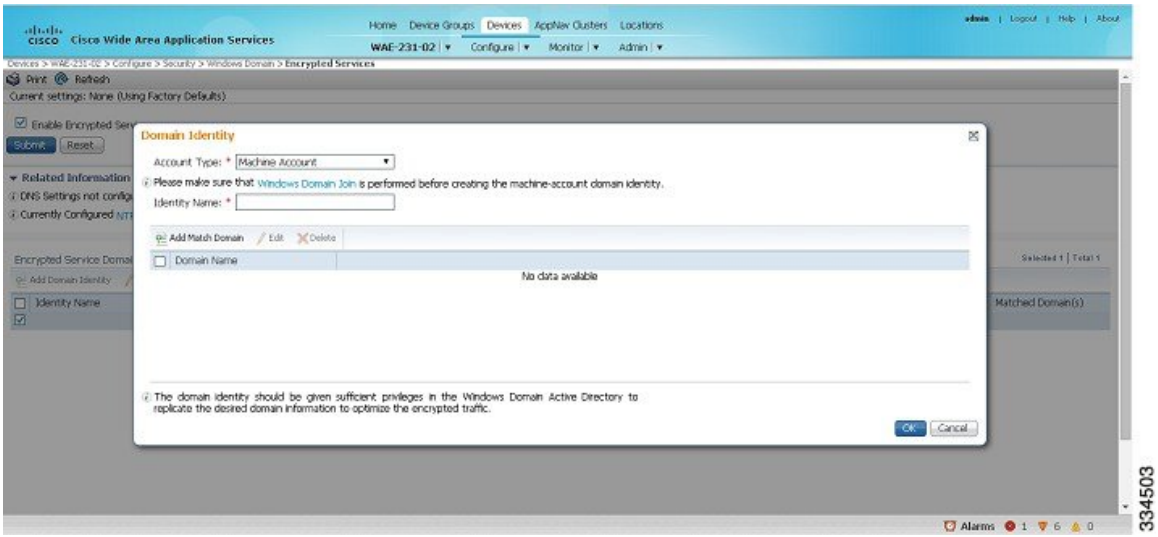
The **Encrypted Services** window appears.

Step 3 Click the **Add Domain Identity** button.

The **Domain Identity** dialog box appears.

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

Figure 4: Add Domain Identity—Machine Account



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

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 Cisco WAAS Device in the chapter "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, on page 23.

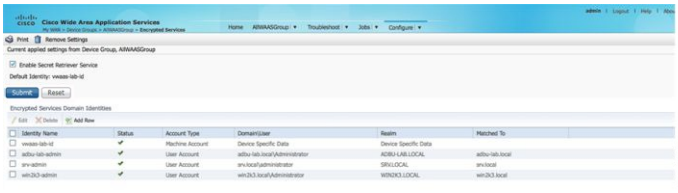
Step 4 Click the **Add Match Domain** button to add the child domains of the domain (with which the device is registered) for which the Domain Identity should optimize the encrypted traffic. You can add up to 32 child domains. If you do not want the Domain Identity to optimize the traffic for any of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

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

Step 5 Click **OK**.

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

Figure 5: Encrypted Services—Domain Identity



333672

Step 6 To configure and verify Encrypted Services Domain Identities from the CLI, run the **windows-domain encrypted-service** global configuration command and the **show windows-domain encrypted-service** EXEC command.

Creating and Configuring a User Account

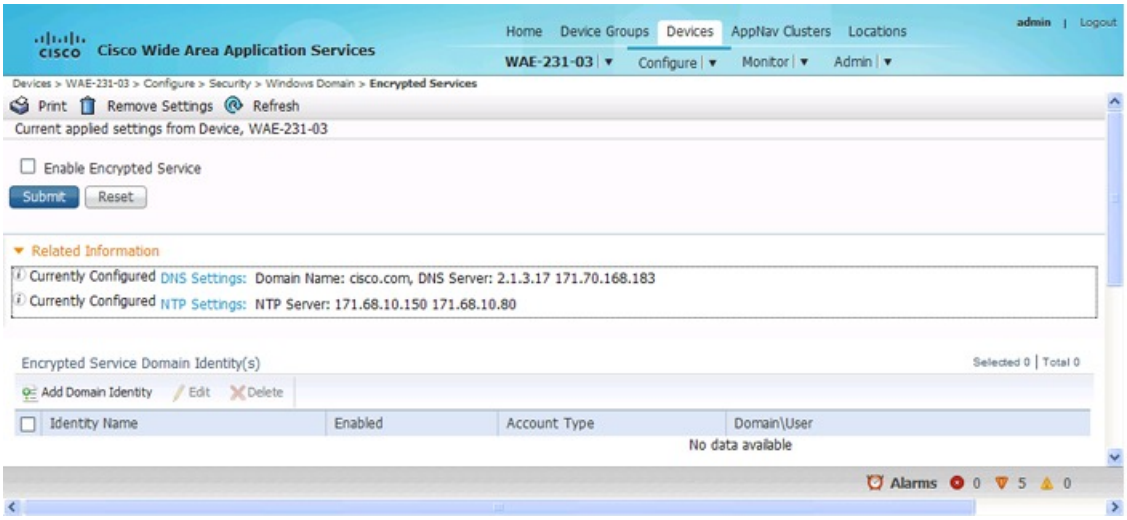
Procedure

Step 1 From the Cisco 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 6: Encrypted Services



Step 3 To add a user account domain identity, in the **Encrypted Service Domain Identity(s)** table listing area, click **Add Domain Identity**.

The **Domain Identity** window appears.

Figure 7: Add Domain Identity—User Account

a) From the **Account Type** drop-down list, choose **User Account**.
b) In the **Identity Name** field, enter the identity name. Use only alphanumeric characters, up to a maximum of 32 characters.
c) Enter username and password.
d) Enter the domain name.
e) Enter the Kerberos realm.
f) To add the child domains of the domain (with which the device is registered) for which the Domain Identity should optimize the encrypted traffic, click the **Add Match Domain** button.

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 more information, see Configuring Microsoft Active Directory, on page 23.

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.

Step 5 To configure and verify Encrypted Services Domain Identities from the CLI, run the **windows-domain encrypted-service** global configuration command and the **show windows-domain encrypted-service** EXEC command.

Configuring Microsoft Active Directory

Procedure

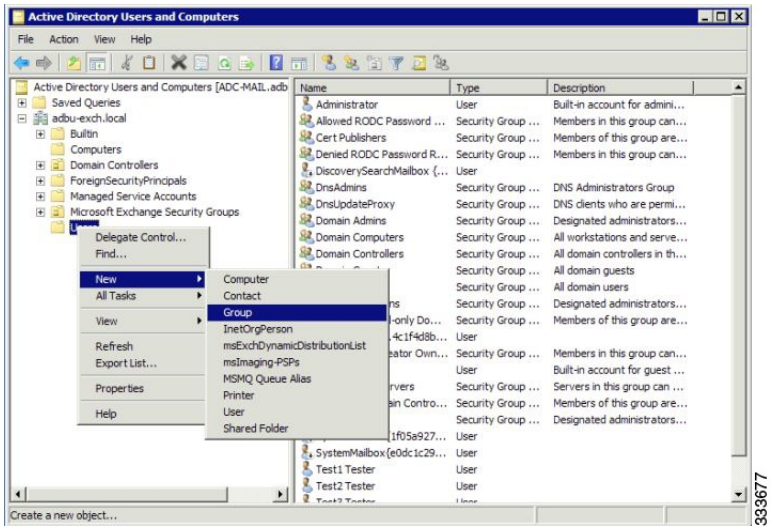
Step 1 To grant Cisco WAAS permission to accelerate Microsoft Exchange-encrypted email sessions: Using an account with Domain Administrator privileges, launch the Active Directory Users and Computers application.

Step 2 Create a new group.

Note This group is for accounts that Cisco WAAS will use to optimize Microsoft Exchange traffic. Regular 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 8: 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**.

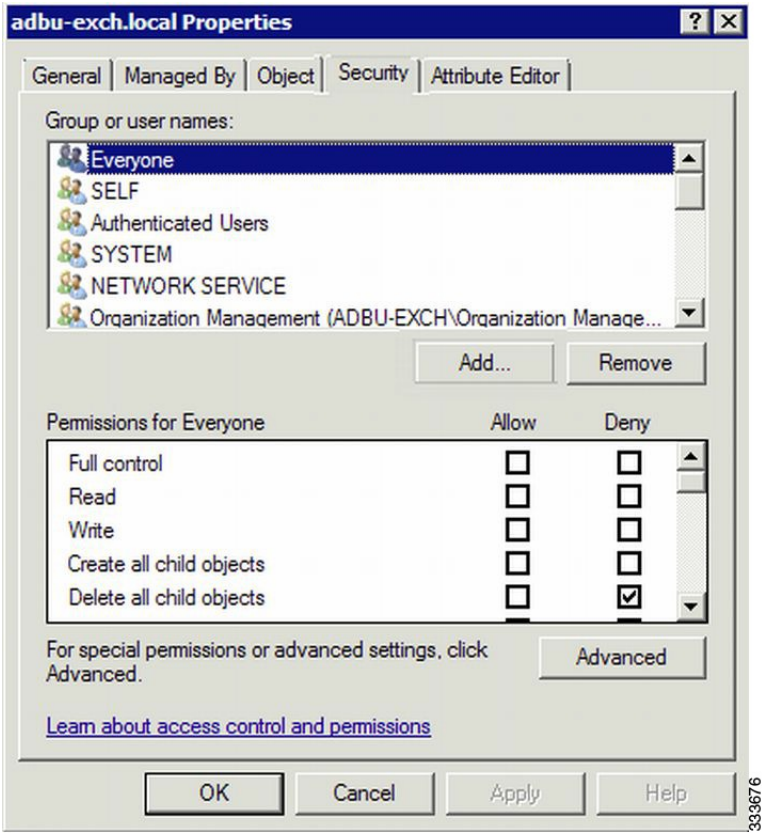
Step 3 Configure the permissions required by Cisco WAAS.

a) At the menu bar of the **Active Directory Users and Computers** window, choose **View > Advanced Features**.

b) Right-click the root of the domain and choose **Properties**.

c) Click the **Security** tab.

Figure 9: Active Directory—Security Tab



d) In the **Group** or **User Names** section, click **Add**.

e) In the **Enter the object names to select** field, enter the name of the new group .

f) To add the new group to the list, click **OK**.

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**.

The configuration of **Active Directory** permissions is complete.

Managing Domain Identities and Encrypted MAPI State

This section contains the following topics:

Note To view the statistics for Encrypted MAPI connections, see MAPI Acceleration Charts in the chapter "Monitoring Your Cisco WAAS Network."

Editing an Existing Domain Identity

Before you begin

You can modify the attributes of an existing domain identity on a Cisco 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 Cisco 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 Cisco 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 Cisco WAAS device.

Procedure

Step 1 To change the password for a user account domain identity on a Cisco WAAS device when the password for the account in the **Active Directory** has changed: From the Cisco 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 In the **Password** field, change the password. The password should be the same as the password for the account in **Active Directory**.

Step 5 Click **OK**.

Deleting an Existing Domain Identity

Procedure

Step 1 From the Cisco 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 Cisco WAAS device.

If the domain identity is being used for optimizing encrypted traffic, a warning message appears.

Step 4 To accept the procedure, click **OK**, or to cancel the procedure, click **Cancel**.

Disabling Encrypted MAPI

Procedure

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

Step 2 Disable **Encrypted Service**.

a) From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.

The **Encrypted Services** window appears.

b) Uncheck the **Enable Encrypted Service** check box.

c) To save your changes, click **Submit**.

Step 3 Disable **Encrypted MAPI Traffic Optimization**.

a) From the menu, choose **Configure** > **Acceleration** > **Enabled Features**.

The **Enabled Features** window appears.

b) Uncheck the **Encrypted MAPI Traffic Optimization** check box.

c) To save your changes, click **Submit**.

To view the statistics for Encrypted MAPI connections, see MAPI Acceleration Charts in the chapter "Monitoring Your Cisco WAAS Network."

Cisco WAAS MAPI RPC over HTTP(S)

Remote Procedure Call over HTTP(S) (RPC over HTTP(S) allows Microsoft Outlook clients to access Exchange servers from outside the enterprise network using HTTP or HTTPS as a transport for RPC protocol. It allows a client on the Internet to connect securely to a Microsoft Exchange Server without having to log into a virtual private network (VPN) first.

An RPC-HTTP (RPC-H) module in Cisco WAAS, integrated into the existing Cisco WAAS MAPI optimizer will provide Cisco WAAS the ability to optimize MAPI over RPC-HTTP(S) traffic.

Cisco WAAS Version 6.2.x and later supports L7 optimization for RPC-HTTP(S) traffic.

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

The following table shows the clients and servers supporting Cisco WAAS MAPI RPC over HTTP(S):

Table 5: Clients and Servers Supporting Cisco WAAS MAPI RPC over HTTP(S)

Clients Supported	Servers Supported
Microsoft Outlook 2016	Microsoft Exchange 2016
Microsoft Outlook 2013(for Windows 7 and Windows 8)	Microsoft Exchange 2013(for Windows Server 2012, 2012 R2, 2008 R2 [full installation])
Microsoft Outlook 2010(for Windows 7 and Windows 8)	Microsoft Exchange 2010(for Windows Server 2012, 2012 R2, 2008, and 2008 R2)
Microsoft Outlook 2007(for Windows Vista, Windows 7)	

Exchange 2013 and Exchange 2016 can be configured for MAPI over HTTP support. MAPI over HTTP traffic will not be optimized by MAPI accelerator. However, MAPI over HTTP traffic will get L4 optimization benefits from WAAS (THSDL).

Configuration Prerequisites for Optimizing MAPI RPC over HTTP(S)

Procedure

Step 1 Ensure that the SSL, HTTP and MAPI accelerators are enabled. If you have enabled SSL Interposer (SSL Accelerator V2) on both branch and data center devices, MAPI over RPC HTTPS will use Smart-SSL and not SSL Accelerator V1.

Step 2 Configure SSL acceleration. For more information, see Configuring SSL Acceleration, on page 37. If you enable SSL Interposer (SSL Accelerator V2) on both branch and data center devices, MAPI over RPC HTTPS will use Smart-SSL and not SSL Accelerator V1.

Step 3 When you configure SSL acceleration, be sure to enable protocol chaining, by checking the **Enable protocol chaining** check box in the **SSL Accelerated Services** window.

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

Step 4 Configure a Microsoft Windows domain identity on the core device, for Encrypted MAPI connections.

Step 5 Verify that encryption is enabled in the MAPI accelerator. For more information, see Configuring Encrypted MAPI Settings, on page 18.

MAPI Acceleration Charts for Cisco WAAS MAPI RPC over HTTP(S)

The MAPI Acceleration report displays MAPI acceleration statistics. For Cisco WAAS Version 5.5.3 and later, 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 the chapter "Monitoring Your Cisco WAAS Network."
- **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 in the chapter "Monitoring Your Cisco WAAS Network."

Cisco WAAS MAPI over HTTP

MAPI over HTTP provides the ability for Messaging API (MAPI) clients and servers to communicate across HTTP connection that no longer use RPC technology. This provides faster re-connects and improved reliability.

Cisco WAAS Version 6.4.3 and later provides optimization support for MAPI over HTTP traffic. This is enabled by default and uses SMART-SSL acceleration and protocol chaining to intercept and accelerate the MAPI over HTTP traffic. To ensure this optimization, you need to enable the SMART-SSL (SSL Accelerator v2) accelerator.

For more information on how to set up the exchange service, see, Using SSL Accelerated Services, on page 56.

The MAPI Acceleration report displays MAPI acceleration statistics. For more information, see MAPI: Handled Traffic Pattern and MAPI: Connection Details in the chapter "Monitoring Your WAAS Network."

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

The following table shows the clients and servers supporting Cisco WAAS MAPI over HTTP:

Table 6: Clients and Servers Supporting Cisco WAAS MAPI over HTTP

Clients Supported	Servers Supported
Microsoft Outlook 2010 (Jan 2015 Public Update – For MAPIoHTTP)	Microsoft Exchange 2013 SP1(Win 2008 R2, Win 2012 R2)
Microsoft Outlook 2013 (SP1 – For MAPIoHTTP)	Microsoft Exchange 2016(Win 2012 R2, Win 2016)
Microsoft Outlook 2016	

Configuring SMB Acceleration

This section contains the following topics:

About SMB Acceleration

The Service Message Block (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:
  - Print from branch client to branch printer.
  - Print from branch client to data center printer.
  - 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 OpLock 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 Microsoft 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, Microsoft 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.
- **SMB v3 Encrypted Optimization**: The SMB accelerator provides L7 optimization of encrypted SMB v3 traffic.

Configuring SMB Acceleration with the Cisco WAAS Central Manager

Procedure

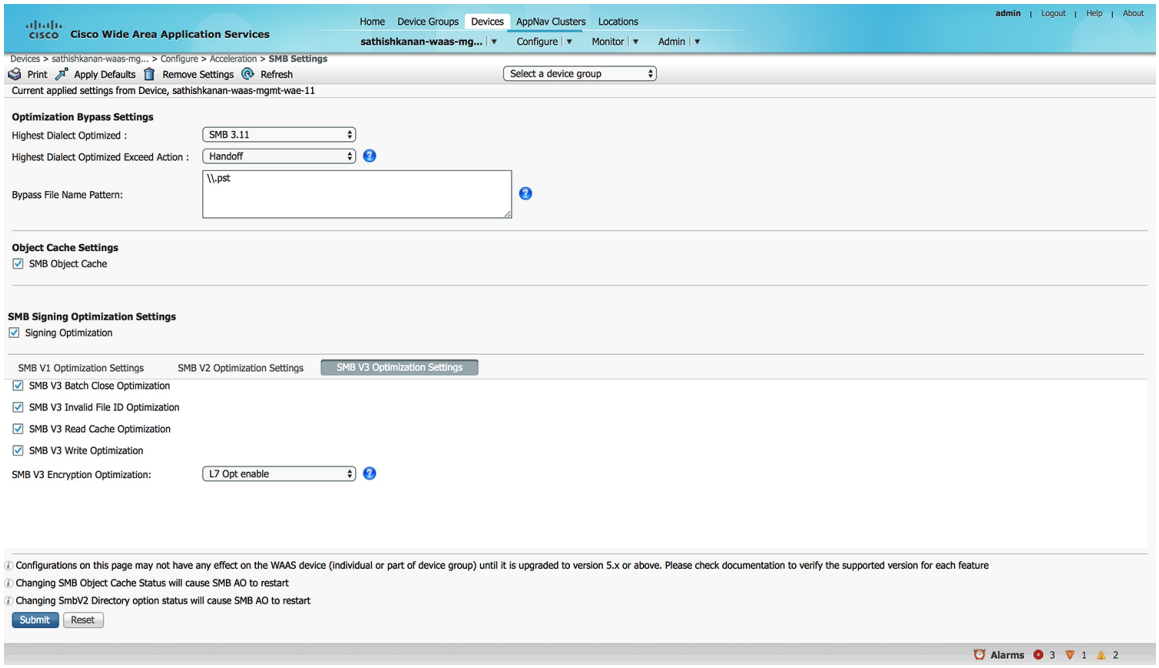
Step 1 To enable the SMB accelerator, check the **SMB Accelerator** check box in the **Enabled Features** window.

Step 2 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 3 Choose **Configure** > **Acceleration** > **SMB Settings**.

The **SMB Settings** window appears.

Figure 10: SMB Settings Window



Step 4 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
- SMB 3.1.1

Step 5 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.

Note For SMB 2.1 only, you must use the Cisco WAAS CLI to configure the Handoff parameter, running the **accelerator smb smb2-1 exceed-action handoff** global configuration command. If you use the Cisco WAAS Central Manager to select the Handoff parameter for SMB 2.1, the Highest Dialect Optimized Exceed Action will not take effect, and Handoff will not be displayed in commands like the **show running-configuration** command or the **show accelerator smb** command.

Step 6 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 7 To enable disk caching for SMB traffic, check the **SMB Object Cache** check box.

Step 8 To enable optimization of signed SMB v2 and v3 traffic, check the **Signing Optimization** check box. 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:

- If an SMB connection is either a signed SMBv2 or an encrypted SMBv3, or has originated from an SMBv3 enabled client such as Windows 8 and above, then you must configure an identity as a pre-requisite to receive SMB optimization at Layer 7. Otherwise, you will only get Layer 4 (TDL) optimization benefits on these connections.
- It is sufficient to configure either a user identity or a machine identity; the administrator can decide based on ease of configuration. Both configurations are equal and serve the purpose of key retrieval. Domain-join is required only for machine identity.
  - On the Cisco Core WAE, configure a valid user-identity with administrator privileges to enable secret-retrieval to fetch and cache the longterm service key of the SMB server by running the following global configuration command.

    windows-domain encryption-service identity [*identity*] *user-account name* [*admin-username*] **domain** [*your.domain*] **realm** [*your.domain*] *password*

    To verify the identity configuration, run the following EXEC Command.

    show windows-domain encryption-service identity detail

    (Optional) To configure a machine identity, instead of using user identity, you can also follow the steps in the procedure Configuring a Machine Account Identity.

  - For Kerberos Authentication to work correctly, ensure time synchronization between Client, Server, Cisco Core WAE and the Domain Controller.
- To verify whether a connection is signed or not, look into the SMBv2 Negotiate packet. The Signing Required field should be set to True in either the Negotiate Request or the Negotiate Response exchange.

- To verify if a connection has originated from a SMB3 capable client, look into the SMBv2 Negotiate Request packet. Under the dialects list, you should see some or all of the following dialects: SMB3.0, SMB3.02, or SMB3.11.

  These configurations are similar to the EMAPI configuration. For more information, see Step 6 of the procedure 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**. To verify the state of **WAN Secure mode**, run the following EXEC command:

    show accelerator wansecure

  - To change the state of WAN Secure, run the following global configuration command:

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

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

Step 9 Click the **SMBV1 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.
- Select the type of optimization you want from the **SMB v3 Encryption Optimization** drop down box - L7 Optimization, L4 only optimization or disable SMB v3 encrypted optimization. L7 optimization is selected by default.

Step 10 Click the **SMBV2 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.
- Select the type of optimization you want from the **SMB v3 Encryption Optimization** drop down box - L7 Optimization, L4 only optimization or disable SMB v3 encrypted optimization. L7 optimization is selected by default.

Step 11 Click the **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.
- Select the type of optimization you want from the **SMB v3 Encryption Optimization** drop down box - L7 Optimization, L4 only optimization or disable SMB v3 encrypted optimization. L7 optimization is selected by default.

Step 12 To save the changes, click **Submit**.

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

Configuring SMB Acceleration with the Cisco WAAS CLI

To configure SMB acceleration using the Cisco WAAS CLI, run the accelerator smb global configuration command.

Consider the following operating guidelines for running the **accelerator smb** global configuration command:

- The enterprise license is required to start the SMB accelerator.
- The **show running-config** EXEC mode command displays non-default settings only. Therefore, the command **no accelerator smb enable** does not display in the running configuration if the SMB accelerator is disabled, while the **accelerator smb enable** command does display if the SMB accelerator is enabled.
- Run the **accelerator smb signing unwrap enable** command to verify signature of the signed request packets at the Cisco Edge WAE. This checks whether the packet is modified/tampered while coming over the LAN. However, since the packet usually travels in the LAN from the Client to the Cisco Edge WAE, chances of man-in-middle attacks are less likely and you may choose to disable Edge side signature verification for request packets
- Run the **accelerator smb wansecure-mode always** command to enable WAN Secure mode for optimizing signed SMBv2 traffic. The default is always. The WAN Secure mode configuration for both the Cisco Edge WAE and Cisco Core WAE must match (be set at always) for the SMB accelerator to optimize signed SMBv2 connections. Even if one side has none set, then the signed connections would be handed over for generic optimization.
- Run the **accelerator smb wansecure-mode none** to disable the wansecure-mode.
- WAN Secure mode requires that the SSL application accelerator is enabled. Use the accelerator ssl enable global configuration command to enable the SSL accelerator
- For more information on the **accelerator smb** global configuration command, see the *Cisco Wide Area Application Services Command Reference*.

Configuring ICA Acceleration

This section contains the following topics:

Procedure for Configuring ICA Acceleration

Before you begin

The Independent Computing Architecture (ICA) application accelerator provides WAN optimization on a Cisco 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 Cisco WAAS device by default.

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

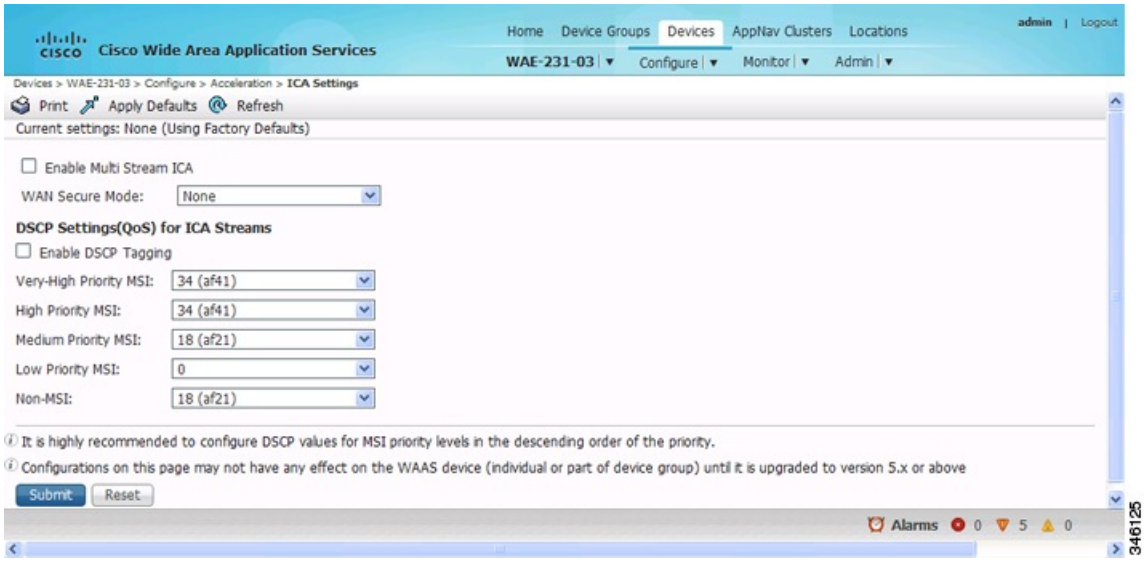
Procedure

Step 1 From the Cisco 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 11: 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 To configure DSCP values for MSI priority levels: In the **DSCP Settings (QoS) under ICA Streams** section, check the **Enable DSCP Tagging** check box. These values override the defaults.

Consider the following ranges and guidelines:

- Configure DSCP values for MSI priority levels in the descending order of the priority.
- **Very High-Priority MSI**: Typically real-time traffic, such as audio. The default is **af41**.
- **High-Priority MSI**: Typically interactive traffic. The default is **af41**.
- **Medium-Priority MSI**: Typically bulk data. The default is **af21**.
- **Low-Priority MSI**: Typically background traffic, such as printing. The default is **0**, best effort.
- **Non-MSI**: (the default is **af21**)
- MSI priority configuration might not apply to devices earlier than Cisco WAAS Version 5.1.x.

Step 6 Click **Submit**.

The changes are saved to the device or device group.

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

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

Configuring ICA over Socket Secure (SOCKS) Server

Before you begin

Consider the following about ICA over SOCKS:

- In a typical deployment where NetScaler is deployed as a SOCKS proxy, the connections from the client go to the SOCKS server instead of the XenApp server.
- Because the ICA optimizer accepts and intercepts only ICA and CGP packets, the packets with SOCKS headers are not recognized and the connection is handed off. The ICA traffic does not get optimized in such scenarios.
- The Cisco WAAS software supports optimizing ICA traffic redirected over SOCKS proxy servers for Cisco WAAS Version 6.3.1 and later.

Considering the following prerequisite configuration guidelines for ICA over SOCKS:

- Make the necessary changes on the NetScaler Gateway to enable the SOCKS proxy (Cache redirection server).
- Make the equivalent and required changes on the StoreFront server along with updates to the **default.ica** file.
- Consider the following NetScaler gateway limitations for ICA over SOCKS:

- Non-default ports configured with Multi-Port Policy on XenApp for Multi-Stream ICA (MSI) are not supported.
- SOCKS with ICA over SSL is not supported.
- SOCKS Version 4 is not supported. ICA over SOCKS Version 5 is supported for the NetScaler gateway.

- For more information on the Netscaler gateway, see Citrix NetScaler documentation.

Procedure

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

Step 2 Next choose **Configure** > **Acceleration** > **Optimization Class-Map**.

Step 3 Edit the class-map named Citrix and add the required port number using the **Add Match Condition** option.

The port number added in the class-map should be the same as the one configured for the SOCKS proxy, on the NetScaler gateway.

Note If the SOCKS proxy port is running on ICA or CGP ports, 1494 or 2498, then you do not need to modify the existing configuration.

Step 4 Select the branch device and make the necessary changes for the port number.

Alternately, run the **class-map type match-any citrix** global configuration command to make these changes.

Configuring ICA over SSL

The Cisco 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, on page 37.

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

Configuring SSL Acceleration

This section contains the following topics:

About SSL Acceleration

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

Consider the following operating guidelines for SSL acceleration:

- On a Cisco WAAS Express device, only SSL cipher list, SSL certificate authorities, and SSL peering service configuration are supported.
- The SSL accelerator does not optimize protocols that do not start their SSL and Transport Layer Security (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 and 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 will not occur. Manual bypass of TLSv1.1 or TLSv1.2 packets is required in order to make these client/server connections.

Workflow for Configuring SSL Acceleration

The following table provides an overview of the steps you must complete to set up and enable SSL acceleration.

Table 7: Workflow for Configuring SSL Acceleration

Step	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 Cisco WAAS devices. For more information, see Prerequisites for Configuring SSL Acceleration.
2	Enable secure store, the Enterprise License, and SSL acceleration.	Describes how to set up the Cisco WAAS 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 Prerequisites for Configuring 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, on page 3.
4	Configure SSL acceleration settings.	(Optional) Describes how to configure the basic setup of SSL acceleration. For more information, see Configuring SSL Global Settings, on page 41.
5	Create and manage cipher lists.	(Optional) Describes how to select and set up the cryptographic algorithms used on your Cisco WAAS devices. For more information, see Working with Cipher Lists, on page 46.

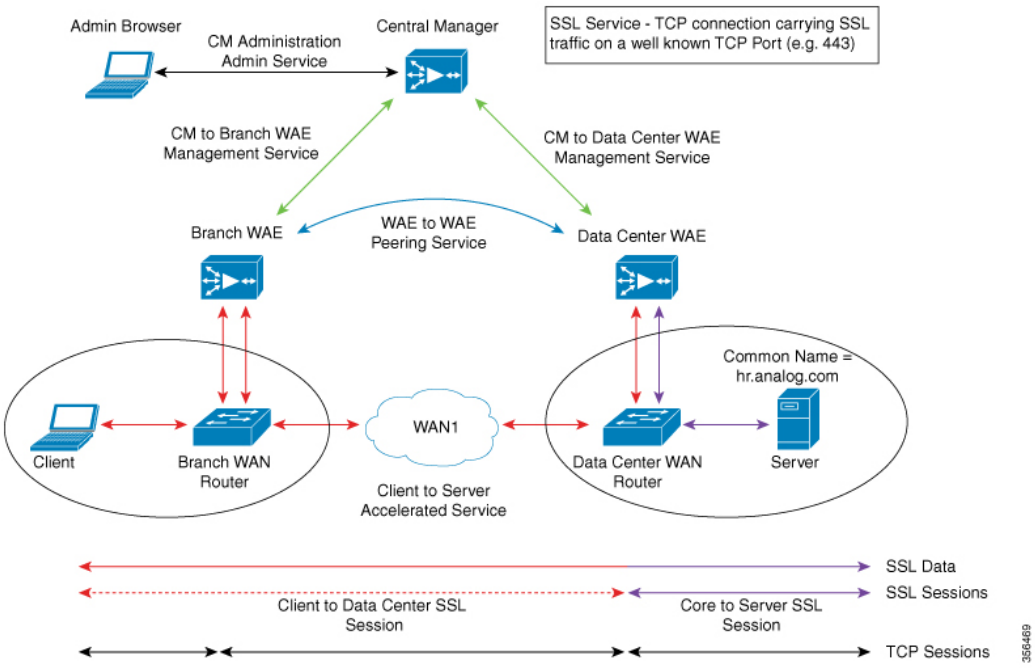
Step	Task	Additional Information and Instructions
6	Set up CA certificates.	(Optional) Describes how to select, import, and manage certificate authority (CA) certificates. For more information, see Working with CA Certificates, on page 48.
7	Configure SSL management services.	(Optional) Describes how to configure the SSL connections used between the Cisco WAAS Central Manager and Cisco WAE devices. For more information, see Configuring SSL Management Services, on page 52.
8	Configure SSL peering service.	(Optional) Describes how to configure the SSL connections used between peer Cisco WAE devices for carrying optimized SSL traffic. For more information, see the Configuring SSL Peering Service, on page 54.
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, on page 56.

Prerequisites for Configuring SSL Acceleration

Considering the following prerequisites for configuring SSL acceleration:

- **Confirming your network information**
  - services that you want to be accelerated on the SSL traffic
  - server IP address and port information
  - Public Key Infrastructure (PKI) certificate and private key information, including the certificate common name and Certificate Authority (CA) signing information
  - cipher suites supported
  - SSL versions supported
  - The following figure shows how the Cisco WAAS software handles SSL application optimization.

Figure 12: SSL Acceleration Block



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

- **Enabling Secure Store Encryption on the Cisco WAAS Central Manager**

  Before you can use SSL acceleration on your Cisco WAAS system, you must enable Secure Store encryption on the Cisco WAAS Central Manager. For more information on this procedure, see Configuring Secure Store Encryption Settings in the chapter "Configuring Other System Settings."

- **Enabling Enterprise licenses on the Cisco WAAS Central Manager and Cisco WAEs**

  Before you can use SSL acceleration on your Cisco WAAS system, you must enable the Enterprise license. For more information on this procedure, see Managing Cisco WAAS Software Licenses in the chapter "Configuring Other System Settings."

- **Enabling SSL acceleration on Cisco WAAS Devices**

  Before you can use SSL acceleration on your Cisco WAAS system, you must enable SSL acceleration on Cisco WAAS devices. For more information, 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 Cisco WAE with a Cisco WAAS Central Manager before making any configuration changes. Otherwise, the changes may not take effect.

Configuring SSL Global Settings

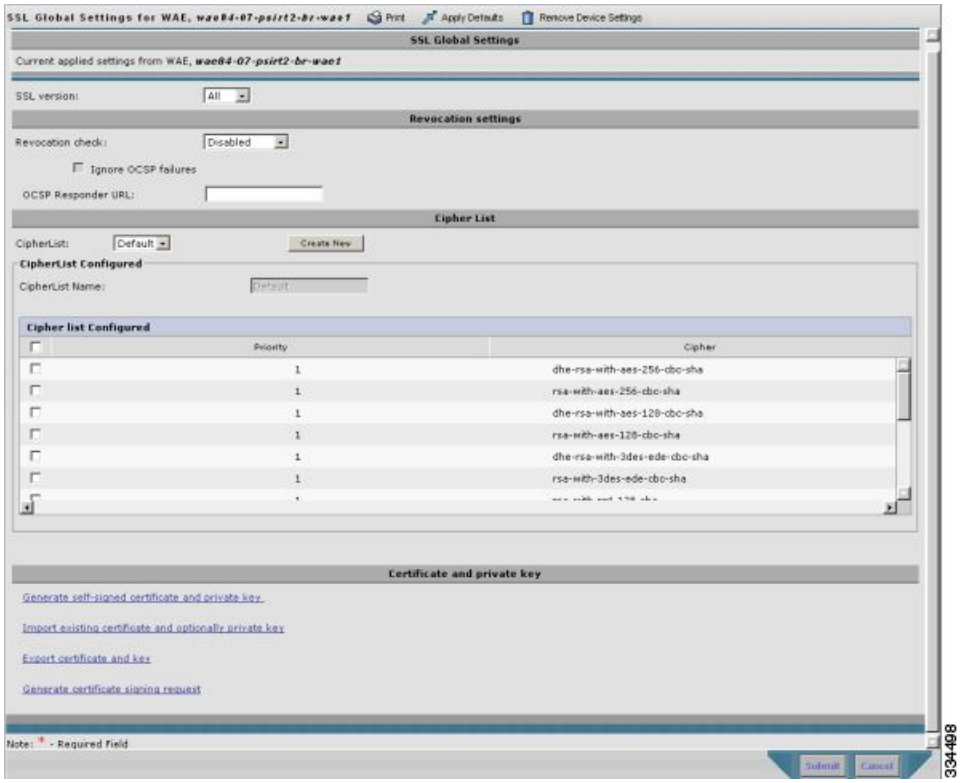
Procedure

Step 1 From the Cisco 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 13: SSL Global Settings Window



Step 3 To configure a device to use SSL settings from a particular device group: From the **Select a Device Group** drop-down list in the **SSL global settings** toolbar, choose a device group.

- A device can use its own SSL settings, or the SSL settings from a device group. However, you cannot configure a device to use SSL settings from multiple device group.

- If you have configured a device with specific SSL Accelerated Services and assigned it to a device group, these configurations are lost when you click the **Override Group Settings in the Device Group > Configure > Security > SSL > Global Settings** window.

Note If you have configured the device with specific SSL Accelerated Services and assigned it to a Device Group, those configurations are lost when you click on the Override Group Settings on the **Device Group > Configure > Security > SSL > Global Settings** window.

Step 4 From the **SSL version** drop-down list, choose the type of SSL protocol to use.

- For the SSL Version 3 protocol, choose **SSL3**.
- For the Transport Layer Security Version 1 protocol, choose **TLS1**.
- To accept both SSL3 and TLS1 SSL protocols, choose **All**.

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 to check the revocation status of certificates:
  - To use the OCSP responder specified in the **OCSP Responder URL** field, choose **ocsp-url**
  - To use the OCSP responder URL specified in the Certificate Authority, choose **ocsp-cert-url**.
- If the **Ignore OCSP failures** check box is checked, 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, on page 46.

Step 7 Choose a certificate/key pair method.

Figure 14: Configuring Service Certificate and Private Key Window

- To direct Cisco WAAS devices to use a self-signed certificate and key pair for SSL, click **Generate Self-signed Certificate Key**.
- To upload or paste an existing certificate and key pair, click **Import Existing Certificate Key**.
- To export the current certificate and key pair, click **Export Certificate Key**.
- 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 a **PKCS12** format or a **PEM** format.

- To use the client configured certificate, click **Import existing client certificate and optionally private key**.

For information about service certificate and private key configuration, see Generating, Importing, or Exporting a Service Certificate and Private Key, on page 43.

Step 8 Click **Submit**.

Generating, Importing, or Exporting a Service Certificate and Private Key

Procedure

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

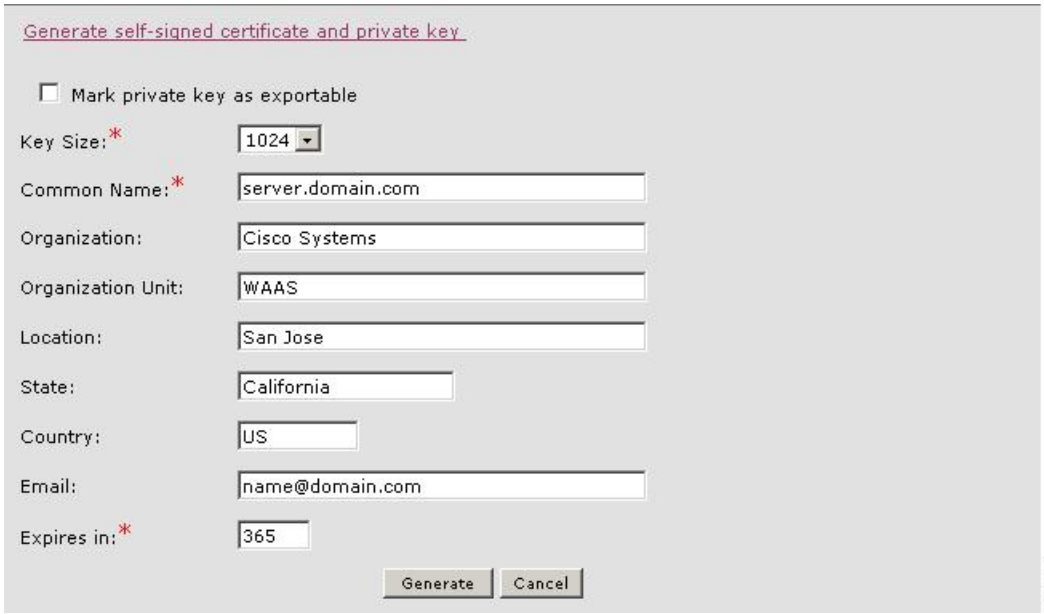
Step 2 Choose **Configure** > **Security** > **SSL** > **Global Settings**.

The **SSL Global Settings** window appears (Figure 13: SSL Global Settings Window).

Step 3 **To generate a self-signed certificate and private key**, at the **Certificate and private key** pane, click **Generate self-signed certificate and private key**.

The **Generate self-signed certificate and private key** window appears.

Figure 15: Generate Self-Signed Certificate and Private Key Window



a) To export this certificate/key in the Cisco WAAS Central Manager and device CLI later, check the **Mark private key as exportable** check box.
b) Fill in the certificate and private key fields.
c) Consider the following guidelines for the **Key Size** drop-down list:

Table 8: Key Size Field Guidelines

Cisco WAAS Version	Key Size Field Guideline
Cisco WAAS Version 6.1.x and earlier	• The **Key Size** drop-down list values are 512, 768, 1024, 1536, and 2048 • A self-signed certificate with an RSA modulus size of 512 is *not* compatible with Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later. • A self-signed certificate with an RSA modulus size of 512 is compatible with Internet Explorer 8 and later. • If you have previously configured the RSA modulus size as 512: to access the Cisco WAAS Central Manager Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later, you must regenerate the self-signed certificate with an RSA modulus size of 2048, and then upgrade to the specified version of Mozilla FireFox or Google Chrome.
Cisco WAAS Version 6.2.x and later	• The **Key Size** drop-down list values are 768, 1024, 1536, and 2048.

Step 4 **To import an existing certificate or certificate chain and, optionally, private key**:

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

At the **Importing Existing Certificate or Certificate Chain** window:

Figure 16: Importing Existing Certificate or Certificate Chain Window

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**

Consider the following operating guidelines for importing an existing certificate or certificate chain and private key:

- If the certificate and private key are already configured, you can update only the certificate. In this case, the Cisco WAAS 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 Cisco WAAS 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 Cisco WAAS 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) At the **Upload** field, use the **Browse** button to browse to the file and then select it.
d) In the **Passphrase to decrypt private key** field, enter a passphrase to decrypt the private key. If the private key is not encrypted, leave this field blank.

Step 5 **To export a configured certificate and private key**, in the **Export Certificate and Key** window:

a) In the **Encryption pass-phrase** field, 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.

The Cisco WAAS 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 6 **To generate a certificate-signing request from a current certificate and private key**, in the **Generate Certificate-Signing Request** window, follow these steps:

Step 7 To update the current certificate with one signed by the Certificate Authority, follow these steps:

a) At the **Certificate and private key** pane, click **Export certificate and key**.

The **Export certificate and key** window appears.

Figure 17: Export Certificate and Key Window

b) In the **Encryption pass-phrase** field, enter the encryption passphrase.
c) Choose an export format for the certificate:

- **Export certificate and private key in PKCS 12 format**
- **Export certificate and private key in PEM format**

For PEM format, both the certificate and private key are included in a single PEM file

Note The Cisco WAAS Central Manager does not allow the export of certificate and private key if the certificate and key were marked as nonexportable when they were generated or imported.

Working with Cipher Lists

Before you begin

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.

For dual-sided deployments that use SMART-SSL acceleration, only **rsa-with-aes-256-cbc-sha** is supported.

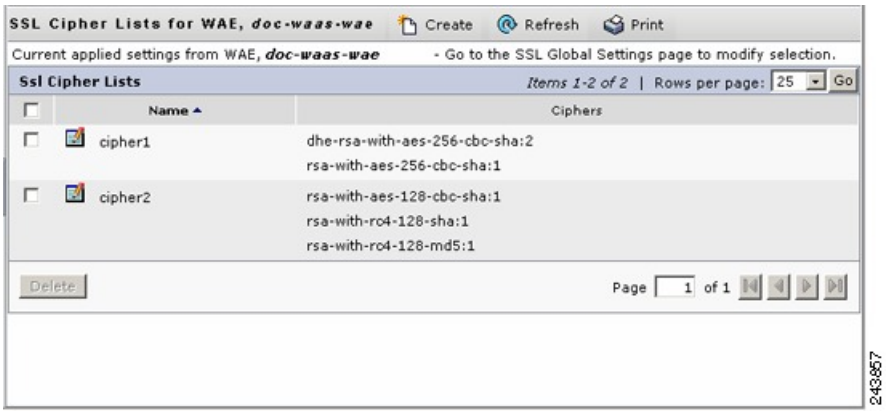
Procedure

Step 1 From the Cisco 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 18: SSL Cipher Lists Window

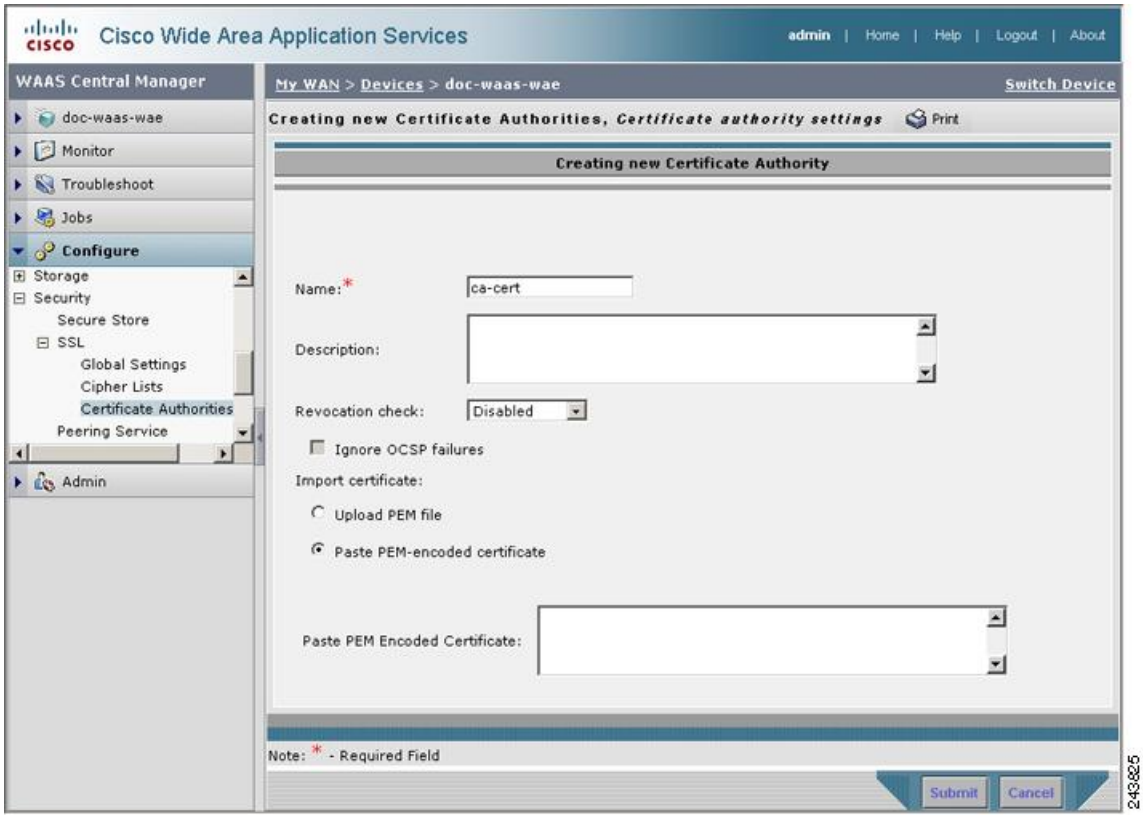


For a Cisco WAAS Express device, the SSL Cipher Lists window shows the same name and cipher fields, but in a slightly different format.

Step 3 To add a new cipher list, click **Create**.

The **Creating New SSL Cipher List** window appears.

Figure 19: Creating New SSL Cipher List Window



To add a new cipher list for a Cisco WAAS Express device, click **Add Cipher List**.

Step 4 In the Cipher List Name field, type a name for your cipher list.

Step 5 To add cipher suites to your cipher list, click **Add Cipher**.

Note For a Cisco WAAS Express device, select the ciphers you wish to add, and proceed 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 From the **Priority** drop-down list, choose the priority for the selected cipher suite.

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 To include the selected cipher suite on your cipher list, click **Add**. To leave the list as it is, click **Cancel**.

Step 9 To add more cipher suites to your list as desired, repeat Step 5 through Step 8 .

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 After you have completed configuring the cipher list, click **Submit**.

Note To save the cipher list configuration for a Cisco WAAS Express device, click **OK**. SSL configuration changes are not applied on the device until the security license has been enabled on the device.

Working with CA Certificates

Before you begin

Use the Cisco WAAS SSL acceleration feature to configure the Certificate Authority (CA) certificates used by your system. You can use one of the many CA certificates included with Cisco WAAS, or import your own CA certificate.

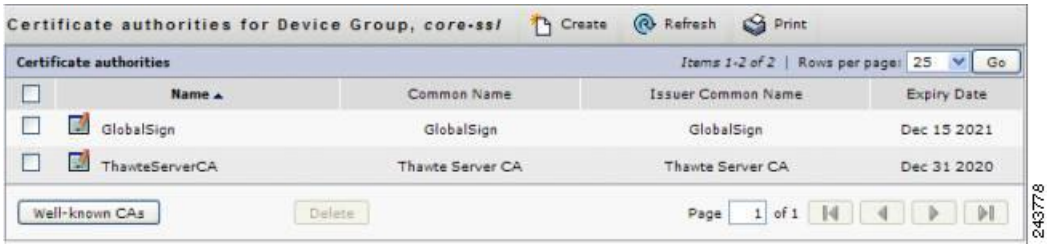
Procedure

Step 1 From the Cisco 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 20: SSL CA Certificate List Window



For a Cisco 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 Cisco WAAS Express, proceed to Step 4 .

Step 3 To add one of the preloaded CA certificates that is included with Cisco WAAS:

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

b) Choose the pre-existing CA certificate you want to add and click **Import**.

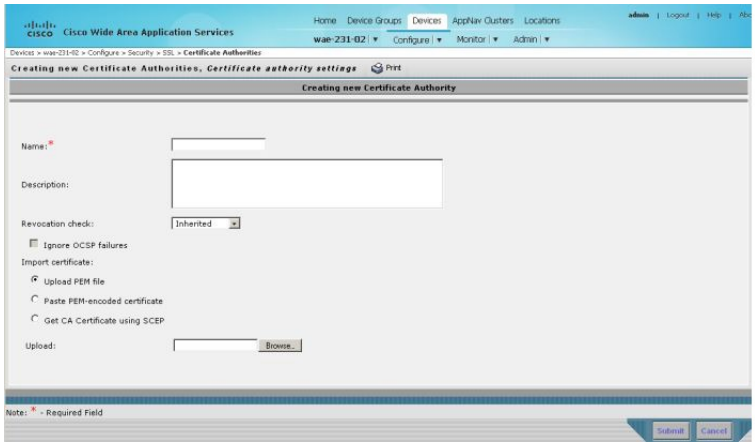
The selected CA certificate is added to the list on the **SSL CA Certificate List** display.

Step 4 To add your own CA certificate:

a) Click **Create**.

The **Creating New CA Certificate** window appears.

Figure 21: Creating New CA Certificate Window



For a Cisco 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, proceed to Step 6.

b) In the **Certificate Name** field, type a name for the certificate.

c) (Optional) In the **Description** field, type a description of the CA certificate.

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) To add the certificate information, choose one of the following:

- **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 Configuring SSL Auto Enrollment, on page 50.

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 After you have completed configuring the CA certificate list, click **Submit**.

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

Configuring SSL Auto Enrollment

Before you begin

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

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

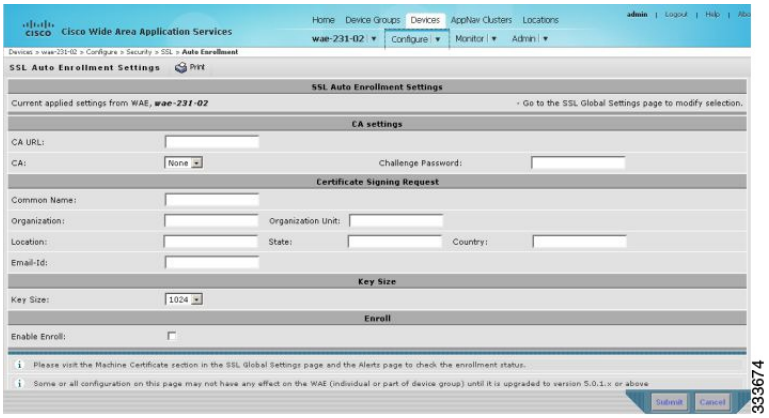
Procedure

Step 1 From the Cisco 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 22: SSL Auto Enrollment Settings Window



Step 3 Configure the following CA settings:

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

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**.

After you have submitted the settings, you can check the enrollment status in the **Machine Certificate** section in the **SSL Global Settings** window and in the **Alerts** window.

Configuring SSL Admin Service

Before you begin

To enable trusted SSL communication between the Cisco WAAS Central Manager the web browser, export the SSL CA signed certificate. The default certificate for enabling SSL communication is the Cisco WAAS Central Manager self signed certificate. To use a different certificate, you must configure it.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices > CM > Configure > Security > SSL Admin Service**.

The default certificate is displayed.

Step 2 Select the PKI operation

a) To upload or paste an existing certificate and key pair, click **Import Existing Certificate Key**.

b) To export the current certificate and key pair, click **Export Certificate Key**.

The file that you import or export must be in either a PKCS12 format or a Privacy Enhanced Mail (PEM) format.

c) To configure the Cisco WAAS Central Manager and Cisco WAAS device to use a self-signed certificate and key pair for SSL, click **Generate Self-signed Certificate Key**.

Operating Considerations for **Key Size** field:

Cisco WAAS Version 6.1.x and earlier

- The **Key Size** drop-down list values are **512**, **768**, **1024**, **1536**, and **2048**.
- A self-signed certificate with an RSA modulus size of **512** is *not* compatible with Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later.
- A self-signed certificate with an RSA modulus size of **512** *is* compatible with Internet Explorer 8 and later.
- If you have previously configured the RSA modulus size as **512**: to access the Cisco WAAS Central Manager Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later, you must regenerate the self-signed certificate with an RSA modulus size of **2048**, and then upgrade to the specified version of Mozilla FireFox or Google Chrome.

Cisco WAAS Version 6.2.x and later

- The **Key Size** drop-down list values are **768**, **1024**, **1536**, and **2048**.

- The key size **512** is *not* used with WAAS Version 6.2.x and later.

Step 3 Click Submit to register the certificate.

Step 4 To register the certificate, click **Submit**.

The Cisco WAAS Central Manager now uses the specified certificate for SSL communication.

Configuring SSL Management Services

Before you begin

SSL management services are the SSL configuration parameters that affect secure communications between the Cisco WAAS Central Manager and the Cisco WAE devices. The certificate and key pairs used are unique for each Cisco WAAS device. Therefore, SSL management services can only be configured for individual devices, not device groups.

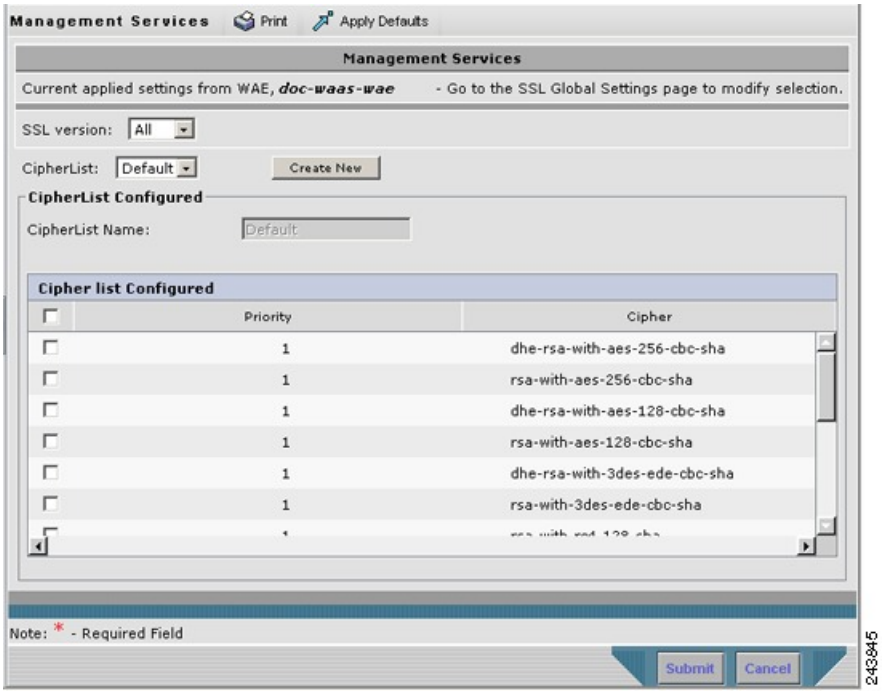
Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.

Step 2 Choose **Configure** > **Security** > **Management Service**.

The **Management Services** window appears.

Figure 23: SSL Management Services Window



Step 3 From the **SSL version** drop-down list, choose the type of SSL protocol to use:

- To use the SSL Version 3 protocol, choose **SSL3**.
- To use the Transport Layer Security Version 1 (TLS Version 1) protocol, choose **TLS1**.
- To use both SSL Version 3 and TLS Version 1 protocols, choose **All**.

Consider the following configuration guidelines for SSL connections:

- Management-service SSL version and cipher settings configured for the Cisco WAAS Central Manager are also applied to SSL connections between the Cisco WAAS Central Manager and the browser of the user.
- Primary and standby Cisco WAAS 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 Cisco WAAS Central Manager and the standby Cisco WAAS Central Manager and Cisco WAE devices.

The following cipher lists are supported in SSL Acceleration (Legacy SSL Acceleration).

- dhe-rsa-with-aes-256-cbc-sha
- rsa-with-aes-256-cbc-sha
- dhe-rsa-with-aes-128-cbc-sha
- rsa-with-aes-128-cbc-sha
- dhe-rsa-with-3des-ede-cbc-sha
- rsa-with-3des-ede-cbc-sha
- rsa-with-rc4-128-sha
- rsa-with-rc4-128-md5
- dhe-rsa-with-des-cbc-sha
- rsa-export1024-with-rc4-56-sha
- rsa-export1024-with-des-cbc-sha
- dhe-rsa-export-with-des40-cbc-sha
- rsa-export-with-des40-cbc-sha
- rsa-export-with-rc4-40-md5
- rsa-with-des-cbc-sha

Consider the following configuration guidelines for ciphers:

- All browsers support SSLv3 and TLSv1 protocols, but TLSv1 may not be enabled by default on certain browsers. 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 Cisco WAAS Central Manager. If this occurs, to restore the connection: configure the Cisco WAAS Central Manager management service SSL settings to the default in the Cisco WAAS 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 Cisco WAAS Central Manager, which can result in the browser showing an error page after you submit the changes. If this occurs, reload the page.

- To configure additional ciphers, see the supported ciphers in Preparing to Use SMART-SSL Acceleration.

Step 4 At the **Cipher List** pane, choose a list of cipher suites to be used for SSL acceleration. For more information, see Working with Cipher Lists, on page 46 for additional information.

Configuring SSL Peering Service

Before you begin

SSL peering service configuration parameters control the secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections. The peering service certificate and private key is unique for each WAAS device and can only be configured for individual devices, not device groups.

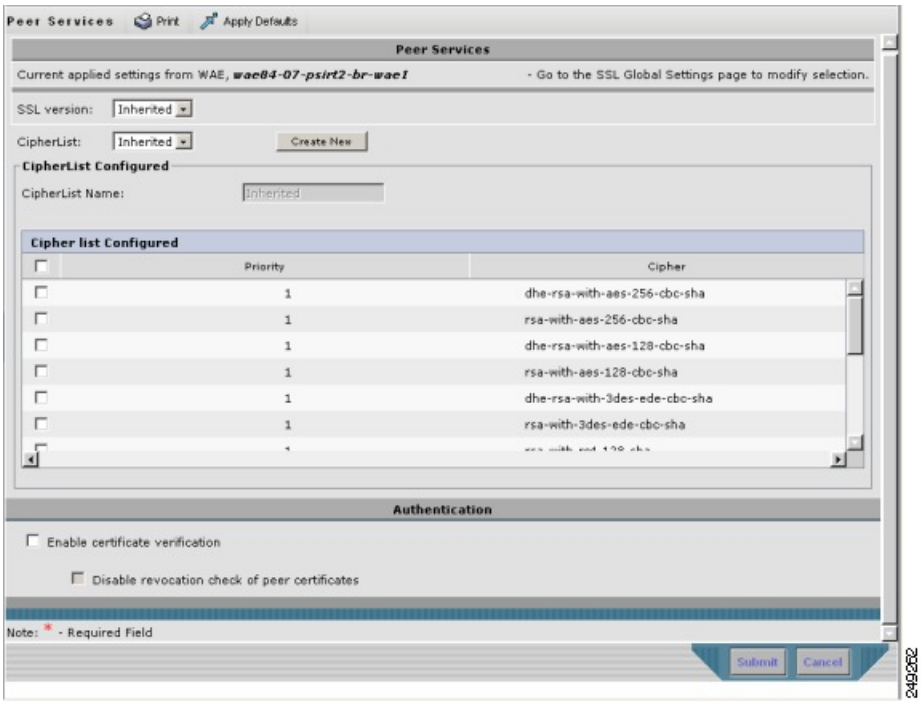
Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.

Step 2 Choose **Configure** > **Security** > **Peering Service**.

The **Peering Service** window appears.

Figure 24: SSL Peering Service Window



Consider the following guidelines for Cisco WAAS Express:

- For a Cisco WAAS Express device, the **Peering Service** window displays 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 Cisco WAAS Express.

Step 3 From the **SSL Version** drop-down list, choose the type of SSL protocol to use:

- For the SSL Version 3 protocol, choose **SSL3**.
- For the Transport Layer Security Version 1 protocol, choose **TLS1**.
- To accept both SSL3 and TLS1 SSL protocols, choose **All**

  .
- To use the protocol configured in **Global SSL Settings**, choose **Inherited**.

Consider the following SSL guidelines:

- For dual-sided deployments that use SMART-SSL acceleration, SSLv3, TLS1.0, TLS1.1, and TLS1.2 are supported.
- In a Cisco 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.
- For dual-sided deployments that use SMART-SSL acceleration, you can use your certificate or use the peer certificate.

Step 5 To disable OCSP certificate revocation checking, check the **Disable revocation check for this service check box**.

This option is not available for Cisco WAAS Express devices.

Step 6 At the **Cipher List** pane, choose a list of cipher suites to be used for SSL acceleration between the WAE device peers.

- To use the cipher list configured in SSL Global Settings, choose **Inherited**.
- For dual-sided deployments that use SMART-SSL acceleration, only **rsa-with-aes-256-cbc-sha** is supported.
- In a Cisco WAAS Express device, the list of cipher suites to be used for SSL acceleration is displayed in the **Cipher List** pane.
- For more information, see Working with Cipher Lists.

Step 7 Click **Submit**.

For a Cisco 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

Before you begin

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.

For Cisco WAAS Version 6.4.3 and later, the SMART- SSL feature has been enhanced to allow you more control of SSL traffic.

- Use the DSCP marking feature for optimized traffic, which allows better QoS management for the overall network.
- Configure more than one service with same port and “Any” Server IP address. However, the secondary flag should be marked to differentiate services with multiple Any/Port which have already been added by other service. Once configured, this is reflected in **Devices >** *device-name* or **Device Groups >** *device-group-name* **> Configure > Acceleration > SSL Accelerated Services**.

To modify the secondary flag the following conditions should be met.

- You should mark a service as Secondary to proceed with IP Any and same port.Once a service is marked as secondary no other IP Any is allowed, but you can add different IP with ports, server, name and domain name to the secondary service.
- You cannot mark a service as Secondary without "Any" server address configuration.
- You cannot remove the Secondary settings if the SSL accelerated service is enabled.
- The above features are visible on the Cisco WAAS Central Manager only when the devices are running Cisco WAAS Version 6.4.3 and later.

Procedure

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

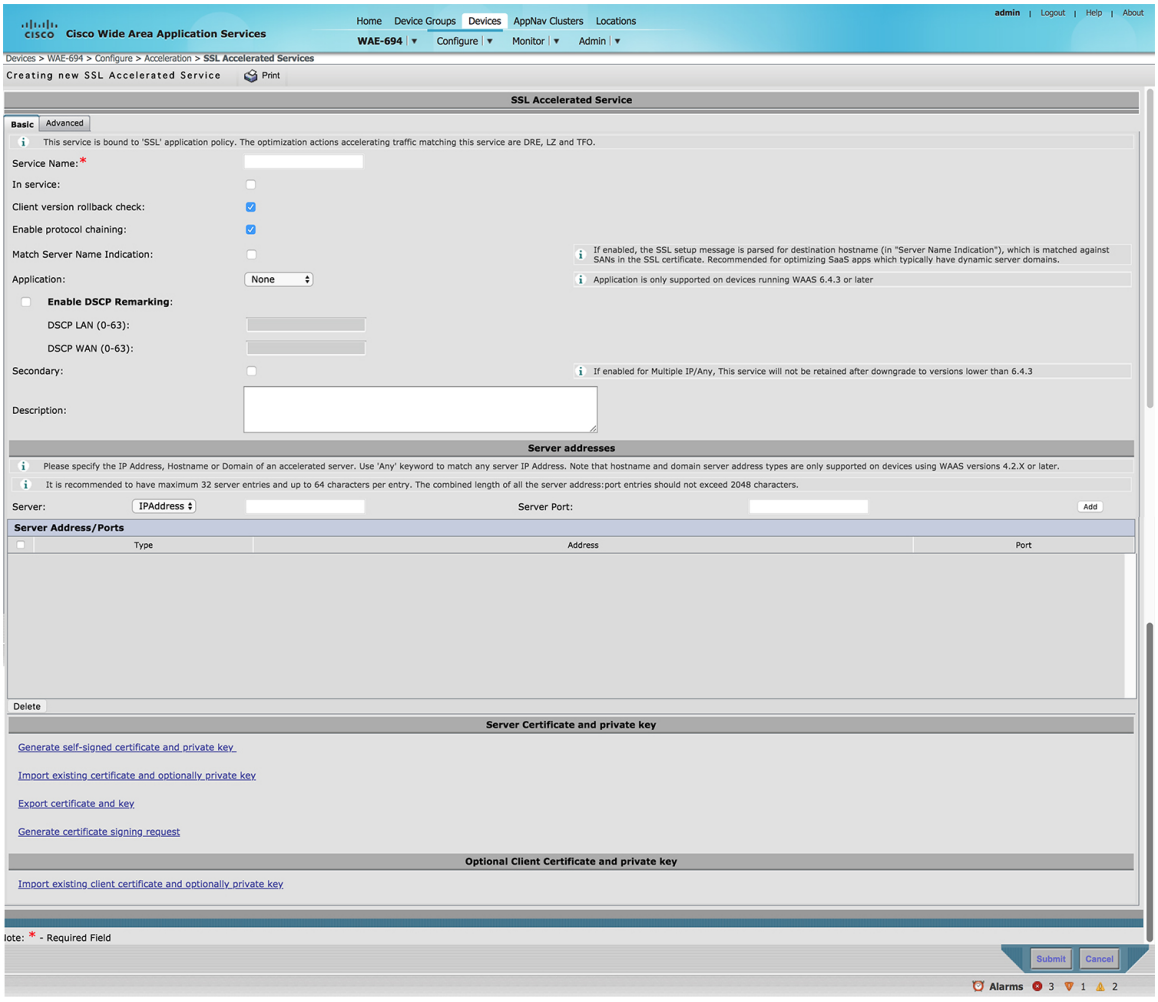
Step 2 Choose **Configure > Acceleration > SSL Accelerated Services**.

Step 3 To delete an accelerated service, select the service and click **Delete**.

Step 4 To define a new accelerated service, click **Create**. A maximum of 512 accelerated services are allowed.

The **Basic SSL Accelerated Services Configuration** window appears.

Figure 25: SSL-Accelerated Services (Basic tab) Window



Step 5 At the **SSL Accelerated Service** pane:

a) In the **Service Name** field, enter a name for the service.

b) To enable this accelerated service, check the **In service** check box.

c) 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.

d) To match subject alternative names, check the **Match Server Name Indication** check box.

For more information, see Configuring SSL Acceleration for SaaS Applications.

e) To enable protocol chaining, check the **Enable protocol chaining** check box.

Enabling protocol chaining allows other protocols to be optimized over SSL.

f) From the **Application** drop-down list, choose the SAAS application that needs to be optimized.

This field is visible only on the devices that are running Cisco WAAS Version 6.4.3 or later.

g) Check the **Enable DSCP Remarking** and enter values in the **DSCP LAN** and **DSCP WAN** fields. The available values are **0** to **63**.

- The **Enable DSCP Remarking** check box is unchecked (disabled) by default.
- For this configuration to be applicable to all devices that are part of a device group, all devices in the device group must be running Cisco WAAS Version 6.4.3 or later. If any of the devices has a version earlier than Cisco WAAS Version 6.4.3, the configurations will not apply to that device.

h) To configure the accelerated service to use multiple IP addresses, check the **Secondary** checkbox.

This is applicable only for Cisco WAAS devices running Cisco WAAS Version 6.4.3 or later.

- (Optional) In the **Description** field, enter a description.

Checking the **Secondary** check box ensures the following actions for this accelerated service:

- This accelerated service is distinguished from the primary accelerated service using multiple IP addresses.
- This accelerated service is not pushed down to other devices that are part of the device group that are running a Cisco WAAS version that is earlier than Cisco WAAS Version 6.4.3.
- This accelerated service is removed during a downgrade.

Step 6 At the **Server addresses** pane:

a) From the **Server** drop-down list, choose **IP Address**, **Hostname**, or **Domain as the SSL service endpoint** type.

b) In the associated **Server** field, enter one of the following:

- **Server IP address** (or **proxy IP address**) of the accelerated server, up to a maximum of 32 IP addresses.To specify any server IP address, use the keyword Any. Server IP address keyword Any is supported for Cisco WAAS Software Version 4.2.x and later.
- **Hostname** of the accelerated server, up to a maximum of 32 hostnames. Hostname server address type is supported for Cisco WAAS Version 4.2.x and later.
- **Domain** of the accelerated server, up to a maximum of 32 domains. Domain server address type is supported for Cisco WAAS Version 4.2.x and later.

c) At the **Server Port** field, enter the port associated with the service to be accelerated.

Step 7 Click **Add** to add each address. If you specify a server hostname, the Cisco WAAS Central Manager resolves the hostname to the IP address and adds it to the **Server IP/Ports** table.

Step 8 To remove an IP address from the list, click **Delete**.

Step 9 Choose a certificate and key pair method.

Figure 26: Configuring Service Certificate and Private Key

- At the **Server Certificate and private key** pane:
  - To configure the Cisco WAAS devices to use a self-signed certificate and key pair for SSL, click **Generate self-signed certificate key**.
  - To upload or paste an existing certificate and key pair, click **Import Existing Certificate Key**.

    For SaaS applications, the certificate must have the Subject Alternative Name (SAN) information.
  - To export the current certificate and key pair, click **Export Certificate Key**.
  - To renew or replace the existing certificate and key pair, click **Generate Certificate Signing Request**. The certificate signing request is used by the CA to generate a new certificate.

    The file to be imported or exported must be in either PKCS12 format or PEM format.
  - To use the client configured certificate, click **Import existing client certificate and optionally private key**.

Step 10 (Optional) To change the service certificate or private key for an existing SSL-accelerated service, follow these guidelines:

a) At the **SSL Accelerated Service** pane, uncheck the In service check box.
b) To disable the service, click **Submit**, and then wait five minutes.
c) Check the **In service** check box.
d) To re-enable the service, click **Submit**.
e) Alternatively, in the Cisco WAE CLI:
   - Run the **no inservice** SSL-accelerated service configuration command.
   - Wait a few seconds.
   - Run the **inservice** SSL-accelerated service configuration command.

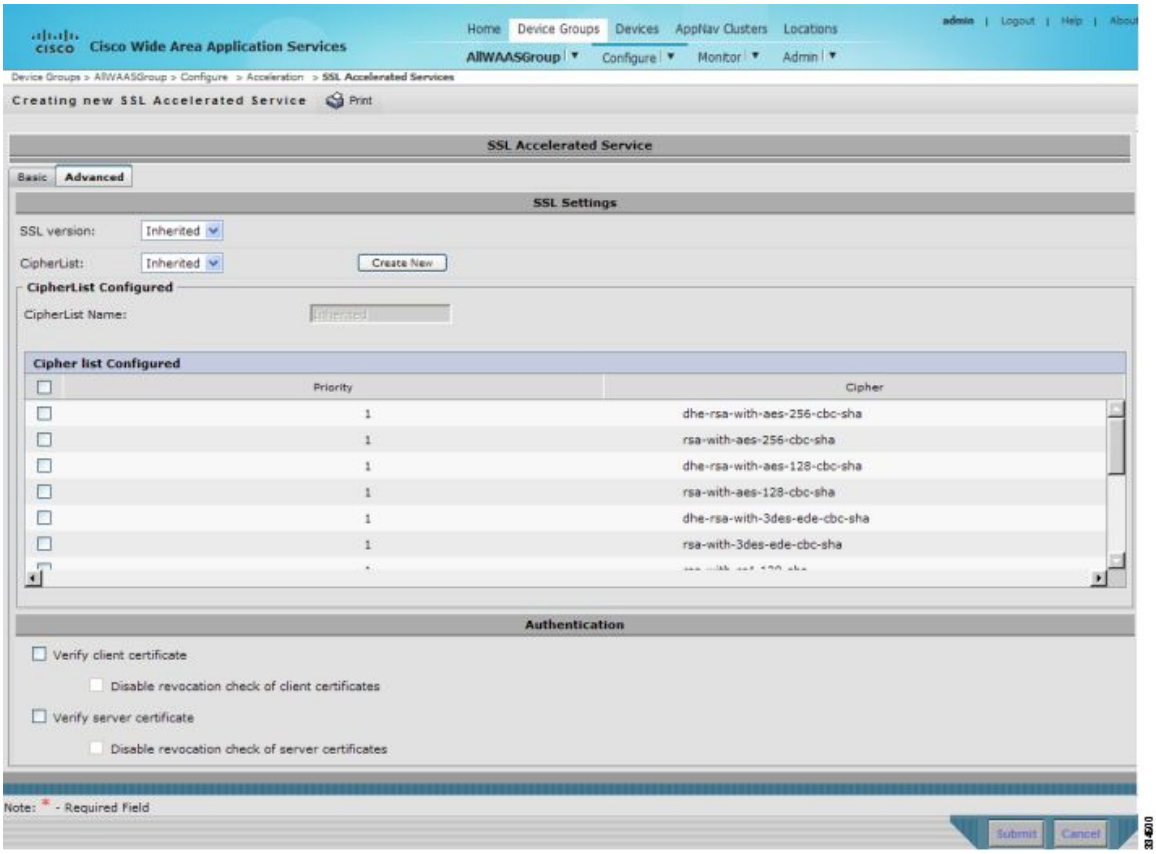
To change the service certificate or private key for multiple SSL-accelerated services, restart all the accelerated services by disabling and then re-enabling the SSL accelerator.

For service certificate and private key configuration steps, see Generating, Importing, or Exporting a Service Certificate and Private Key.

Step 11 To configure SSL parameters for the service, click the **Advanced Settings** tab.

The **SSL Accelerated Services Configuration** window, **Advanced** tab appears.

Figure 27: SSL Accelerated Services (Advanced tab) Window



a) (Optional) At the **SSL Settings** pane, from the **SSL version** drop-down list, choose the type of SSL protocol to use:

- To use the SSL protocol configured in **Global SSL Settings** window, choose **Inherited**. For more information on configuring global SSL settings, see Configuring SSL Global Settings.
- To use the SSL Version 3 protocol, choose **SSL3**.
- To use the Transport Layer Security Version 1 protocol (TLS Version 1), choose **TLS1**.
- To use both the SSL Version 3 and TLS 1 protocols, choose **All**.

b) (Optional) At the **SSL Settings** pane, from the **Cipher List** drop-down list, choose a list of cipher suites to be used for SSL acceleration between the Cisco WAE device peers, or choose Inherited to use the cipher list configured in SSL global settings. For more information, see Working with Cipher Lists.

c) (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.
- To disable OCSP client certificate revocation checking, check the **Disable revocation check for this service** check box.
- To enable verification of server certificate check, check the **Verify server certificate** check box.

- To disable OCSP server certificate revocation checking, check the **Disable revocation check for this service** check box.

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

d) After you have completed the configuration of the SSL accelerated service, click **Submit**.

Updating a Certificate or Private Key in an SSL Accelerated Service

Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **SSL Accelerated Services**.

Step 3 In the **Name** column for the specified service, click **Edit SSL Accelerated Service**.

Step 4 Choose a certificate and key pair method to either regenerate a self-signed certificate and private key or to import an updated certificate and/or key.

a) Enter the required details.
b) Depending on the chosen method, click **Generate** or **Import**.
c) Click **Submit**.

- When you update a certificate for an 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 5 In the **Name** column for the specified service, click **Edit SSL Accelerated Service** button.

Step 6 Remove the check mark for **In service**, and then click **Submit**.

Step 7 Click the **Edit SSL Accelerated Service** button in the **Name** column for the service in question for one last time.

Step 8 Enable the check mark for **In service**.

Step 9 Click **Submit**.

Configuring SSL Acceleration for SaaS Applications

Before you begin

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 Cisco data center WAAS. But for an 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 and certificate mismatch for SaaS applications.
- Cisco WAAS Version 6.4.3 and later support acceleration of two additional SaaS applications: ServiceNow and SalesForce over the SSL protocol. These are in addition to the existing applications: Microsoft Office 365 and YouTube.
- The configuration of SSL-accelerated services for SaaS applications solves the issue of namespace and certificate mismatch for SaaS applications, and ensures that these applications are optimized.

Procedure

Step 1 To create an SSL-accelerated service for a SaaS application, use Step 1 through Step 8 outlined in Using SSL Accelerated Services, on page 56.

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

Consider the following guidelines to match subject alternative names:

- 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 CIsco WAAS device.

  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.
- Most current browsers provide Server Name Indication (SNI) support. Ensure that you use a browser that supports SNI.
- The **Match Server Name Indication** option is available on devices running Cisco WAAS Version 5.3.5 and later.

Step 3 To specify the server IP address of the accelerated server, use the keyword **Any**.

Step 4 Direct all SSL traffic for SaaS applications to **port 443**.

Consider the following guidelines for directing SSL traffic for SaaS applications to port 443.

- The above configuration overrides any wildcard configuration.
- If you have configured port 443 for traffic other than SaaS applications, review and reconfigure it appropriately.

Step 5 To upload or paste a certificate and key pair, click **Import Existing Certificate Key**.

- 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.
- To identify the server domains that need to be added for optimizing SaaS applications, follow the steps described in Determining Server Domains Used by SaaS Applications .

- To ensure that the connections are optimized, you *must* create a new certificate with the missing server domain names derived from the list at regular intervals.

Step 6 To complete the configuration of the SSL-accelerated service for the SaaS application, click **Submit**.

Determining Server Domains Used by SaaS Applications

Before you begin

This section describes how determine server domains used by SaaS applications, and (optionally) how to optimize these server domains.

To view the list of server domain names that do not match the existing SSL certificate, and therefore are not optimized:

1. Check the Match Server Name Indication check box.
2. Log in to the core Cisco WAAS device.
3. Run the **sh crypto ssl services accelerated-service service-name** command.
4. 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.

Procedure

Step 1 Identify the relevant servers to be added.

Step 2 Run the **sh crypto ssl services accelerated-service** *service-name* command to see additional details regarding the count and last seen information of the server name.

Step 3 To enable SNI debugs, to view additional information regarding IP address and hostnames, run the **debug accelerator ssl sni** command.

Step 4 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, log in to the Microsoft Management Console (MMC), or OpenSSL, or other available customer tool.

- When you add the SAN to the certificate: use commas to separate domain names.
- A list of hostnames on a domain can be secured with a single certificate. For example, you can add **a.b.c.com** and **c.b.com** as ***.b.c.com**.
- For a new hostname on another domain, you must make a new entry. For example, you must add **b.c.com** as **b.c.com** or ***.c.com**.
- You can also secure hostnames on different base domains in the same certificate. For example, you can add **a.b.com** and **a.b.net**.
- Refer to the highlighted area in the example certificate below.

```
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 5 Submit the certificate to the Enterpise CA.

Step 6 Import the signed certificate from the Enterprise CA to the Trusted Root Certification Authorities store.

The Enterprise root CA must be present in the browser as trusted root CA.

Step 7 To disable the accelerated service, uncheck the In service checkbox and click **Submit**.

Step 8 Upload the new certificate and re-enable the service.

The server names vary as per the accelerated service that you have configured. Refer to the names below that need to be included in the certificate for the respective accelerated service.

Service Now

```
DNS:*.service-now.com, DNS:service-now.com, DNS:*.servicenow.com, DNS:servicenow.com,
DNS:*.cisco.com, DNS:cisco.com, DNS:*.cloudapps.cisco.com, DNS:cisco.sc.omtrdc.net,
DNS:tags.tiqcdn.com, DNS:ssl.gstatic.com, DNS:dpm.demdex.net, DNS:beacons.gcp.gvt2.com
```

SalesForce

```
DNS:ssl.gstatic.com, DNS:*.force.com, DNS:*.lightning.force.com, DNS:*.salesforce.com,
DNS:*.content.force.com, DNS:*.ap5.content.force.com, DNS:*.sfdcstatic.com,
DNS:*.demdex.net, DNS:salesforcecom.demdex.net, DNS:*.rlcdn.com, DNS:*.krxd.net,
DNS:*.partners.salesforce.com, DNS:*.everesttech.net
```

Configuring SMART-SSL Acceleration

This section contains the following topics:

About SMART-SSL Acceleration

SMART-SSL is an encryption service that enables Layer 7 application network services, such as FTP, HTTP, DNS, to optimize traffic on SSL and TLS encrypted applications. SMART-SSL enables content caching for SSL and TLS applications (HTTP object cache for HTTPS traffic) in both single-sided and dual-sided deployment.

With the evolution of cloud services, there is a critical need to provide application optimization. For Cisco WAAS Version 6.4.1 and later, SMART-SSL optimization is enabled using both single-sided and dual-sided mode.

- In a single-sided deployment, the interposing device does not require a peer device to process the SMART-SSL traffic flow. SMART-SSL traffic flows directly to the edge device without having to go through the core device.
- The dual-sided deployment uses the same configuration procedure as in SSL Accelerator V1. Therefore, the SSL accelerator service configuration is done at the core device in the data center.

  Dual-sided deployments for SMART-SSL (or SSL Accelerator V2), use TLS1.2 as the SSL version and **rsa-with-aes-256-cbc-sha** as the cipher suit.
- To configure SMART-SSL acceleration, you can use your own certificate or use the peering device's certificate. For more information, see Configuring SSL Peering Service.
- To ensure this optimization, you must to enable the SMART-SSL (SSL Accelerator v2) accelerator.

The table below provides an overview of the steps you must complete to set up and enable SMART-SSL acceleration.

Table 9: Checklist for Configuring SSL v2 Acceleration

Task	Additional Information and Instructions
1. Prepare to configure SMART-SSL acceleration.	Identifies the information that you need to gather before configuring SMART-SSL acceleration on your WAAS devices. For more information, see Preparing to Use SMART-SSL Acceleration, on page 66.

Task	Additional Information and Instructions
2. Set up to use existing Enterprise Root CA certificates.	(Optional) Describes how to create, import, and manage existing Enterprise Root certificate authority (CA) certificates. For more information, see Using an Existing Root CA Certificate, on page 68.
3. Enable SMART-SSL application optimization.	Describes how to activate the SMART-SSL acceleration feature. For more information, see Enabling and Disabling the Global Optimization Features, on page 3.
4. Set up accelerated service certificates.	Describes how to create, import, and use certificates for SMART-SSL acceleration. For more information, see Creating Single-Sided SMART-SSL Accelerated Service Certificate , on page 68.
5. Configure and enable SSL-accelerated services.	Describes how to add, configure, and enable services to be accelerated by the SMART-SSL application optimization feature. For more information, see Configuring and Managing SMART-SSL Accelerated Services on a Single-Sided Device Group, on page 69.

Preparing to Use SMART-SSL Acceleration

Before configuring SMART-SSL acceleration, consider these specifications:

- Services to be accelerated on the SMART-SSL traffic: You must create a certificate to optimize these services using their URLs or domain names, such as **www.google.com**, or ***.google.com**.
- Server IP address and port information: Optionally, if the URL or domain name cannot be used, you can specify a server IP address. If you have specified a URL, you can still specify a port.
- Public key infrastructure (PKI) certificate and private key information, including the certificate common name and CA-signing information.
- SSL versions supported: SSLv3, TLS1.0, TLS1.1, TLS1.2.

Note For SMART-SSL to work, the default SSL policy must be in place. If the policy is modified, for example, if the command **accelerate http policy** is applied for an SSL class map, the SSL accelerator starts optimizing, but the SMART-SSL accelerator does not optimize.

Supported ciphers: The following is a list of the 27 supported ciphers.

```
TLS_RSA_WITH_3DES_EDE_CBC_SHA, /* 0x000A */
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,/* 0x0016 */
TLS_RSA_WITH_AES_128_CBC_SHA,    /* 0x002F */
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, /* 0x0033 */
TLS_RSA_WITH_AES_256_CBC_SHA, /* 0x002F */
TLS_DHE_RSA_WITH_AES_256_CBC_SHA, /* 0x0039 */
TLS_RSA_WITH_AES_128_CBC_SHA256, /* 0x003C */
TLS_RSA_WITH_AES_256_CBC_SHA256, /* 0x003D */
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,/* 0x0041 */
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA, /* 0x0045 */
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, /* 0x0067 */
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, /* 0x006B */
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA, /* 0x0084 */
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA, /* 0x0088 */
TLS_RSA_WITH_SEED_CBC_SHA,   /* 0x0096 */
```

```
TLS_DHE_RSA_WITH_SEED_CBC_SHA, /* 0x009A */
TLS_RSA_WITH_AES_128_GCM_SHA256, /* 0x009C */
TLS_RSA_WITH_AES_256_GCM_SHA384, /* 0x009D */
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, /* 0x009E */
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, /* 0x009F */
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, /* 0xC012 */
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, /* 0xC013 */
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, /* 0xC014 */
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, /* 0xC027 */
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, /* 0xC028 */
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, /* 0xC02F
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 /* 0xC030 */
```

SSL compression is not supported.

Creating a Root CA Certificate

Before you begin

A root Certificate Authority (CA) certificate is a certificate issued by a trusted certificate authority and is in turn trusted by domain clients. A root CA certificate is used to sign all the certificates that will be used by the Cisco WAAS for SSL interposing during client and server SSL handshake for optimizing the applications or the URLs.

The root CA certificate must be able to accept Certificate Signing Requests (CSRs) that include subject alternative names and generate certificates that include subject alternative names.

- The subject alternative name is an extension to the X.509 protocol that allows various values to be associated with a security certificate (SSL certificate).
- Subject alternative names can include IP addresses, email addresses, universal resource identifiers (URIs), alternative common Domain Name System (DNS) names, alternatives to the distinguished name, and other information.You can install this on all machines that will be communicating with services using SSL certificates generated by this root certificate.
- If your organization already has a root CA for its internal use, you can use it instead of a new root CA. If not, use a Linux machine with openssl version of 1.0.1e or greater to create these certificates.

Procedure

Step 1 To create a new root CA certificate, use a Linux machine with an OpenSSL version of 1.0.1e or later.

Step 2 Create the root CA certificate key. This signs all issued certificates.

```
openssl genrsa -out rootCA.key.pem 2048
```

Step 3 Create the self-signed root CA certificate, with the key generated in Step 2.

```
openssl req -x509 -new -nodes -key rootCA.key -days 365 -out rootCA.crt
```

Step 4 Verify the root certificate.

Step 5 Import the certificate from the **Enterprise CA** to the **Trusted Root Certification Authorities** store in the client browser.

Step 6 Install the root CA certificate and intermediate CA certificate.

Using an Existing Root CA Certificate

If your organization already has a well-known root CA certificate, you can use it. You can also import a new CA certificate using the Cisco WAAS Central Manager GUI.

For more information, see Working with CA Certificates and Creating a Root CA Certificate.

Creating Single-Sided SMART-SSL Accelerated Service Certificate

Procedure

Step 1 To create a new encryption key pair, use OpenSSL as shown below:

```
openssl genrsa -out proxyserver.key 1024
```

Step 2 For the application to be optimized, create a Certificate Signing Request (CSR), key pair, and other needed attributes, such as **Common Name**, **Company** and **SubjAltName**.

For example, for YouTube, ensure that the **subjectAltNames** have all URLs that YouTube servers include in their certificate, which you want to optimize.

```
openssl req -new -key server.key -out server.csr
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
NGSSL Demo Certificate
X509v3 Subject Key Identifier:
65:C1:42:98:47:81:0E:04:7A:7D:83:A7:43:C9:A3:B8:1F:DB:BF:1E
X509v3 Authority Key Identifier:
keyid:8C:F6:0A:BC:E4:EB:2C:D9:6B:68:95:09:1B:B5:82:66:CE:ED:6B:77
X509v3 Subject Alternative Name:
DNS:*.google.com, DNS:*.android.com, DNS:*.appengine.google.com, DNS:*.cloud.google.com,
DNS:*.google-analytics.com, DNS:*.google.ca, DNS:*.google.cl, DNS:*.google.co.in,
DNS:*.google.co.jp, DNS:*.google.co.uk, DNS:*.google.com.ar, DNS:*.google.com.au,
DNS:*.google.com.br, DNS:*.google.com.co, DNS:*.google.com.mx, DNS:*.google.com.tr,
DNS:*.google.com.vn, DNS:*.google.de, DNS:*.google.es, DNS:*.google.fr, DNS:*.google.hu,
DNS:*.google.it, DNS:*.google.nl, DNS:*.google.pl, DNS:*.google.pt,
DNS:*.googleadapis.com, DNS:*.googleapis.cn, DNS:*.googlecommerce.com,
DNS:*.googlevideo.com, DNS:*.gstatic.cn, DNS:*.gstatic.com, DNS:*.gvt1.com,
DNS:*.gvt2.com, DNS:*.metric.gstatic.com, DNS:*.urchin.com, DNS:*.url.google.com,
DNS:*.youtube-nocookie.com, DNS:*.youtube.com, DNS:*.youtubeeducation.com,
DNS:*.ytimg.com, DNS:android.clients.google.com, DNS:android.com, DNS:g.co, DNS:goo.gl,
DNS:google-analytics.com, DNS:google.com, DNS:googlecommerce.com, DNS:urchin.com,
DNS:www.goo.gl, DNS:youtu.be, DNS:youtube.com, DNS:youtubeeducation.com
```

Alternately, to create a CSR from the CM GUI, follow the steps in Generating, Importing, or Exporting a Service Certificate and Private Key, on page 43.

Step 3 To create a new proxy server certificate, sign the above generated CSR with your existing Enterprise Root CA, or the one created above. This will generate a **.crt** or **.pem** certifcate file.

To ensure that the created accelerated service proxy certificate will be authenticated and accepted by the client browser, the CA certificate used to sign this accelerated service certificate must be present in the client browser root CA certificate store.

a) Refer to your browser's Settings or Options menu for that browser's Certificates and Import locations.
b) Import the certificate.
c) Clear the browser cache.

d) Reload the browser for the cloud application.

The browser will pick up the new certificate.

Step 4 Cisco WAAS allows importing certificates with **PKCS12** format. To generate the **PKCS12** format from the certificate file and your private key, run the **open ssl** command.

```
openssl pkcs12 -export -out server.p12 -inkey proxyserver.key -in proxyserver.crt
-certfile CACert.crt
```

Step 5 To import this certificate into the Cisco WAAS device group, run the **crypto import** EXEC command and thereafter be used in the accelerated server configuration as server-cert-key.

```
WAE# crypto import pkcs12 newcert.p12 pkcs12{disk| ftp | http | sftp | tftp}
```

Step 6 Follow these guidelines for importing the certificate:

- The CA certificate used to sign this Accelerated SSL Service (ASVC) certificate must exist in the browser root CA certificate store in order for the accelerated service proxy certificate creation to be authenticated and accepted by the browser.
- The Cisco WAAS Central Manager CA certificate repository does not include the **CN=GTE CyberTrust Global Root** certificate. You must manually import the **CN=GTE CyberTrust Global Root** certificate and then configure it from the Cisco WAAS Central Manager, or the device that will use it, to validate Microsoft Office 365 certificates.

Configuring and Managing SMART-SSL Accelerated Services on a Single-Sided Device Group

Before you begin

Consider the following prerequisites for using Cisco WAAS to optimize SMART-SSL traffic:

- Ensure that the Cisco WAAS Central Manager and Cisco WAEs are running Cisco WAAS Software Version 6.2.x or later.
- Ensure that the new device group supports single-sided acceleration. To create a device group, see Creating a Device Group in the chapter "Using Device Groups and Device Locations."
- Create an accelerated service certificate for WAN optimization.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose Device Groups > device-group-name.

Step 2 Select the device group to enable for SMART-SSL settings.

Note Add only branch devices to this group.These devices will optimize the SSL traffic as it passes through them.

Step 3 From the Cisco WAAS Central Manager menu, choose **Configure > Acceleration > Enabled Features**.

Step 4 To enable SMART SSL acceleration, at the **Accelerator Optimization** pane, check the **SSL Interposer (SSL Accelerator V2)** check box.

Step 5 To create an SSL accelerated service for the device group, choose **Acceleration > SSL Accelerated Services**.

Step 6 Click **Create**.

The **Creating New SSL Accelerated Service** window appears.

Step 7 At the **SSL Accelerated Service** pane, enter the name of your service, and check the **In service** box.

(Optional) Enter a short description for the SSL accelerated service.

Step 8 At the **Server Addresses** pane:

a) In the IP Address field, enter **Any**.
b) In the **Server Port** field, enter **443**.
c) Click **Add**.

Step 9 At the **Certificate and Private Key** pane:

a) Click **Import Existing Certificate and Optionally Private Key**.
b) Click **Upload File in PKCS#12 Format**.
c) In the **Password** field, enter the password to be used to export the certificate.
d) Use the **Browse** button to locate the certificate to be imported.
e) Click **Import** to import the certificate.

A confirmation screen appears, with the certificate information.

Step 10 To complete the configuration of the SSL-accelerated service to use single sided optimization, click **Submit**.

(Optional) Alternatively, to automate the entire process using a script, contact the Cisco Technical Assistance Center (TAC). For further information on contacting TAC, see the Cisco Support and Downloads page, Contacts/Support Cases section.

Step 11 To monitor the SMART-SSL accelerated service optimization statistics:

- To use the Cisco WAAS Central Manager, see the chapter "Monitoring Your Cisco WAAS Network."
- To use the Cisco WAAS CLI, run the **show statistics encryption-services** EXEC command.

What to do next

To configure and manage SMART-SSL accelerated services on a single-sided device group using the Cisco WAAS CLI, use these command guidelines:

Before You Begin

- Ensure that the Cisco WAAS Central Manager and Cisco WAEs are running Cisco WAAS Software Version 6.2.x or later.
- Ensure that the new device group supports single-sided acceleration. To create a device group, see Creating a Device Group in the chapter "Using Device Groups and Device Locations."
- Create an accelerated service certificate for Cisco WAN optimization.

To configure and manage SMART-SSL accelerated services on a single-sided device group using the Cisco WAAS CLI, use these command guidelines:

- To enable SMART-SSL acceleration from the Cisco WAAS CLI, run the **crypto encryption-service enable** global configuration command.
- The SSL accelerator and the SMART-SSL accelerator use the same configuration commands. However, for the SMART-SSL configuration, only a limited set of keywords are supported. The following table shows the Cisco WAAS CLI command keywords that are supported for SMART-SSL acceleration.

Table 10: Cisco WAAS CLI Command Keywords Supported for SMART-SSL Acceleration

Cisco WAAS CLI Command Mode	Keywords Supported for SMART-SSL Acceleration	Cisco WAAS CLI Command Mode	Keywords Not Supported for SMART-SSL Acceleration
(config-ssl-accelerated)	client-cert-key	(config-ssl-accelerated)	cipher-list
	client-cert-verify		client-version-rollback
	description		match
	inservice		protocol-chaining
	server-cert-key		version
	server-cert-verify		
	server-domain + port		
	configure IP + port		

Configuring Microsoft Office 365 for Cisco WAAS

This section contains the following topics:

About Microsoft Office 365 for Cisco WAAS

Microsoft Office365 supports business-critical applications such as Outlook, SharePoint, Excel and PowerPoint, and use of Microsoft Office 365 as SaaS has also increased. As enterprises move toward SaaS applications such as Microsoft Office 365, performance and user experience of these applications has also become more important.

Cisco WAAS support for Microsoft Office 365 traffic acceleration and optimization was introduced in Cisco WAAS Version 5.3.5 (for optimization between the on-premise data center and the customer branch, only). For Cisco WAAS Version 6.2.1 and later, traffic to Microsoft Office 365 is optimized until it reaches the cloud, by implementing a solution that includes:

- Enabling Cisco WAAS as SaaS over Microsoft Azure.
- Positioning Cisco WAAS as SaaS near to Microsoft Office 365 service by configuration.
- Routing and DNAT using CSR in Microsoft Azure.
- Using Cisco Intelligent WAN (Cisco IWAN) as transport.
- Detecting Microsoft Office 365 traffic using the Cisco SSL accelerator.

Checklist for Configuring Microsoft Office 365 for Cisco WAAS

The following list shows the steps needed to set up and enable Microsoft Office 365 for Cisco WAAS using the Cisco WAAS Central Manager.

1. **Prerequisites**: Before you create a Microsoft Office 365 accelerated service using the Cisco WAAS Central Manger, you must have completed the following:
   - Deployed Virtual Network in Azure
   - Deployed CSR 1000v for secure network extension and Destination Network Address Translation (DNAT)
   - Deployed Microsoft Azure on Cisco vWAAS
   - Configured Microsoft Azure route tables
   - Configured Microsoft Azure CSR
   - Registered the Microsoft Azure Cisco vWAAS device with the Cisco WAAS Central Manager
2. **Prepare to configure SSL acceleration**:

   Identify the information that you need to gather before configuring SSL acceleration on your Cisco WAAS devices.

   For more information, see Prerequisites for Configuring SSL Acceleration.
3. **Set up root CA certificates**:

   (Optional) Create, import, and manage certificate authority (CA) certificates.

   For more information, see Creating a Root CA Certificate.
4. **Enable SSL application optimization**:

   Enable the SSL acceleration feature.

   For more information, see Enabling and Disabling the Global Optimization Features and Configuring SSL Acceleration.
5. **Set up accelerated service certificates**:

   Create, import, and use certificates for Microsoft Office 365 acceleration.

   For more information, see Creating Microsoft Office 365 Accelerated Service Certificate.
6. **Configure and enable Microsoft 365 acceleration**:

   Add, configure, and enable Microsoft 365 acceleration using the Cisco WAAS Central Manager.

   For more information, see Configuring Microsoft Office 365 for Cisco WAAS.

Creating Microsoft Office 365 Accelerated Service Certificate

Procedure

Step 1 To create a new Certificate Signing Request (CSR) with the relevant server domain names of the Microsoft Office 365 application in the subject alternative names extension of the certificate, log in to the Microsoft Management Console (MMC), OpenSSL, or other available customer tool.

In the following example certificate, refer to the bolded text.

```
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.1 = *.virtualearth.net; DNS.2 = *.msocdn.com; DNS.3 = *.office365.com; DNS.4 =
*.outlook.com; DNS.5 = outlook.com; DNS.6 = *.microsoftonline.com; DNS.7 = *.res.outlook.com;
 DNS.8 = *.googleapis.com; DNS.9 = *.google-analytics.com; DNS.10 = *.google.com; DNS.11 =
 *.googleusercontent.com; DNS.12 = *.gstatic.com; DNS.13 = *.microsoftonline-p.com; DNS.14
 = *.aadcdn.microsoftonline-p.com; DNS.15 = *.aspnetcdn.com; DNS.16 = *.client.hip.live.com;
 DNS.17 = *.hip.live.com; DNS.18 = *.infra.lync.com; DNS.19 = *.linkedinlabs.com; DNS.20 =
 *.live.com; DNS.21 = *.lync.com; DNS.22 = *.microsoft.com; DNS.23 = *.microsoftonline-p.net;
 DNS.24 = *.microsoftonlineimages.com; DNS.25 = *.microsoftonlinesupport.net; DNS.26 =
*.msecnd.net; DNS.27 = *.msocdn.com; DNS.28 = *.office.net; DNS.29 = *.office365.com; DNS.30
 = *.officeapps.live.com; DNS.31 = *.officecdn.microsoft.com; DNS.32 = *.online.lync.com
DNS.33 = *.onmicrosoft.com; DNS.34 = *.sharepoint.com; DNS.35 = *.sharepointonline.com;DNS.36
 = *.telemetry.microsoft.com; DNS.37 = *.testexchangeconnectivity.com; DNS.38 =
*.vo.mscend.net; DNS.39 = *.webtrends.com; DNS.40 = *.office.com; DNS.41 =
*.portal.office.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:
```

Step 2 Submit the certificate to the Enterprise CA.

Step 3 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 4 To ensure that the created accelerated service proxy certificate will be authenticated and accepted by the client browser, the CA certificate used to sign this accelerated service certificate must be present in the client browser root CA certificate store.

a) Refer to your browser's **Settings** or **Options** menu for that browser's **Certificates** and **Import** locations.
b) Import the certificate.
c) Clear the browser cache.
d) Reload the browser for the cloud application.

The browser will pick up the new certificate.

Procedure for Configuring Microsoft Office 365 for Cisco WAAS

Procedure

Step 1 Register your Azure vWAAS device with the Cisco WAAS Central Manager. If the Cisco WAAS Central Manager is in a different network add routes for reachability.

Step 2 Create a Microsoft Office 365 accelerated service for the device group:

a) Choose **Acceleration > SSL Accelerated Services**.
b) Click **Create**.

The **Creating New SSL Accelerated Service** window appears.

Step 3 At the **SSL Accelerated Service** pane:

a) In the **Service Name** field, enter the name of the service, **o365**.
b) To enable this service, check the **In Service** check box.
c) To match subject alternative names, check the **Match Server Name Indication** check box or run the match sni command on the core WAAS device.

Consider the following guidelines to match subject alternative names:

- 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.

- 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.
- Most current browsers provide Server Name Indication (SNI) support. Ensure that you use a browser that supports SNI.
- The **Match Server Name Indication** option is available on devices running Cisco WAAS Version 5.3.5 and later.

d) (Optional) Provide a short description.

Step 4 At the Server addresses pane:

a) To specify the server IP address of the accelerated server, in the **Server Port** field, enter the keyword **Any**.
b) To direct traffic to port 443, in the **Server Port** field enter **443**.
c) Click **Add**.

Step 5 At the **Certificate and Private Key** pane:

a) Click **Import Existing Certificate and Optionally Private Key**.
b) Click **Upload File in PKCS#12 Format**.
c) In the **Password** field, enter the password to be used to export the certificate.
d) Use the **Browse** button to locate the certificate to be imported.
e) Click **Import** to import the certificate.

A confirmation screen appears, with the certificate information.

Step 6 To complete the configuration of the Microsoft Office 365, click **Submit**.

Step 7 To monitor accelerated service optimization statistics, see SSL Acceleration Charts in the chapter "Monitoring Your Cisco WAAS Network."

What to do next

To configure Microsoft Office 365 for Cisco WAAS using the Cisco WAAS CLI:

- To copy the Microsoft Office 365 certificate (**o365.pfx**) to the Cisco data center WAE and to import the certificate, run the following EXEC command:

  crypto import pkcs12 *Azure_o365.p12* **pkcs12 disk** *office365.pfx*

  Instead of importing multi-domain certificates from the device, you can use remote methods to import the certificate from servers, including the methods FTP and HTTP.

- To configure the application accelerated service in the Cisco WAE with the imported certificate, run the following SSL Accelerated Service Configuration Mode command:

  crypto ssl services accelerated-service *Azure_o365*

- To view statistics for Microsoft Office 365 acceleration, run the following EXEC command:

  show statistics connections optimized

Cisco Support for Microsoft Windows Update

This section contains the following topics:

About Cisco Support for Microsoft Windows Update

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

The Microsoft Windows OS and application updates are managed by update clients such as Microsoft Update. Microsoft Update downloads the updates via HTTP, often in combination with Background Intelligent Transfer Service (BITS) 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 Microsoft Windows 7 and Microsoft Windows 8 OS updates, via direct Internet or Windows Server Update Services (WSUS), Version 2012 and 2012 R2, 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:

- To use the Cisco WAAS Central manager to view data generated by Cisco support for Microsoft Windows Update, see Top Sites in the chapter "Monitoring Your Cisco WAAS Network." The Top Sites report provides information such as WAN response time and WAN offload bytes.
- For Cisco WAAS Version 6.1.1 and later, the cache engine access log file has two additional 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 (fl=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 (fl=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 (fl=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.

Note Cisco Support for Microsoft Windows update is enabled by default, and enabled only for specific sites. The enabled sites are updated via OTT metadata. 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, 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 and Managing the Akamai Connect License in the chapter "Configuring Cisco WAAS with Akamai Connect."

Creating a New Traffic Optimization Policy

This section contains the following topics:

Checklist for Creating an Optimization Policy

The following table provides a checklis for creating a new optimization policy.

Table 11: Checklist for Creating a New Optimization Policy

Task	Description
1. Prepare to create an optimization policy.	Complete prerequisite tasks before creating a new optimization policy on your Cisco WAAS devices. For more information, see the **Before You Begin** section of Creating an Optimization Policy, on page 79.

Task	Description
2. Create an application definition.	Identify general information about the application to be optimized, such as the application name and whether or not the Cisco WAAS Central Manager will collect statistics about this application. For more information, see Creating an Application Definition.
3. Create an optimization policy.	Determine the type of action your Cisco WAAS device or device group performs on specific application traffic. This step includes the following required tasks: • Create application class maps that enable a Cisco 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 Cisco WAAS device or device group performs on the defined traffic. For example, you can specify that Cisco WAAS apply TFO and LZ compression to all traffic for a specific application. For more information, see Creating an Optimization Policy.

Creating an Application Definition

Before you begin

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 Cisco WAAS Central Manager to collect statistics about the application. You can create up to 255 application definitions on your Cisco WAAS system.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure > Acceleration > Applications**.

The **Applications** window appears, which displays a list of all the applications on your Cisco WAAS system, and the device or device group from which it gets the settings.

Step 2 From the **Applications** window, perform the following tasks:

- To modify a definition, select an application and click the **Edit** icon in the task bar.
- To delete a definition, click the **Delete** icon in the task bar.
- Determine if the Cisco WAAS system is collecting statistics on an application.

  If the statistics are being collected for the application, the **Enable Statistics** column displays **Yes**.
- Create a new application, as described in the steps that follow.

Step 3 Create a new application:

a) Click the **Add Application** icon in the taskbar.

The **Applications** window appears.

b) In the **Name** field, enter a name for this application. Use only alphanumeric characters; the application name cannot contain spaces and special characters.

c) (Optional) In the **Comments** field, enter a comment.

The entered comment appears in the **Applications** window.

d) To allow the Cisco WAAS Central Manager to collect data for this application, check the **Enable Statistics** check box. To disable data collection for this application, uncheck the **Enable Statistics** check box.

- The Cisco 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 applications or class maps.

  However, you can use the Cisco WAAS CLI to view statistics for all the applications that have policies on a specific Cisco WAAS device. For more information, refer to the *Cisco Wide Area Application Services Command Reference*.

- Historical data for an application that has statistics collection enabled, and then disabled, and then re-enabled:

  The historical data is retained from when the statistics collection was first enabled, and when it was re-enabled, but a gap in data will exist for the period when statistics collection was disabled.

- Historical data for a deleted and then re-created application for which statistics were collected:

  An application cannot be deleted if there is an optimization policy using it. However, if you delete an application for which statistics were collected, 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.

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

e) Click **OK**.

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

Creating an Optimization Policy

Before you begin

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

- Review the list of optimization policies on your CIsco 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 Cisco 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 Cisco WAAS devices.
- After you create an application definition, create an optimization policy that determines the action a Cisco WAAS device takes on the specified traffic.

  Example:

  - You create an optimization policy that directs a Cisco WAAS device to 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 Cisco 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.

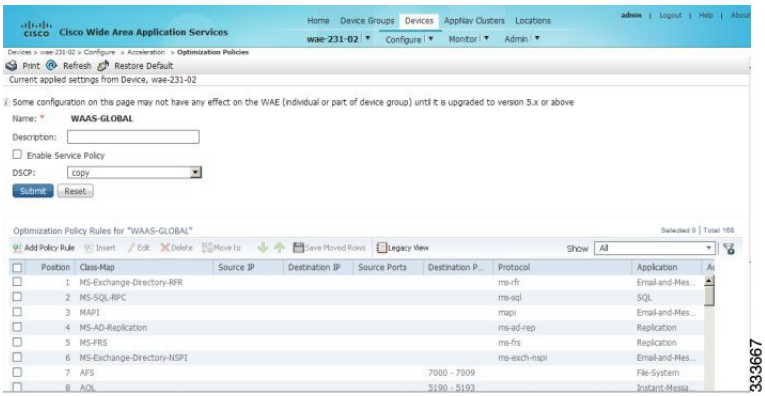
Procedure

Step 1 From the Cisco 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. This window displays information about all the optimization policies that reside on the selected device or device group, as well as the position of each policy.

Figure 28: Optimization Policies Window



Consider the following guidelines for configuring optimization policies:

- The position of each policy determines the order in which Cisco 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.
- The **Optimization Policies** window also displays the class map, source and destination IP addresses, source and destination ports, protocol, application, action, and accelerates assigned to each policy.
- If there are Cisco WAAS Version 4.x devices, click the **Legacy View** taskbar icon to view the policies as they appear in a Cisco WAAS Version 4.x device.

- All new devices, or devices that been configured with restore factory default settings, have their own polices and class maps. These devices that are not assigned to any device group within two data feeds continue to have their own policies, even after being registered with the Cisco WAAS Central Manager.
  - After these devices are assigned to device groups, the **Force Device Group Settings** icon appears in the **Optimization Policies** window in device group level. To correct this, use the **Force Group Settings** to ensure that all devices in the specified group have the same configuration.
  - For more information on **Force Group Settings**, see Procedure for Forcing Device Group Settings in the chapter "Using Device Groups and Device Locations."

At the **Optimization Policies** window, you can perform the following tasks:

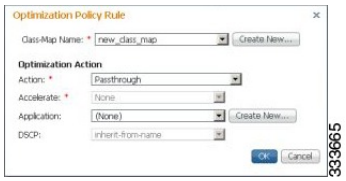
- Configure a description.
- Configure the **Enable Service Policy** setting.
- Configure the **DSCP** setting. This **DSCP setting** field configures DSCP settings at the device or device group level.

  The device uses this policy setting to determine what optimizations are performed only if the **Enable Service Policy** is set.
- To delete one or more optimization policies, select the policies to be deleted, and click the **Delete** icon.
- To modify a policy, check the policy and click the **Edit** icon.
- To restore predefined policies and class maps, see **Restoring Optimization Policies and Class Maps**.
- Create an optimization policy, as described in the following steps.

Step 3 To create a new optimization policy, click the **Add Policy Rule** icon in the taskbar.

The **Optimization Policy Rule** pop-up window appears.

Figure 29: Add Optimization Policy Rule Window



Step 4 From the **Class-Map Name** drop-down list, choose an existing class map for this policy, or click **Create New** to create a new class map for this policy. For more information, see Creating an Optimization Class Map.

Step 5 From the **Action** drop-down list, choose the action that your Cisco WAAS device should take on the defined traffic. The following table describes each action.

For a Cisco 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: Class Map Action Descriptions

Class Map Action	Description
Passthrough	Prevents the Cisco 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 different TFO techniques to matching traffic. TFO techniques include BIC-TCP, window size maximization and scaling, and selective acknowledgment. For more information on the TFO feature, see Transport Flow Optimization in the chapter "Introduction to Cisco 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.
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.

Step 6 Consider the following guidelines for class map actions:

- For a Cisco WAAS Express device, the following subset of actions is available: **Passthrough**, **TFO Only**, **TFO with LZ**, **TFO with DRE**, and **TFO with DRE and LZ**.
- 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).
- When configuring optimization policies on a device group:
  - If the device group contains devices running a Cisco WAAS version earlier than 4.4.1 and you are configuring an action that includes **Unidirectional** or **Adaptive** caching, the caching mode is converted to **Bidirectional**.

- When devices running a Cisco WAAS version earlier than 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 both of these 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 7 From the **Accelerate** drop-down list, choose one of the following additional acceleration actions that your Cisco 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 Adapter**: Accelerate using the SMB Accelerators.
- **HTTP Adapter**: Accelerate using the HTTP Accelerator.
- **MAPI Adapter**: Accelerate using the MAPI Accelerator.
- **ICA Adapter**: Accelerate using the ICA Accelerator.
- **For a Cisco WAAS Express device**, HTTP Express is available as an accelerator.

Step 8 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 Cisco WAAS system.
- To create an application, click **New Application**.
  - Specify the application name.
  - Enable statistics collection.
  - To save the new application and return to the **Optimization Policy** window, click **OK**.

    The new application is automatically assigned to this device or device group.

Step 9 (Optional) From the **DSCP Marking** drop-down list, choose one of the following:

- To copy the DSCP value from the incoming packet and use it for the outgoing packet, choose copy.
- To use the DSCP value defined at the application or global level, choose inherit-from-name.
- Consider the following guidelines for using DSCP:
  - DSCP is the combination of IP Precedence and Type of Service (ToS) fields. 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. For more information, see RFC 2474.
  - DSCP marking does not apply to pass-through traffic.
  - In a Cisco 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. Or, you can use copy, as described above.

Step 10 Click **OK**.

The new policy appears in the **Optimization Policies** window.

Creating an Optimization Class Map

Before you begin

You can create an optimization class map for an optimization policy in two ways:

- In the device context, choose **Configure > Acceleration > Optimization Class-Map**, and then click the **Add Class-Map** taskbar icon.

  The **Optimization Class-Map** pane is displayed.

- 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.

Procedure

Step 1 Enter a name for this application class map.

Consider the following guidelines:

- The name cannot contain spaces or special characters.
- 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.
- For Cisco 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.

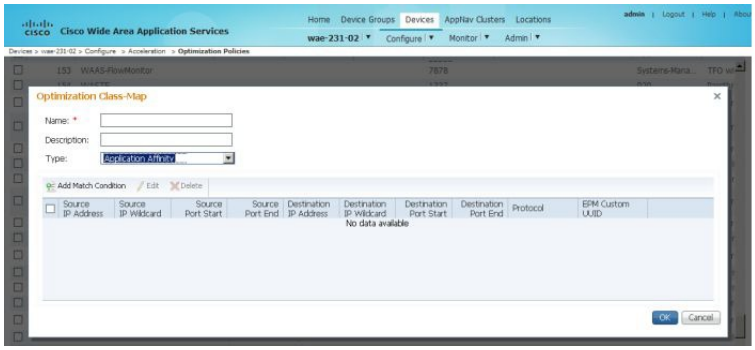
Step 3 From the **Type** drop-down list, choose the class map type.

- To match specific TCP traffic, choose **Application Affinity**.
- To match all TCP traffic choose **Any TCP Traffic**.

Step 4 After you have chosen the class map type, enter the match conditions. Click the **Add Match Condition** icon.

The **Adding a New Match Condition** Window appears.

Figure 30: Adding a New Match Condition Window



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

Step 5 To create a condition for a specific type of traffic, enter a value in a **Destination** or **Source** field.

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.

Consider the following guidelines for creating conditions:

- To specify a range of IP addresses, enter a wildcard subnet mask in either the **Destination IP Wildcard** field 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, from the **Protocol** drop-down list, choose the corresponding application identifier.

  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.
- 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 To save the class map, click **OK**.

Managing Application Acceleration

This section contains the following topics:

Modifying the Accelerator Load Indicator and CPU Load-Monitoring Threshold

Before you begin

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.
- 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 cleared *only when* the overload condition does not reappear in the next 2-minute-interval poll.

Procedure

Step 1 From the Cisco 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** and **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** and **120**. The default value is **10**.

Step 10 Click **Submit**.

If the device group is running the Cisco WAAS Version 6.x, 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** and **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** and **120**. The default value is **10**.

Step 20 Click **Submit**.

Viewing a List of Applications

Procedure

Step 1 From the Cisco 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 Cisco WAAS Version 4.x devices, click the **Legacy View** taskbar icon to view the policies as they appear in a Cisco 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

Procedure

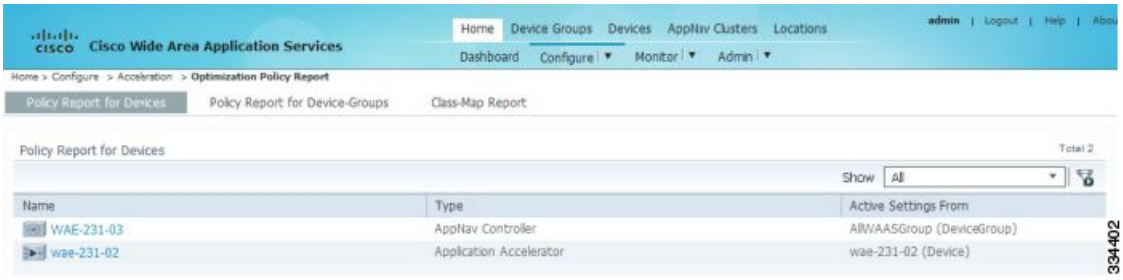
Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **Acceleration** > **Optimization Policy Report**.

The **Policy Report for Devices** tab appears.

Consider the following guidelines for viewing a policy report:

- The policy report lists each device (or device group) and the overall policy count on the device (or device group) referencing this application.
- The policy report 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 31: Optimization Policy Report



Step 2 To view the number of devices per device group and the number of active policies in the device group, click the **Policy Report for Device-Groups** tab.

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

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **Acceleration** > **Optimization Policy Report**.

The **Policy Report for Devices** tab appears.

Step 2 To view a report of the devices and device groups on which the class map is configured, click the **Class-Map Report** tab.

Step 3 To see the devices or device groups on which the class maps reside, select the class map and click the **View** icon.

Restoring Optimization Policies and Class Maps

Before you begin

The Cisco WAAS system allows you to restore the predefined policies and class maps that shipped with the Cisco 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 Cisco WAAS device handles application traffic, you can override your changes by restoring the predefined policy settings.

Procedure

Step 1 From the Cisco 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 To restore over 150 policies and class maps that shipped with the Cisco WAAS software, and to remove any new policies that were created on the system, click the **Restore Default** taskbar icon. If a predefined policy has been changed, these changes are lost and the original settings are restored.

Monitoring Applications and Class Maps

Before you begin

After you create an optimization policy, monitor the associated application to verify that your Cisco WAAS system is handling the application traffic as expected.

Before you monitor an application, you must have enabled statistics collection for that application, as described in the Creating an Application Definition.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **Acceleration** > **Monitor Classmaps**.

Step 2 Select the class map on which to enable statistics and then click **Enable**.

Consider the following guidelines for monitoring applications and class maps:

- The Cisco WAAS Central Manager GUI can display statistics for up to 25 applications and 25 class maps.
  - To monitor a specific application, run the **TCP Summary report**. For more information, see the TCP Summary Report in the chapter "Monitoring Your Cisco WAAS Network."
  - If you try to display more than 25 statistics for either applications or class maps, an error message is displayed.
- To view statistics for all applications that have policies on a specific Cisco WAAS device, use the Cisco WAAS CLI. For more information, see the *Cisco Wide Area Application Services Command Reference*.

Step 3 To configure Cisco WAAS charts to display Class Map data:

a) Click the chart **Edit** icon.

b) Choose the **Classifier** series.

This configuration option applies to most Cisco WAAS charts.

Defining Default DSCP Marking Values

Before you begin

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 Cisco WAAS. DSCP is the combination of **IP Precedence** and **Type of Service (ToS)** fields.
- For more information, see RFC 2474.

These attributes can be defined at the following levels:

- **Global**: 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**: 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.

Procedure

Step 1 From the Cisco 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 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 To save the settings, click **OK**.

Modifying the Position of an Optimization Policy

Before you begin

Considering the following configuration guidelines for optimization policy positions:

- Each optimization policy has an assigned position that determines the order in which a Cisco WAAS device refers to the policy in an attempt to classify traffic.

For example, when a Cisco 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 Cisco WAAS device moves on to the next policy in the list.

- Consider the position of policies that pass through traffic as 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 Cisco WAAS system unoptimized.

  For this reason, ensure that your policies do not have overlapping matching conditions, and monitor the applications you create to make sure that WAAS is handling the traffic as expected.

- For more information on monitoring applications, see the chapter Monitoring Your Cisco WAAS Network

  .

Procedure

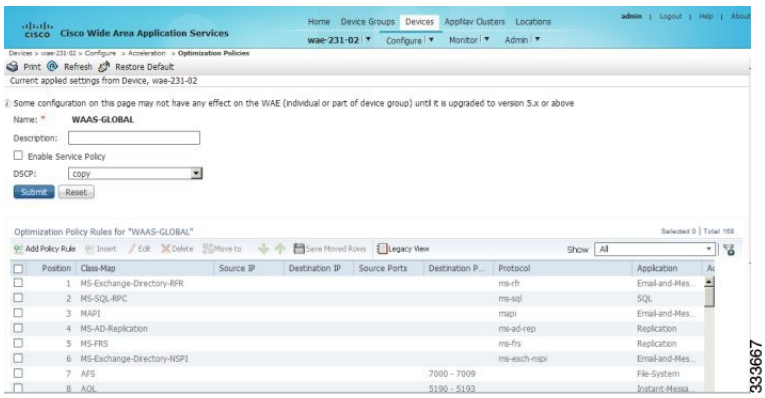
Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

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

The **Optimization Policies** window appears.

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

Figure 32: Optimization Policies Window



Step 3 To modify the position of the optimization policy, use one of the following methods, and then click the **Save Moved Rows** icon:

- Select the policy you want to move, and then 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 then, to specify the new position, click **Move To**.
- Select the policy, and then drag and drop it into the new position.

Step 4 To save the new policy position(s), click **Save Moved Rows**.

Step 5 (Optional) To create a new optimization policy at a particular position:

a) Select the policy *above* the location.

b) Click **Insert**.

Step 6 If a device goes through all the policies in the list without making a match, the Cisco WAAS device passes the traffic through unoptimized.

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

Step 7 To save changes, click the **Save Moved Rows**.

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

a) Select the policy you want to delete.

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

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

Step 9 If you determine that a new policy is needed, click the **Add Policy** taskbar icon to create the policy.

For more information, see Creating an Optimization Policy.

Modifying the Acceleration TCP Settings

Before you begin

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

- Cisco WAAS automatically configures the settings only under the following circumstances:
  - When you first install the Cisco WAE device in your network.
  - When you run the **restore factory-default** CLI command on the Cisco WAAS device.

    For more information about this command, see the *Cisco Wide Area Application Services Command Reference*.

- The Cisco WAAS system automatically adjusts the maximum segment size (MSS) to match the advertised MSS of the client or server for each connection. The Cisco WAAS system uses the lower of 1432 or the MSS value advertised by the client or server.
- If your Cisco WAAS network has high BDP links, you may need to adjust the default buffer settings automatically configured for your WAE device. For more information, see Modifying the TCP Adaptive Buffering Settings.
- If you want to adjust the default TCP adaptive buffering settings for your Cisco WAE device, see Modifying the TCP Adaptive Buffering Settings.

Procedure

Step 1 From the Cisco 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 Cisco WAE device or group to disconnect the TCP connection from 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.
- To use the CLI to configure TCP keepalives:
  - To configure TCP keepalives, run the **tfo tcp keepalive** global configuration command.
  - To configure TCP acceleration settings, run 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**
    - **tfo tcp original-send-buffer**
  - To show the TCP buffer sizes, run the **show tfo tcp** EXEC command.

Step 4 Modify the TCP acceleration settings, as needed. See the following table for a description of these settings.

For information on how to calculate these settings for high BDP links, see Modifying the TCP Adaptive Buffering Settings.

Table 13: TCP Settings

TCP Setting	Description
Optimized Side	

TCP Setting	Description
Maximum Segment Size	Maximum packet size allowed between a Cisco WAAS device and other Cisco 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 Cisco WAAS device to other Cisco 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 Cisco 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 Cisco WAAS device. The default is 1432 bytes.
Send Buffer Size	Allowed TCP sending buffers size (in kilobytes) for TCP packets sent from a Cisco 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, see Modifying the TCP Adaptive Buffering Settings.

Step 6 Consider the following guideliens for segment sizes and configuring jumbo MTU settings:

- 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, see Configuring a Jumbo MTU in the chapter "Configuring Network Settings."

Modifying the TCP Adaptive Buffering Settings

Before you begin

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

Procedure

Step 1 From the Cisco 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, run 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, run the no tfo tcp adaptive-buffer-sizing enable global configuration command.

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

What to do next

Calculating the TCP Buffers for High BDP Links:

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

- Cisco WAE-512: Default BDP is 32 KB
- Cisco WAE-612: Default BDP is 512 KB
- Cisco WAE-674: Default BDP is 2048 KB
- Cisco WAE-7326: Default BDP is 2048 KB
- Cisco WAE-7341: Default BDP is 2048 KB
- Cisco WAE-7371: Default BDP is 2048 KB
- All Cisco WAVE platforms: Default BDP is 2048 KB

Consider the following operating guidelines for BDP:

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

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

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

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

- If the calculated **MaxBDP** is greater than the **DefaultBDP** for your Cisco WAE model, modify the **Acceleration TCP** to accommodate that calculated BDP.
- After you calculate the size of the **MaxBDP**, enter a value that is equal to or greater than twice the **MaxBDP** in the **Send Buffer Size** and **Receive Buffer Size** fields for the optimized connection in 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 Cisco WAAS system to dynamically vary the buffer sizes.