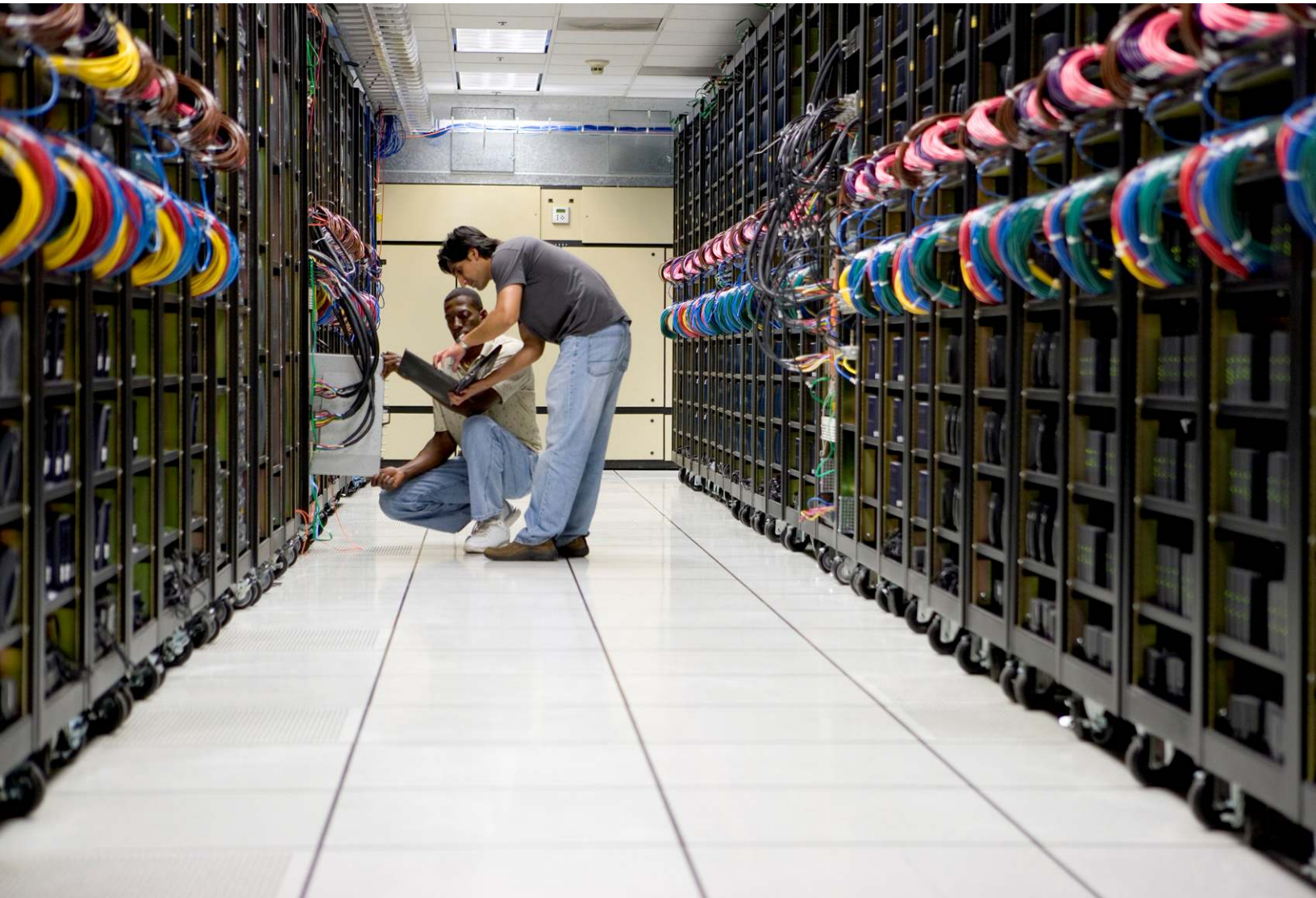
Cisco Wide Area Application Services SSL Application Optimizer

Deployment Guide



Contents

Overview

Cisco® Wide Area Application Services (WAAS) is a comprehensive WAN optimization and application acceleration solution that is a key component of Cisco Borderless Networks and Data center/Virtualization architectures. Cisco WAAS accelerates applications and data over the WAN, optimizes bandwidth, empowers cloud computing, and provides local hosting of branch-office IT services - all with industry-leading network integration. Cisco WAAS allows IT organizations to centralize applications and storage while maintaining productivity for branch-office and mobile users.

Cisco WAAS supports Secure Sockets Layer (SSL) acceleration. Among the several cryptographic protocols used for encryption, one of the most important is SSL Version 3 (SSLv3), also known as Transport Layer Security Version 1 (TLSv1). SSL provides data encryption, server authentication, message integrity, and optionally, client authentication. With SSL, each certificate is signed either by a trusted third-party certificate authority (CA), or root CA, such as VeriSign, or by an internal enterprise authority, or enterprise CA, such as Microsoft Active Directory Certificate Authority. The clients and servers must trust these authorities to accept their signed certificates.

SSL and TLS secured applications represent a growing proportion of traffic traversing the WAN links today. This encrypted secure traffic cannot be accelerated natively by Cisco WAAS data redundancy elimination (DRE) because the encryption process generates an ever-changing stream of data, making it inherently nonredundant. Even without its new specific SSL acceleration feature, Cisco WAAS could provide some generic optimization with its transport flow optimization (TFO) feature. Full SSL optimization requires termination of the SSL session, decryption of the traffic to apply Cisco WAAS DRE or Lempel-Ziv (LZ) compression techniques to the data, reencryption of the traffic for transport over the WAN using Cisco WAAS TFO, and then reversal of the process before delivery of the original encrypted traffic to the destination host.

Cisco WAAS provides SSL optimization capabilities that integrate easily with existing data center key management and trust models and can be used by both WAN optimization and application acceleration components. Private keys and certificates are stored in a secure vault on the Cisco WAAS Central Manager. The private keys and certificates are distributed in a secure manner to the Cisco WAAS devices in the data center and stored in a secure vault, maintaining the trust boundaries of server private keys. Cisco WAAS also supports hostname and domain name in the SSL accelerated service configuration to simplify deployment of SSL optimization services for cloud-based software-as-a-service (SaaS) providers.

This document provides guidelines and best practices for the configuration, management, and support of the Cisco WAAS SSL Application Optimizer solution. The Cisco WAAS SSL Application Optimizer can be used to accelerate any web application that uses SSLv3 or TLSv1.

Prerequisites

The following prerequisites are required to deploy the Cisco WAAS SSL Application Optimizer:

- Experience with basic networking and troubleshooting
- Experience installing the Cisco WAAS product families
- Experience with SSL certificates and public key infrastructure (PKI)
- Working knowledge of Cisco IOS® Software

Hardware Platform Considerations

Cisco WAAS SSL acceleration is supported on all Cisco Wide Area Application Engine (WAE) and Wide Area Virtualization Engine (WAVE) platforms running Cisco WAAS Software Version 4.1.3 or later. An Enterprise license is also required to enable the Cisco WAAS SSL Application Optimizer services.

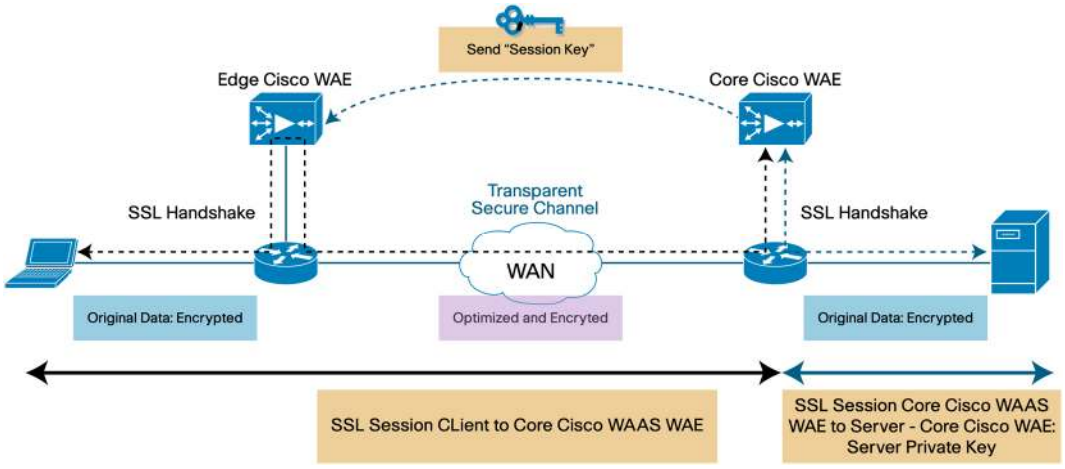
Solution Description

Cisco WAAS is an industry-leading, comprehensive WAN optimization and application acceleration solution. It now includes SSL optimization features that integrate transparently into the existing PKI trust model in customer deployments and can be easily deployed without compromising the existing data center key management security.

With Cisco WAAS, the SSL trusted model is maintained in the data center. Server private keys are stored securely on the core Cisco WAE and WAAS Central Manager and never leave the security of the data center. The temporary SSL session keys are distributed from the secure core Cisco WAEs to the edge Cisco WAEs over a secure HTTPS connection between an edge Cisco WAE and a core Cisco WAE. In addition, the Cisco WAAS SSL Application Optimizer operates in a transparent mode that does not require any changes to either the client or the server participating in the SSL connection. Figure 1 shows how Cisco WAAS SSL optimization integrates transparently into existing application key exchanges and preserves the trust boundaries of server private keys.

- During the initial client SSL handshake, the core Cisco WAE in the data center participates in the conversation. The connection between the Cisco WAEs is established securely using the Cisco WAE device certificates, and the Cisco WAEs cross-authenticate each other.
- After the client SSL handshake is complete and the data center Cisco WAE has the session key, the data center Cisco WAE transmits the session key (which is temporary) over its secure link to the edge Cisco WAE so that the edge Cisco WAE can start decrypting the client transmissions and apply DRE.
- The optimized traffic is then reencrypted using the Cisco WAE peer session key and transmitted, in-band, over the current connection, maintaining full transparency, to the core Cisco WAE in the data center.
- The core Cisco WAE then decrypts the optimized traffic, reassembles the original messages, and reencrypts the traffic using a separate session key negotiated between the server and the data center Cisco WAE.
- If the back-end SSL server requests that the client submit an SSL certificate, the core Cisco WAE requests one from the client. The core Cisco WAE authenticates the client by verifying the SSL certificate using a trusted CA or an Online Certificate Status Protocol (OCSP) responder.

Figure 1. Cisco WAAS SSL Optimization



Information Collection

You must collect some basic information about the SSL services running in the customer environment before applying Cisco WAAS SSL acceleration. Study the customer environment to gather information about the SSL application type to be accelerated before implementing proof-of-concept testing or deployment. The minimum basic information required prior to SSL accelerated service configuration is listed in Table 1.

Table 1. Minimum Information Required for SSL Acceleration

Information	Requirement
Server hostname, IP address or domain name, and port number	Mandatory
SSL server certificate and private key (or collect information about alternate certificates)	Mandatory
Certificate chain if the back-end SSL server is set up to send a certificate chain instead of the server certificate alone	Important
HTTPS proxy server port number if clients in the branch office use an HTTPS proxy server in the data center	Important
CA server certificate if a private root CA server is used	Optional
Determination of whether client certificate authentication is required for SSL negotiation	Important
OCSP responder URL if an OCSP responder is in use	Optional
SSL version supported by the SSL server	Optional
SSL cipher suites supported by the SSL server	Optional

SSL Accelerated Service Configuration

The SSL accelerator is similar to other application accelerator services running on Cisco WAAS devices. It is enabled by default on all Cisco WAE devices. The SSL accelerator requires the server private key and SSL server certificate to participate in the SSL session and obtain the session key required for encrypting and decrypting traffic. A basic SSL accelerated service configuration requires two additional configuration steps, summarized in Table 2. Please follow SSL Application Optimizer best practices when configuring SSL accelerated services.

Table 2. Configuration Steps

Step	Configuration Task	Device to Which Step Applies
Step 1	Initialize and open the Cisco WAAS Central Manager secure store.	Cisco WAAS Central Manager
Step 2	Create an SSL accelerated service on the core Cisco WAE: • Add the server hostname, IP address or domain name, and port information. • Add the server certificate and private key data. For domain name add domain wildcard certificate and private key data. • Enable service.	Core Cisco WAAS WAE

The Cisco WAAS Central Manager secure store must be initialized and then opened to allow it to store the SSL server private data and certificates before you configure an SSL accelerated service. Although initialization is a one-time configuration activity, the Cisco WAAS Central Manager secure store must be reopened whenever the Cisco WAAS Central Manager is reloaded. The SSL accelerated service can then be configured on core Cisco WAAS devices so that they can identify SSL connections that should be accelerated by the Cisco WAAS SSL Application Optimizer.

SSL Application Optimizer Best Practices for SSL Accelerated Service Configuration

We recommend the following set of guidelines for configuring SSL accelerated service in your network:

1. You should apply the SSL accelerated service configuration only to the Data Center or core Cisco WAE devices that are closest to the SSL servers to be accelerated.
2. Configuring server IP address is preferred when the SSL server IP address is known in advance and is not subject to change. This option has the lowest processing latency because no Domain Name System (DNS) lookup is required to accelerate SSL connections.
3. Server hostname, or fully qualified domain name (FQDN), should be second preference when there are a large number of SSL servers or the server IP address is subject to frequent changes. This option requires the WAE to perform DNS resolution to map the configured hostname to one or more IP addresses. We recommend that you configure a local DNS server for low DNS lookup latency. The WAE performs a DNS lookup every 10 minutes to refresh the list of IP addresses mapping to the configured server hostname.

4. The server IP address can also accept “any” option that is a wildcard IP address entry that enables SSL acceleration for all IP addresses for the configured TCP port. This option is provided for a proof-of-concept use case and should not be used in production or pilot production networks.
5. You should consider the server domain option (for example, *.webex.com) when configuring SSL accelerated service for cloud-based SaaS applications. The WAE performs a reverse DNS lookup on the IP address of the incoming SSL connection requests to match the results against the configured domain name.
6. The SSL accelerated service can use either the original SSL server certificate or a self-signed wildcard domain certificate or an Enterprise CA signed wildcard certificate. The Common Name in the SSL Certificate Common should match the hostname (FQDN) or it should match the wildcard domain name (for example, *.webex.com).
7. If a self-signed certificate is used, the browser normally throws a popup warning saying that the certificate is self-signed. To avoid the popup, use Active Directory’s Group Policy Option (GPO) to publish the certificate as “Trusted People”.
8. If an Enterprise CA signed certificate is used, there is no need to push the enterprise CA signed certificate through GPO to end clients because the Enterprise CA is typically already installed as a trusted authority in certificate stores. If there is no Enterprise CA and Enterprise is creating one, then you can use GPO to push the CA certificate as a “Trusted Root Certification Authority” or “Trusted Intermediate Certificate Authority” as appropriate to end clients.

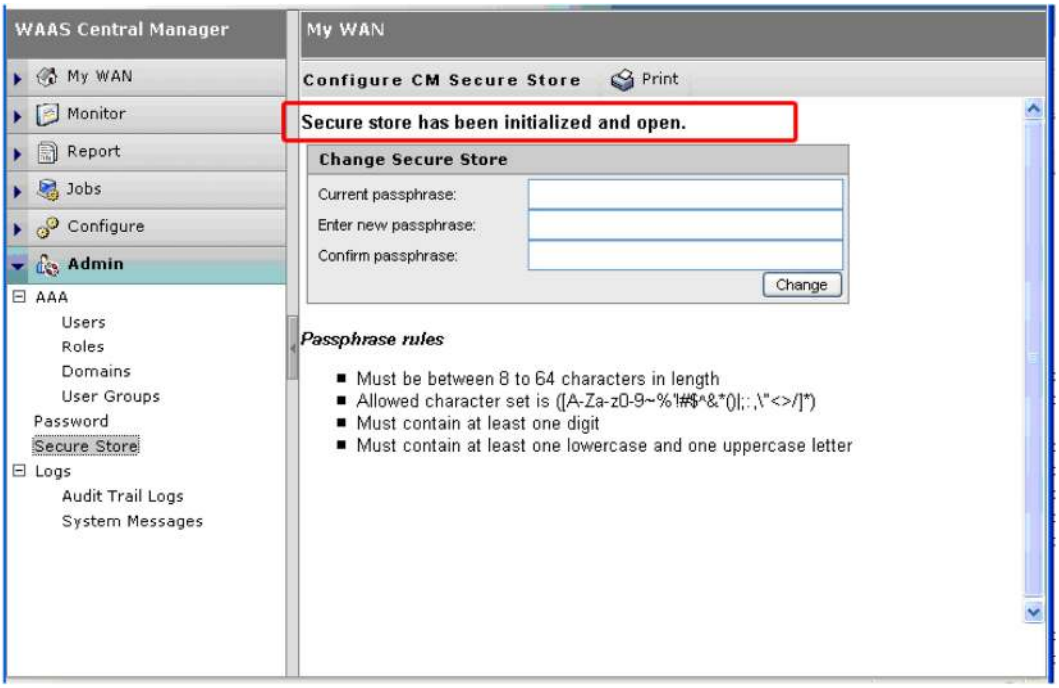
Deployment Details

Enable Cisco WAAS Central Manager Secure Store

The Cisco WAAS Central Manager is used to securely store the certificates and private keys associated with SSL accelerator services configured on the core Cisco WAE appliances. The storage location for these keys and certificates on the Cisco WAAS Central Manager is called the CM Secure Store. Before enabling SSL acceleration on any Cisco WAAS appliance, this secure store needs to be initialized and open.

To initialize and open the CM Secure Store using the Cisco WAAS Central Manager GUI, go to the **Cisco WAAS Central Manager homepage**. On the homepage, from the navigation pane, choose **Admin > Secure Store** and enter the passphrase to initialize and open the CM Secure Store for the first time. Each time the Cisco WAAS Central Manager is rebooted, the CM Secure Store must be reopened by entering the same passphrase that was entered when the CM Secure Store was initialized. Figure 2 shows a CM Secure Store initialized and in an open state.

Figure 2. Cisco WAAS CM Secure Store



The Cisco WAAS Central Manager GUI process just described can also be achieved using the device command-line interface (CLI) by issuing the commands shown here:

CLI Equivalent

```
CM# cms secure-store init
Stopping cms.
*****************************************************************
* 1) Must be between 8 to 64 characters in length               *
* 2) Allowed character set is ([A-Za-z0-9~%'!#$^&*()|;:,"<>/]*)   *
* 3) Must contain at least one digit                            *
* 4) Must contain at least one lowercase and one uppercase letter *
*****************************************************************
enter pass-phrase:
confirm pass-phrase:
Successfully migrated Cifs preposition password
Successfully migrated key store
***** WARNING : REBOOTING CM REQUIRES RE-OPENING SECURE STORE MANUALLY. AFTER
REBOOT, DISK ENCRYPTION AND CIFS PREPOSITION FEATURES ON REMOTE WAE(S) WILL NOT
OPERATE PROPERLY UNTIL USER RE-OPENS SECURE STORE ON CM BY INPUTTING THE PASSPHRASE
*****
successfully initialized and opened secure-store.
Starting cms.
WAAS-CM# show cms secure-store
secure-store is initialized and open.
CM#
```

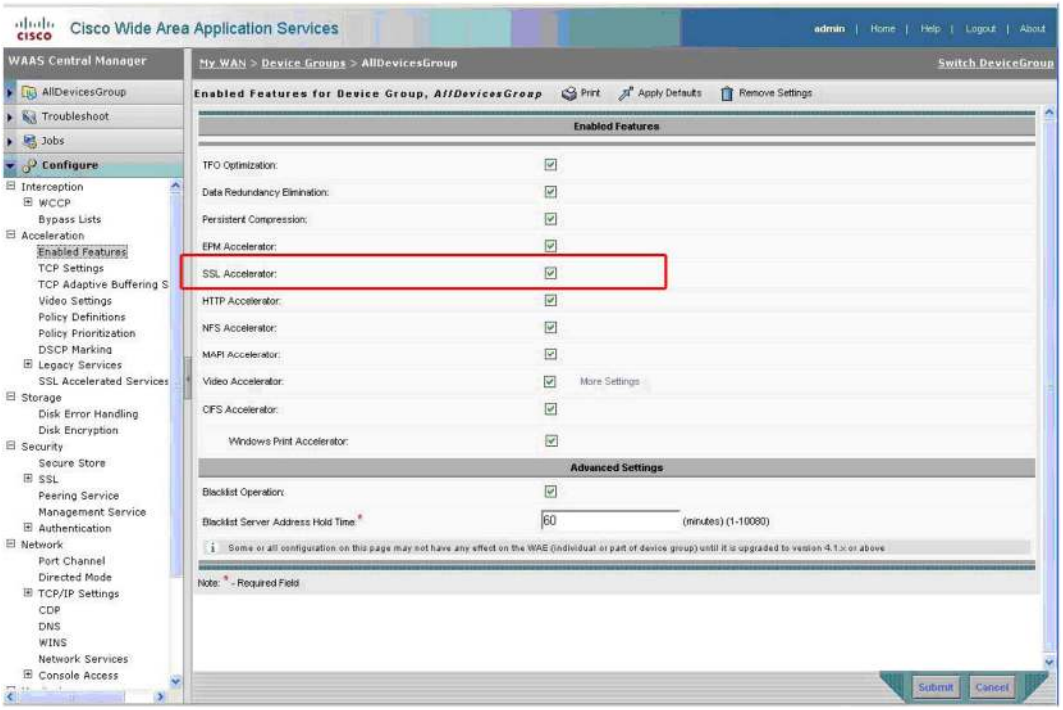
After opening the CM Secure Store on the Cisco WAAS Central Manager, verify the status of the secure store by issuing the CLI command **show cms secure-store**:

```
CM# show cms secure-store
secure-store is initialized, enter pass-phrase to open store.
WAAS-CM# cms secure-store open
enter current pass-phrase:
Successfully migrated key store
***** WARNING : REBOOTING CM REQUIRES RE-OPENING SECURE STORE MANUALLY. AFTER
REBOOT, DISK ENCRYPTION AND CIFS PREPOSITION FEATURES ON REMOTE WAE(S) WILL NOT
OPERATE PROPERLY UNTIL USER RE-OPENS SECURE STORE ON CM BY INPUTTING THE PASSPHRASE
*****
successfully opened secure-store
CM# show cms secure-store
secure-store is initialized and open.
CM#
```

Verify the Status of SSL Accelerator Services

The SSL accelerator is enabled by default on all Cisco WAAS WAE devices. The SSL accelerator must be enabled and running to accelerate SSL traffic passing through the Cisco WAAS WAE devices. If the SSL accelerator is not enabled on a Cisco WAE device, use the Cisco WAAS Central Manager GUI to enable it. Select the Cisco WAE from the **My WAN/Managed Devices** page; then from the navigation pane choose **Configure > Acceleration > Enabled Features > SSL Accelerator**. Select the **Enable** check box and then click **Submit**. Figure 3 shows how to enable SSL accelerator service on a Cisco WAE appliance through the Cisco WAAS Central Manager GUI.

Figure 3. Enabling SSL Accelerator Service on a Cisco WAE Appliance



Note: The Cisco WAAS SSL accelerator requires an Enterprise license to be installed before it can run. Verify that the Cisco WAAS appliance has the Enterprise license applied before enabling the SSL accelerator.

You can check the license information from the device CLI by issuing the following command:

```
WAE# show license
License Name   Status      Activation Date Activated By
-------------- ----------- -------------- --------------
Enterprise     active      02/25/2009      admin
Video          active      02/25/2009      admin
Virtual-Blade  active      02/25/2009      admin
WAE#
```

The Cisco WAAS Central Manager GUI process just described can also be achieved using the device CLI by issuing the command shown here:

CLI Equivalent

```
WAE(config)# accelerator ssl enable
Enabled ssl accelerator
WAE(config)#
```

After enabling the SSL accelerator on the Cisco WAE, verify the status by issuing the CLI command **show accelerator ssl**. The SSL accelerator should be reported as **Enabled** and **Running**.

```
WAE# show accelerator ssl
Accelerator     Licensed        Config State    Operational State
-----------     --------        ------------    -----------------
ssl             Yes             Enabled         Running
SSL:
   Policy Engine Config Item            Value
   -------------------------            -----
   State                                Registered
   Default Action                       Use Policy
   Connection Limit                     300
   Effective Limit                      300
   Keepalive timeout                    5.0 seconds
WAE#
```

Configure SSL Accelerated Service on the Core Cisco WAE Devices in the Data Center

SSL accelerated service configuration is required on the core Cisco WAAS WAE appliance to apply the full set of optimizations, DRE, LZ compression, and TFO to the SSL traffic. The SSL accelerated service terminates the SSL session on the core Cisco WAE and performs encryption and decryption of SSL traffic to apply or remove DRE and LZ compression from the data traversing the WAN.

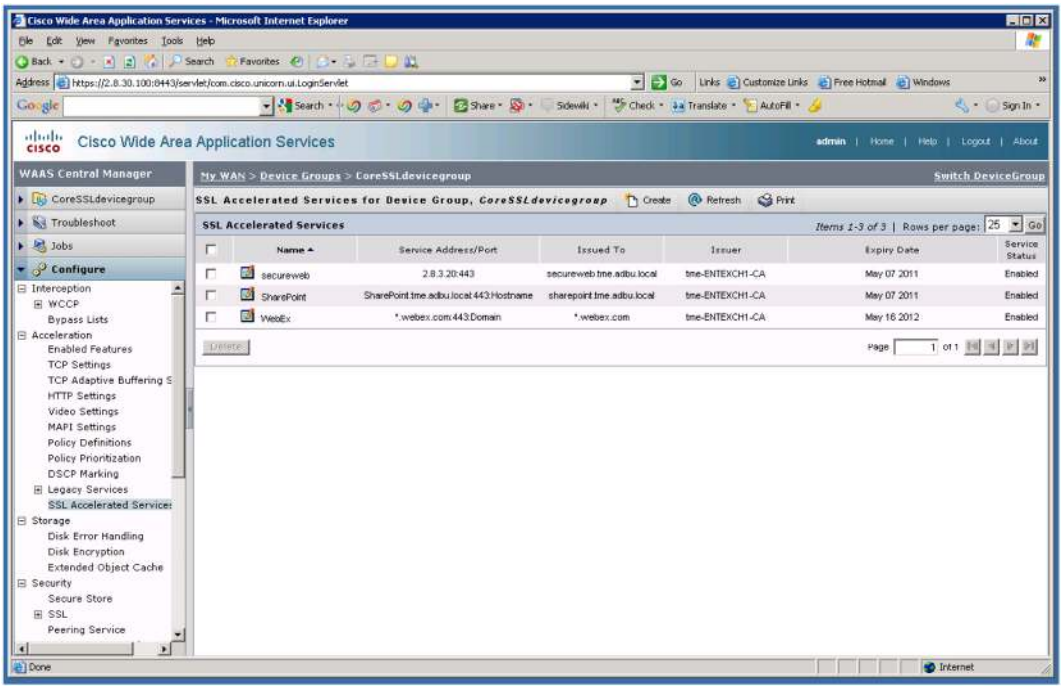
Note: By default, Cisco WAAS optimizes SSL encrypted traffic. However, the benefit it provides for SSL encrypted traffic is limited to TFO because the default application policy configuration on Cisco WAAS for SSL traffic is TFO only. Applying TFO only to the encrypted secure data is helpful in many situations in which the network has a high bandwidth delay product and the need is only to fill the WAN pipe.

As a design best practice, you should create a core Cisco WAE devices group with the Cisco WAAS Central Manager GUI and apply the SSL accelerator service configuration to that group. This step eliminates the risk of having inconsistent configuration across multiple core Cisco WAE devices in the data center, as may be the case when each core Cisco WAE is configured individually.

In the sample configuration example here, a new core device group has been created for SSL accelerated service configuration. This device group is named coreSSLdevicegroup.

To configure an SSL accelerated service for coreSSLdevicegroup, from Cisco WAAS Central Manager GUI choose **My WAN > Managed Device Groups** and select the coreSSLdevicegroup Cisco WAE. On the selected coreSSLdevicegroup device group navigation pane, choose **Configure > Acceleration > SSL Accelerated Services** and then click the **Create** button. Figure 4 shows how to create a new SSL accelerated service on coreSSLdevicegroup using the Cisco WAAS Central Manager GUI.

Figure 4. Cisco WAAS SSL Accelerated Service Configuration

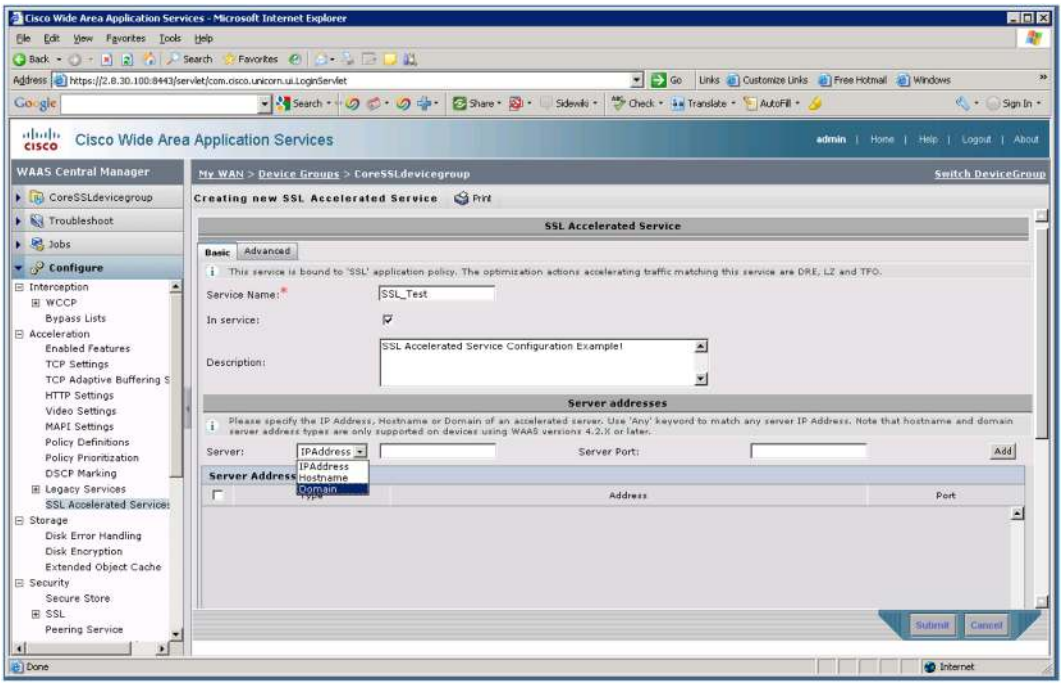


To create a new SSL accelerated service on the coreSSLdevicegroup device group, go to the Cisco WAAS Central Manager GUI **Creating new SSL Accelerated Service** page (Figure 5) and follow the steps in Table 3.

Table 3. Steps for Creating a New SSL Accelerated Service

Step	Configuration Task
Step 1	Enter a unique service name for the SSL accelerated service. The service **Description** entry is optional.
Step 2	• In the **Server Address** field, enter the hostname, IP address, or domain name of the SSL server in the data center. • In the **Server Port** field, enter the TCP port number on which the SSL service is running. • Click the **Add** button to add the server IP address and server port to the configuration. A single SSL accelerated service can be used with multiple IP addresses and port numbers.
Step 3	If you have an existing server SSL certificate and private key corresponding to that certificate, the certificate and private key can be imported in either Privacy Enhanced Mail (PEM) or Public Key Cryptography Standards 12 (PKCS#12) format. You can copy the PEM format and paste it into the Cisco WAAS Central Manager GUI directly, or you can upload it through the browser.
Step 4	Mark the new service operational by clicking the check box to the right of **In service**.
Step 5	Click the Submit button to create the new SSL accelerated service.

Figure 5. Creating a New SSL Accelerated Service



To verify the SSL accelerated service configuration, establish a Telnet session with the core Cisco WAE console and enter the **show running-config | begin crypto** command.

```
WAE# show running-config | begin crypto
...skipping
crypto ssl services global-settings
   version all
   exit
!
!
!
crypto ssl services accelerated-service SSL_Test
   description SSL accelerated service config
   server-cert-key SSL_Test.p12
   server-ip 2.8.3.30 port 443
   inservice
   exit
!
… many lines omitted …
```

Configure SSL Accelerated Service and SSL Server Certificate

The Cisco WAAS Central Manager GUI supports various options to add an SSL server certificate to the SSL accelerated service. Table 4 describes the options and when to use them.

Table 4. SSL Accelerated Service and SSL Server Certificate Configuration Options

Configuration Option	Description
Generate a self-signed certificate and private key	This option lets the admin user create a self-signed certificate and private key to be associated with an SSL accelerated service. This key can be used for demonstration testing when the actual back-end server private key and certificate are not available for import. The client browser displays a security warning message stating that the certificate is invalid with this option. However, SSL acceleration will work, and the user will see SSL accelerated connections.
Import existing certificate and optionally private key	The Import option allows the admin user to import an SSL server certificate and private key to associate with the SSL accelerated service configuration. The import method supports two certificate formats: • PEM format (allows both file import and plaintext copy and paste) • PKCS#12 format (this format is the same as the .pfx format used by the Microsoft Internet Information Services [IIS] server)
Export certificate and key	This option allows the Cisco WAAS admin user to export the server private key and certificate from the core Cisco WAE if required.
Generate certificate signing request	This option can be used to generate a PKCS#10 format certificate signing request (CSR), which can be submitted offline to a CA server to obtain an X.509 SSL certificate.

Note: In a proof-of-concept pilot testing environment, the self-signed certificate can be used to quickly demonstrate the SSL acceleration benefits.

In cases in which customers have their own CA servers and the capability to issue SSL server certificates, the admin user can use the **Generate certificate signing request** option to create a CSR and submit it to the CA server to obtain an SSL certificate.

The import option supports two formats: PEM and PKCS#12. The PEM file format may contain either the private key or the server certificate in Base-64 encoded ASCII text. The certificate and private key can be copied and pasted into the Cisco WAAS Central Manager GUI through the browser when Base-64 encoding is used with the PEM file. The PEM files can also be imported by choosing the browse-to-file option.

The PKCS#12 format is the same as the format obtained with the Microsoft IIS server and Microsoft SharePoint Server .pfx file extension. Typically, the PKCS#12 file contains both the private key and certificate in the same file and can be imported as a file.

Note: Tools such as OpenSSL can be used to convert certificate and key files from one format to the other if required.

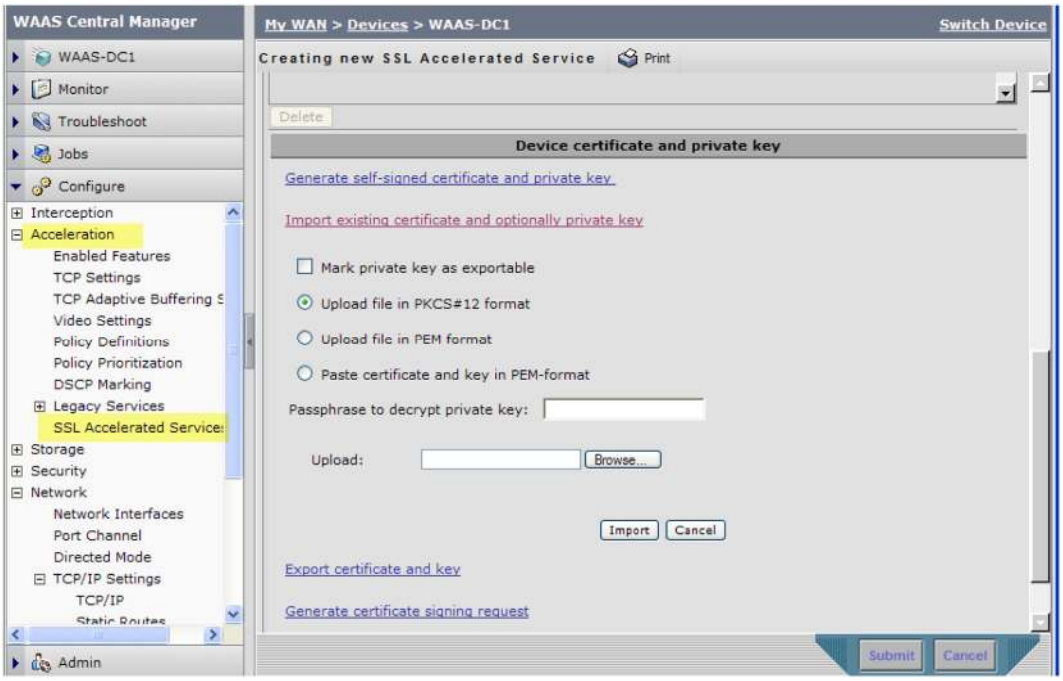
The following example shows how to import a PKCS #12 file that contains the SSL server private key and certificate into the SSL accelerated service configuration. The PKCS#12 file used in this example was exported from a Microsoft IIS web server with a .PFX file extension. Please refer to Appendix A to learn about how to export private keys and certificates from a Microsoft IIS web server.

Note: To use the **Generate a self-signed certificate and private key** option, refer to Appendix A.

Import SSL Server Private Key and Certificate in PKCS#12 Format

To import the PKCS#12 file with the server private key and certificate in the SSL accelerated service configuration, scroll down to the **Device certificate and private key** section. Figure 6 shows how to import a PKCS#12 file with a server certificate and private key. In the web browser, click the **Import existing certificate and optionally private key** link and select **Upload file in PKCS#12 format**. Enter the exact passphrase used at the time of private key export into the text box next to **Passphrase to decrypt private key**. Click the **Browse** button and browse to the file folder on the local machine where the PKCS#12 file is located. After selecting the file to import, click the **Import** button.

Figure 6. Cisco WAAS SSL Accelerated Service Certificate Import Using PKCS#12 File



The certificate will appear in the SSL accelerated service configuration after it is successfully imported. Figure 7 shows the certificate information after it was imported by uploading a PKCS#12 file. To finish the SSL accelerated service configuration, click the **Submit** button.

After an SSL accelerated service is configured on the Cisco WAAS Central Manager, it sends the SSL accelerated service configuration and the server private key and certificate to the core Cisco WAE devices. To verify that the service is configured and the certificate is installed on the core Cisco WAE device, establish a Telnet session with the core Cisco WAE device and enter the CLI command **show crypto certificates**:

```
WAE#show crypto certificates
Managed Store:
--------------
File: SSL_Test.p12                Format: PKCS12
EEC: Subject: C=US/ST=ca/L=San Jose/O=WAAS/OU=WAAS.LOCAL/CN=server
     Issuer: DC=local/DC=waas/CN=server
CA1: Subject: DC=local/DC=waas/CN=server
     Issuer: DC=local/DC=waas/CN=server
```

In this example, an SSL accelerated service named SSL_Test is configured, and a PKCS#12 file with a certificate and private key is added to the service configuration. The **show** output on the core Cisco WAE shows the file certificate stored with the filename SSL_Test.p12 in PKCS#12 format on the core Cisco WAE.

Figure 7. SSL Accelerated Service Certificate Information After Importing the Certificate

Verify SSL Acceleration Policy

When an SSL accelerated service is created and put into service on the core Cisco WAE, the following policy actions take place:

- The server IP address, hostname or domain name, and port number are used to generate a dynamic classifier.
- This dynamic classifier is attached to the application policy called SSL.
- The optimization action for this dynamic classifier is set to DRE, LZ, and TFO.

SSL accelerated services use the application policy named SSL for statistics collection. The SSL application policy is predefined in the Cisco WAAS policy definitions and is applied to the HTTPS classifier by default. If the SSL application policy is missing from the policy definition on the Cisco WAE, it must be defined by the administrator. From the Cisco WAE CLI console, enter the **show policy-engine application dynamic** command to verify that the dynamic policy for SSL accelerated service exists:

```
WAE#show policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 5  Max In Use: 6  Allocations: 1742

Dynamic Match Type/Count Information:
  None                    0
  Clean-Up                0
  Host->Host              0
  Host->Local             0
  Local->Host             0
  Local->Any              0
  Any->Host               4
  Any->Local              0
  Any->Any                1
```

```
Individual Dynamic Match Information:
  Number:     1   Type: Any->Host (6)  User Id: SSL (4)
    Src: ANY:ANY  Dst: 2.8.3.30:443
    Map Name: basic
    Flags: SSL
    Seconds: 0  Remaining: - NA -  DM Index: 32763
    Hits: 0  Flows: - NA -  Cookie: 0x40000001
    DM Ref Index: - NA -  DM Ref Cnt: 0

  Number:     3   Type: Any->Host (6)  User Id: SSL (4)
    Src: ANY:ANY  Dst: 2.8.3.20:443
    Map Name: basic
    Flags: SSL
    Seconds: 0  Remaining: - NA -  DM Index: 32765
    Hits: 1  Flows: - NA -  Cookie: 0x80000000
    DM Ref Index: - NA -  DM Ref Cnt: 0

  Number:     5   Type: Any->Any (8)  User Id: SSL (4)
    Src: ANY:ANY  Dst: ANY:443
    Map Name: basic
    Flags: REPLACE SSL
    Seconds: 0  Remaining: - NA -  DM Index: 32767
    Hits: 87  Flows: - NA -  Cookie: 0x2FFFFFFF
    DM Ref Index: - NA -  DM Ref Cnt: 0

WAE#
```

The application policy engine uses a cookie value in the dynamic policy to determine which SSL accelerated service will be matched for a particular incoming connection, depending upon the type of server entry. Table 5 shows the different cookie types in the dynamic policy configuration that are used to distinguish between the types of server address entry.

Table 5. Cookie Values Used in Dynamic SSL Application Policies

Cookie Value	Type of Configuration Entry	Comments
0x8 xxxxxxx	Server IP address	Static IP address configuration is used for pattern matching.
0x4 xxxxxxx	Server hostname	The data center WAE is required to perform DNS lookup for the hostname.
0x2FFFFFFF	Server domain name	This special entry means a reverse DNS lookup is required on the destination host IP address to match against the domain.
0x1xxxxxxx	Server Any	All SSL connections will be accelerated using this accelerated service configuration.

Note: Cisco WAAS treats SSL connections slightly differently than other traffic. By default, Cisco WAAS applies TFO-only optimizations to all SSL connections, as specified by the default HTTPS classifier settings.

However, when the Cisco WAAS SSL Application Optimizer is enabled on the Cisco WAE and the Cisco WAE finds a dynamic classifier match for the SSL connection, it applies full optimization (DRE, LZ, and TFO) to the SSL connection.

Test SSL Application Optimization

After successfully configuring an SSL accelerated service and verifying that a dynamic classifier was automatically configured on the core Cisco WAE devices, you can test SSL acceleration. Open a web browser on the client machine and send an HTTPS request to the SSL server in the data center. The SSL web request must go through the edge and the core Cisco WAEs for SSL acceleration.

From the Cisco WAE CLI console, enter the **show statistics connection** command to verify that the new SSL connections matching the dynamic classifier are, in fact, SSL accelerated. The SSL accelerated connections listed in the command output will show TSDL as the acceleration policy, where "S" stands for SSL accelerated connection.

```
WAE# show statistics connection
Current Active Optimized Flows:                    2
   Current Active Optimized TCP Plus Flows:        2
   Current Active Optimized TCP Only Flows:        0
   Current Active Optimized TCP Preposition Flows: 0
Current Active Auto-Discovery Flows:               0
Current Reserved Flows:                            10
Current Active Pass-Through Flows:                 0
Historical Flows:                                  429
D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO
ConnID        Source IP:Port          Dest IP:Port            PeerID Accel RR
 29328       2.8.35.100:4667         2.8.3.30:443 00:23:7d:06:6e:08 TSDL  91.9%
 29330       2.8.35.100:4678         2.8.3.20:443 00:23:7d:06:6e:08 TSDL  99.6%
WAE#
```

The SSL accelerated connections on the Cisco WAAS Central Manager will display a lock icon in the applied policy, as shown in Figure 8. Note that the SSL accelerated connections have a PC icon with a lock.

Figure 8. Connection Summary Table in Cisco WAAS Central Manager Showing an SSL Accelerated Connection

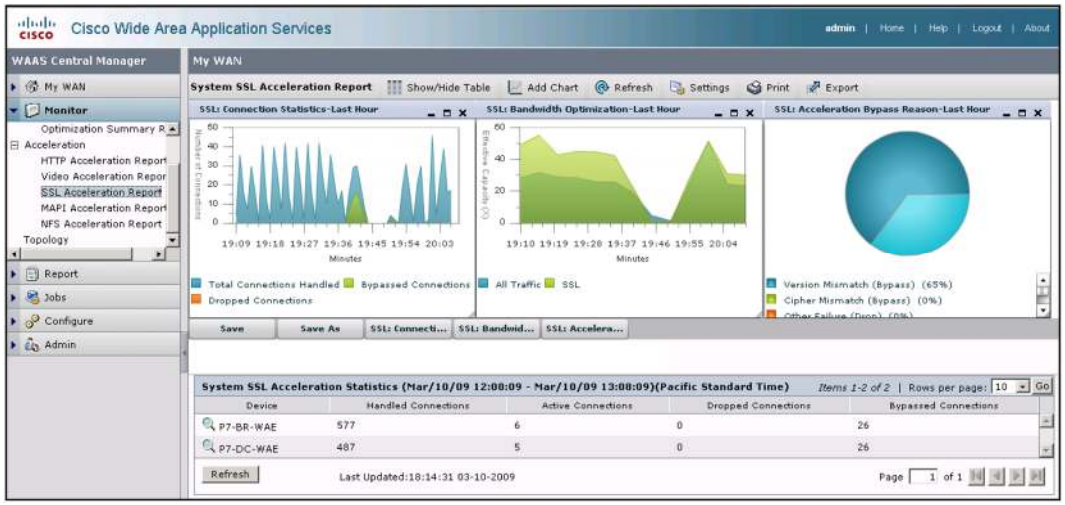
Monitor and Report SSL Accelerated Connections

Cisco WAAS Central Manager now has an SSL acceleration report in its monitoring and reporting section. The SSL acceleration report displays the SSL acceleration statistics. The following charts are included in the SSL acceleration report:

- SSL: Connection Statistics: The SSL: Connection Statistics chart displays the SSL session connection statistics, showing the total number of connections handled, the number of unaccelerated (bypassed) connections, and the number of dropped connections.
- SSL: Bandwidth Optimization: The SSL: Bandwidth Optimization chart displays the effective bandwidth capacity of the WAN link as a result of SSL acceleration, as a multiplier of its base capacity.
- SSL: Acceleration Bypass Reason: The SSL: Acceleration Bypass Reason pie chart displays the reasons that SSL traffic is not accelerated: version mismatch, cipher mismatch, revocation failure, certificate verification failure, other failure, or non-SSL traffic.

Figure 9 shows the Cisco WAAS Central Manager SSL Acceleration Report with the three charts.

Figure 9. Cisco WAAS Central Manager SSL Acceleration Report



A new application definition named SSL is added to the default policy definition list in Cisco WAAS 4.1.3.

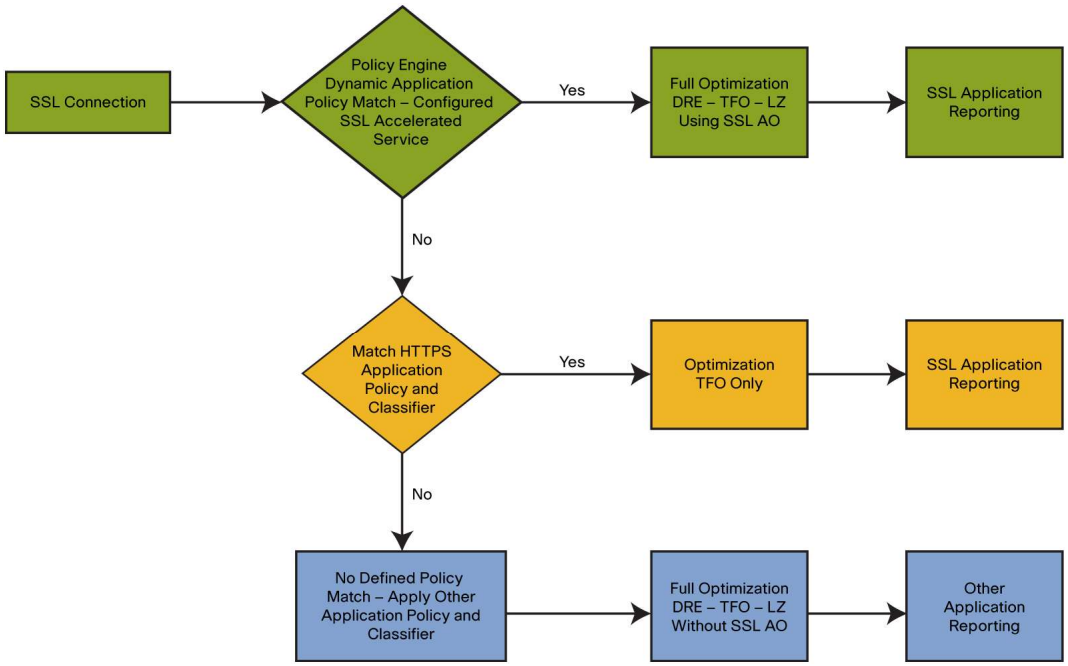
Non-HTTPS Proxy SSL Connections

Statistics for all optimized SSL traffic are reported under application SSL in the Cisco WAAS Central Manager Traffic Summary chart. The traffic summary report for SSL includes both SSL accelerated connections using the SSL accelerator and HTTPS connections optimized using TFO only.

HTTPS Proxy SSL Connections

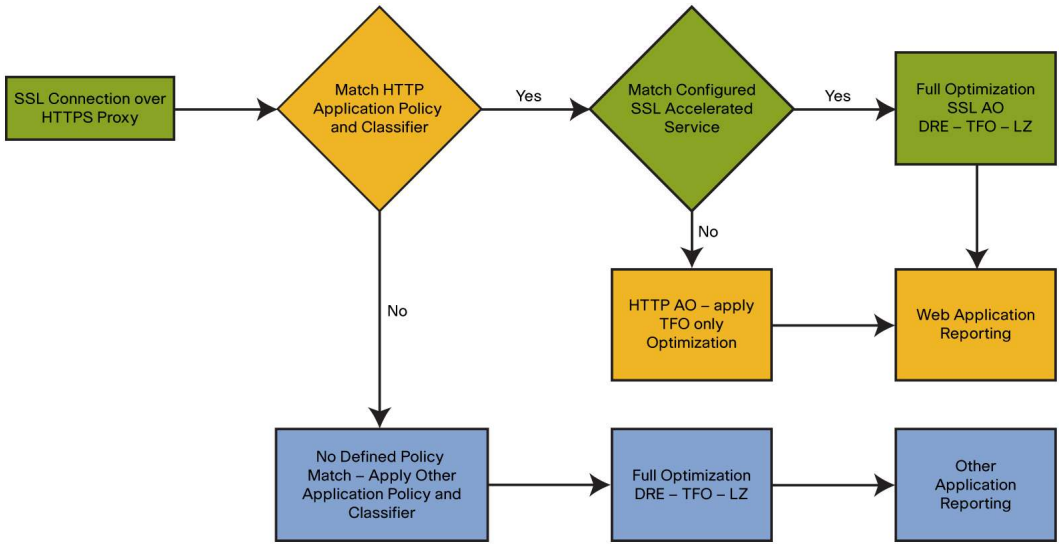
For SSL connections going through an HTTPS proxy server in the data center, the initial request is handled by an HTTP accelerator, and these connections are reported as application web traffic. Figure 10 shows how SSL connections are accelerated by Cisco WAAS and how they are reported in the Central Manager Traffic Optimization reports.

Figure 10. Cisco WAAS Reporting Flow for Optimized SSL Connections (Non-HTTPS Proxy Use Case)



The flow chart in Figure 11 explains how SSL connections going through an HTTPS proxy server are accelerated by Cisco WAAS and how they are reported in the Cisco WAAS Central Manager Traffic Optimization reports.

Figure 11. Cisco WAAS Reporting Flow for Optimized SSL Connections (HTTPS Proxy Use Case)

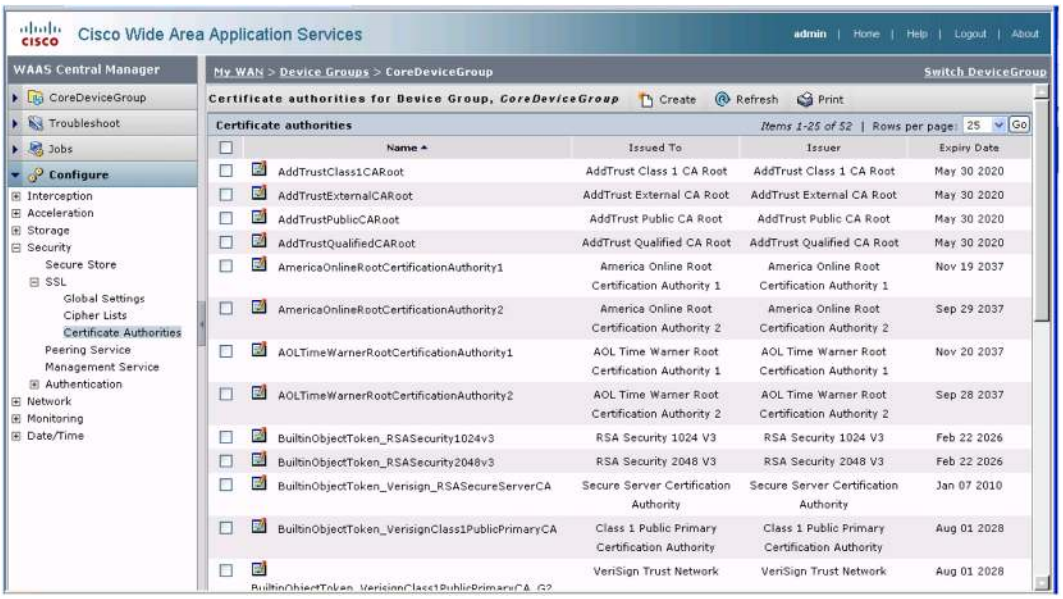


Manage the Certificate Authority

A CA is a trusted third party that issues certificates used to verify the identity of a site. Cisco WAAS SSL acceleration features by default include a list of many well-known CA certificates that can be used on the Cisco WAE. This feature also allows you to import your own CA certificate into the CA store on a Cisco WAE. The CA certificates are mainly used to verify a client or a server certificate.

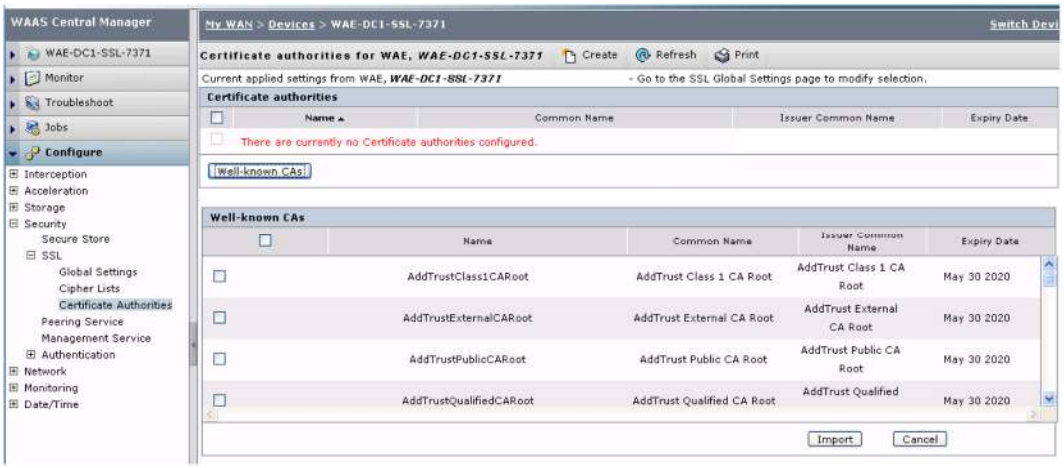
Certificate authorities provide third-party verification of client and server certificates and act as trust points for other Cisco WAAS SSL services. Well-known CA certificates can be imported into the core Cisco WAE device through device group configuration, as shown in Figure 12.

Figure 12. Well-Known CA Certificates Imported into the Core Cisco WAE CA Store



By default, Cisco WAAS includes a list of well-known root CA certificates that are already preinstalled and can be used. The Cisco WAAS SSL accelerator also allows import of a new CA certificate. To import a new CA certificate, from the Cisco WAAS Central Manager GUI, choose **My WAN > Managed Devices** and select the Cisco WAE. In the selected Cisco WAE device navigation pane, choose **Configure > Security > SSL > Certificate Authorities** and click the **Import** button. Figure 13 shows how to import a new CA certificate from the Cisco WAAS Central Manager.

Figure 13. Importing new CA Certificate on the Core Cisco WAE from the Cisco WAAS Central Manager



From the Cisco WAE CLI console, enter the **show crypto certificates** command to view the imported CA certificates. The command lists all the certificates imported into the Cisco WAE, including the management service certificate:

```
WAE# show crypto certificates
Certificate Only Store:
-----------------------
File: 1024.ca            Format: PEM
Subject: C=US/ST=CA/L=SJ/O=Cisco/OU=ADBU/CN=SSL/emailAddress=sumohame@cisco.com
Issuer: C=US/ST=CA/L=SJ/O=Cisco/OU=ADBU/CN=SSL/emailAddress=sumohame@cisco.com
--------------------------------------------------------------------------------
```

```
Managed Store:
--------------
File: s1024.p12          Format: PKCS12
EEC: Subject:
C=US/ST=CA/L=SJ/O=Cisco/OU=ADBU/CN=SSL/emailAddress=sumohame@cisco.com
     Issuer: C=US/ST=CA/L=SJ/O=Cisco/OU=ADBU/CN=SSL/emailAddress=sumohame@cisco.com
--------------------------------------------------------------------------------
Local Store:
------------
Machine Self signed Certificate
-------------------------------
Format: PKCS12
Subject: C=US/ST=California/L=San Jose/OU=ADBU/O=Cisco Systems/CN=NO-
HOSTNAME/emailAddress=tac@cisco.com
Issuer: C=US/ST=California/L=San Jose/OU=ADBU/O=Cisco Systems/CN=NO-
HOSTNAME/emailAddress=tac@cisco.com
Management Service Certificate
------------------------------
Format: PKCS12
EEC:Subject: C=US/ST=California/L=San Jose/OU=ADBU/O=Cisco Systems/CN=NO-
HOSTNAME/emailAddress=tac@cisco.com
    Issuer: C=US/ST=California/L=San Jose/OU=ADBU/O=Cisco Systems/CN=NO-
HOSTNAME/emailAddress=tac@cisco.comThe WAAS Self Signed Certificate is being used
as the Management Service Certificate
WAE#
```

The CA certificates are used when certificate verification is turned on for either the client or server certificate, or both.

Verify the Certificate

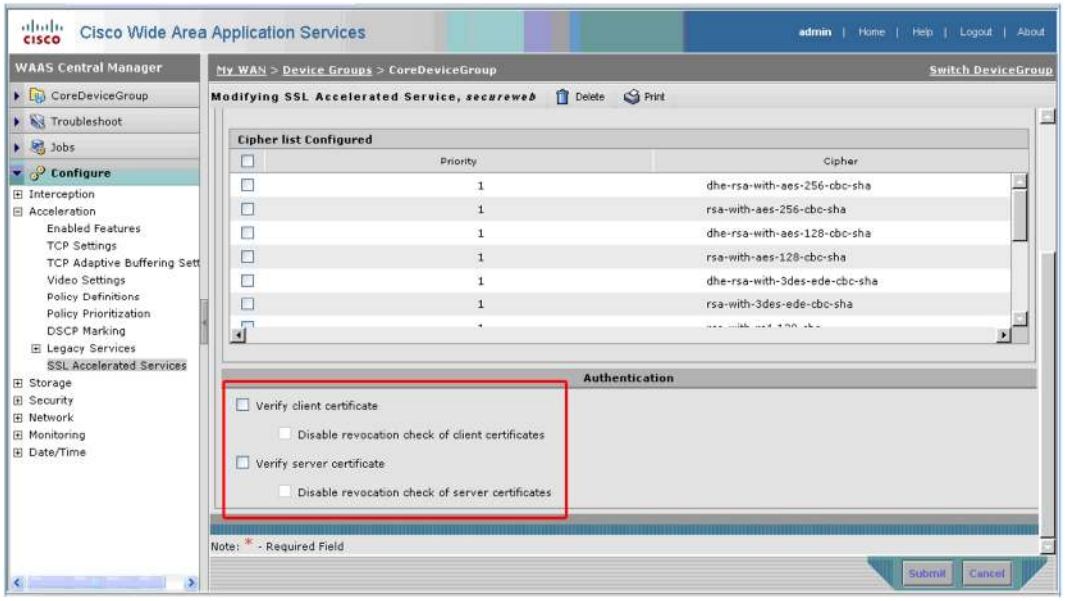
In an SSL-protected session, the server and client can authenticate one another and negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The core Cisco WAE in the data center acts as a trusted intermediary node and terminates the SSL session with the client and initiates another SSL session with the back-end server. The core Cisco WAE can be configured to verify the server certificate before accepting the SSL connection.

Client certificates provide an additional way to authenticate a client to a server using SSL. The Cisco WAAS WAE can also perform a verification check on the client before allowing the SSL session with the server to proceed. Client certificate authentication is commonly deployed in highly secure environments in which message layer authentication mechanisms using user IDs and passwords or tokens are not considered sufficient for security purposes.

The Cisco WAAS SSL feature checks the certificate presented to it by the client or the server by validating the certificate all the way up to a trusted root CA certificate in its CA store. If it fails to verify the certificate in the hierarchy, the Cisco WAE reports that the certificate verification process failed. The certificate verification process can also include an OCSP revocation check on the presented certificate to check the validity of the certificate in real time. This check can be disabled in environments in which an OCSP responder is unavailable for revocation check.

To configure certificate verification for an SSL accelerated service for a Cisco WAE using the Cisco WAAS Central Manager GUI, choose **My WAN > Managed Devices** and select the Cisco WAE. In the selected Cisco WAE device navigation pane, choose **Configure > Acceleration > SSL Accelerated Service**. From the **SSL Accelerated Services** list, click the service you want to edit and select the **Advanced** properties tab. To enable client and server certificate verification, check the appropriate check boxes in the **Authentication** section, as shown in Figure 14.

Figure 14. Configuring Certificate Verification for SSL Accelerated Service



Perform Certificate Revocation Check

Certificates may be revoked by a certification authority for various reasons. For example, if a certificate and its associated key are compromised or need to be retired for any reason, the certification authority can revoke the existing certificate. Certification authorities can provide an online service called an OCSP responder that can be used to check the revocation status of a certificate issued by the certification authority.

Cisco WAAS supports OCSP for real-time revocation status of a certificate in compliance with the U.S. Department of Defense (DoD) Class 3 PKI definition. This support is especially useful in highly secure environments because OCSP can provide the real-time status of a certificate. OCSP is also useful when client certificates are used in the SSL handshake for client authentication.

Cisco WAAS WAE performs an OCSP revocation check on a certificate presented to it during the SSL handshake when certificate verification is configured for the SSL accelerated service. The certificate verification process follows the SSL global settings on the device to determine the OCSP responder.

Global settings for OCSP revocation check can be configured under the device or device group SSL Global Settings page, as shown in Figure 15.

Figure 15. SSL Global Settings for OCSP Responder Service

Following are the global settings for the OCSP revocation check feature:

- **Disabled:** If revocation check is disabled globally, then an OCSP revocation check is performed.
- **ocsp-url:** If revocation check is configured to use ocsp-url, then the Cisco WAE uses the OCSP responder URL configured as shown in Figure 15.

- **ocsp-cert-url:** If revocation check is configured to use ocsp-cert-url, then the Cisco WAE looks for an OCSP responder URL included in the certificate presented to it. If it does not find one, it uses the OCSP responder URL configured as shown in Figure 15.

Configure Certificate Chaining Support in Cisco WAAS

A certificate chain is a sequence of certificates in which each certificate is signed by the next. The final certificate, called the root certificate, is owned by a certificate authority. Client web browsers may not accept an SSL server certificate if it is signed by an intermediate CA server, and the client machine then will be unable to verify the certificate hierarchy up to a root CA certificate. This scenario is commonly observed when browsing a secure site in the following cases:

- The SSL server sends only the server certificate during negotiation.
- The client cannot verify the issuer of the certificate (intermediate CA).
- The client has an expired copy of the intermediate CA server certificate.

Cisco WAAS SSL accelerated service configuration supports certificates chains with a depth of up to eight certificates in the chain, including the server SSL certificate. The Cisco WAAS Central Manager allows import of 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 a root CA at the end. The Cisco WAAS Central Manager validates the chain and rejects it if the validity date of the CA certificate is expired or if the signing order of certificates in the chain is not consecutive.

Configure Global SSL Settings: Supported SSL Versions and Cipher Lists

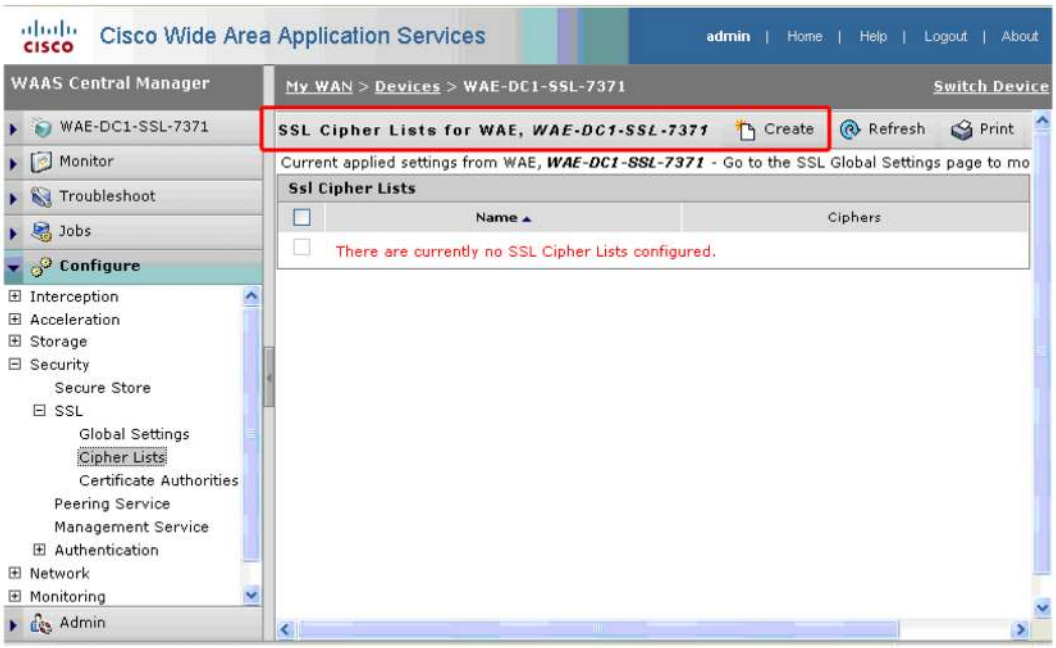
The Cisco WAAS SSL feature supports both SSLv3 and TLSv1 by default. Cipher lists are sets of cipher suites that can be assigned to your SSL acceleration configuration. A cipher suite is an SSL encryption method that includes the key exchange algorithm, the encryption algorithm, and the Secure Hash Algorithm. Cisco WAAS comes configured with a predefined cipher list that is applied to all SSL services by default.

The predefined cipher list contains the following cipher suites:

```
dhe-rsa-with-aes-256-cbc-sha:1
rsa-with-aes-256-cbc-sha:1
dhe-rsa-with-aes-128-cbc-sha:1
rsa-with-aes-128-cbc-sha:1
dhe-rsa-with-3des-ede-cbc-sha:1
rsa-with-3des-ede-cbc-sha:1
rsa-with-rc4-128-sha:1
rsa-with-rc4-128-md5:1
dhe-rsa-with-des-cbc-sha:1
rsa-with-des-cbc-sha:1
rsa-export1024-with-rc4-56-sha:1
rsa-export1024-with-des-cbc-sha:1
dhe-rsa-export-with-des40-cbc-sha:1
rsa-export-with-des40-cbc-sha:1
rsa-export-with-rc4-40-md5:1
```

To configure a new cipher list, from the Cisco WAAS Central Manager GUI choose **My WAN > Managed Devices** and select the Cisco WAE. In the selected Cisco WAE device navigation pane, choose **Configure > Security > SSL > Cipher Lists** and then click **Create**. Figure 16 shows how to create a new cipher list from the Cisco WAAS Central Manager.

Figure 16. Creating a New Cipher List on the Core Cisco WAE in the Cisco WAAS Central Manager



From the Cisco WAE CLI console, enter the **show running-config** command to verify the new cipher list configuration:

```
WAE# show running-config
… many lines omitted …
!
crypto ssl cipher-list test
   cipher dhe-rsa-with-aes-256-cbc-sha priority 1
   cipher rsa-with-aes-256-cbc-sha priority 1
   exit
!
… many lines omitted …
```

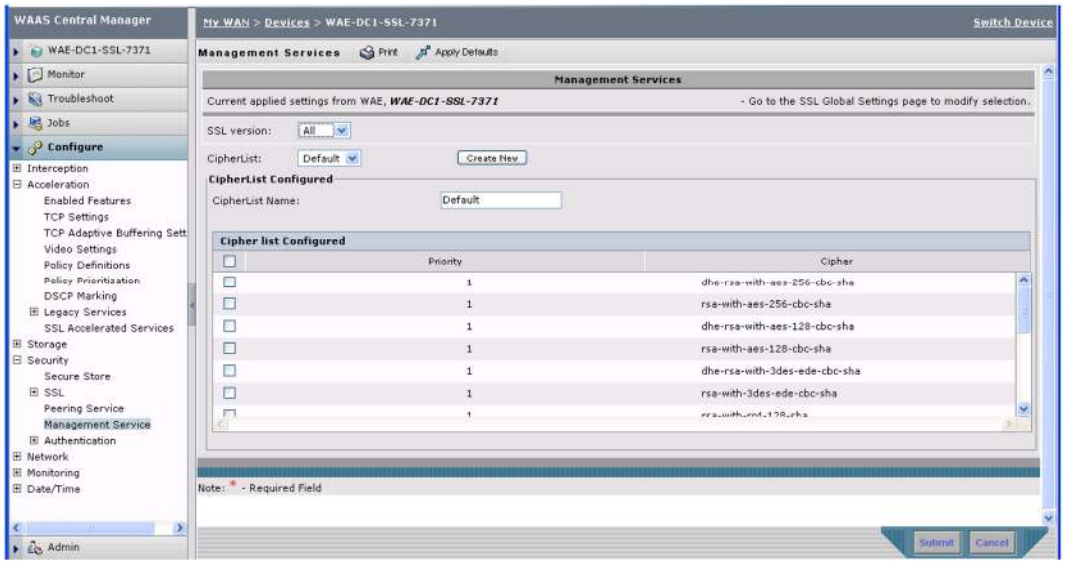
The new cipher list can either be set as the default in the global SSL settings or applied to an SSL accelerated service.

Configure SSL Management Service

The Cisco WAAS Central Manager and the Cisco WAE appliances communicate with each other over a secure channel using SSL. This process is known as SSL management service, and it uses the default settings from the global SSL configuration page. The SSL management service uses a self-signed certificate by default, and this setting cannot be changed. However, the SSL management service allows you to specify the SSL version and cipher list that will be used for secure communication between the Cisco WAAS Central Manager and the Cisco WAE.

To change or view the properties for the SSL management service for a Cisco WAE, from the Cisco WAAS Central Manager GUI choose **My WAN > Managed Devices** and select the Cisco WAE. In the selected Cisco WAE device navigation pane, choose **Configure > Security > Management Service**. Figure 17 shows the SSL management service configuration page in the Cisco WAAS Central Manager.

Figure 17. SSL Management Service Configuration in the Cisco WAAS Central Manager

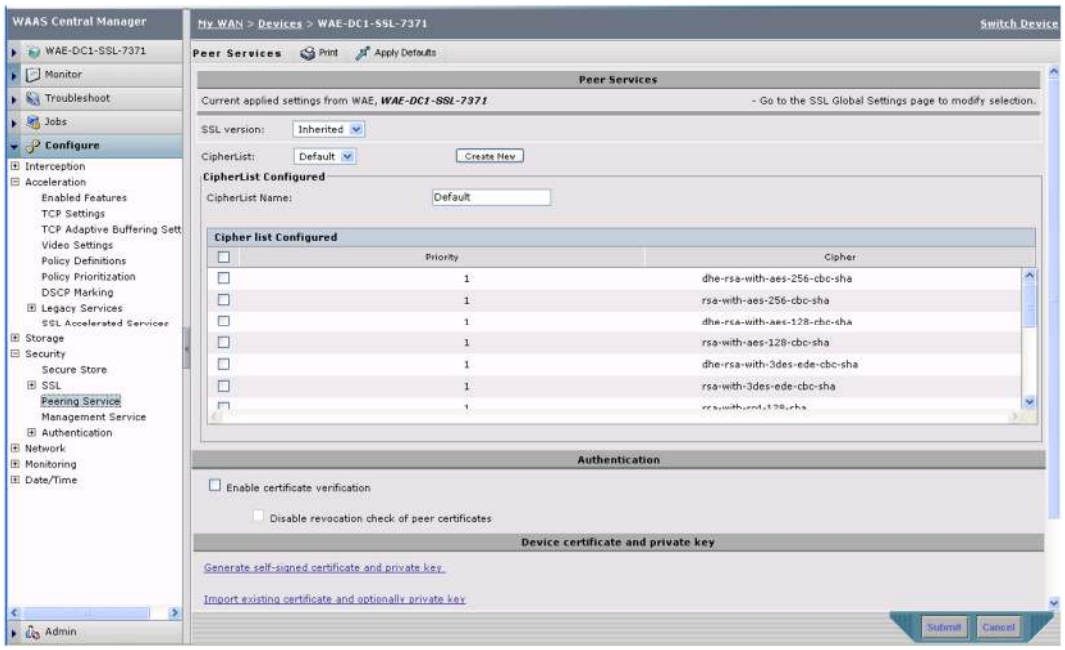


Configure SSL Peering Service

The SSL peering service defines the secure communication between the edge and the core Cisco WAE appliances. The SSL peering service uses a self-signed machine certificate, default cipher list, and SSLv3. The SSL peering service allows you to change the certificate used for secure communication and specify the SSL version and cipher list that will be used for secure communication between the Cisco WAAS Central Manager and the Cisco WAE. The SSL peering service also allows you to configure peer certificate verification if required.

To change or view the properties for the SSL peering service for a Cisco WAE, from the Cisco WAAS Central Manager GUI choose **My WAN > Managed Devices** and select the Cisco WAE. In the selected Cisco WAE device navigation pane, choose **Configure > Security > Peering Service**. Figure 18 shows the SSL peering service configuration page in the Cisco WAAS Central Manager.

Figure 18. SSL Peering Service Configuration in the Cisco WAAS Central Manager



Simplified Deployment Model for Cloud-Based Services

Cloud-based SaaS providers such as WebEx.com and Salesforce.com primarily use HTTPS to securely deliver services to their clients. Using SSL Application Optimizer, Cisco WAAS can optimize delivery of these services to the remote branch-office users who connect to these services through a backhaul connection to the data center.

However, the solution poses some unique challenges in terms of simplifying the implementation and deployment model. Typically these SaaS providers have multiple SSL server farms with multiple hosts spanning across several data centers. When a client initiates an SSL connection request to an SSL server in the SaaS farm, the SSL Application Optimizer should be able to intercept this incoming SSL request and map the destination IP address in the request to an SSL accelerated service to present the right SSL certificate to the client to perform an SSL handshake.

For SSL services hosted in the enterprise data center, the IT administrator knows and controls the SSL server IP and can provide it to the data center WAAS. But for SSL service hosted at a third-party SaaS provider cloud, the SSL server IP address is not controlled by the IT administrator. In addition, there may be not just one but multiple server IP addresses - even for a single SaaS service - and these addresses are subject to change.

To simplify the SaaS optimization model, Cisco WAAS provides support for domain name in the SSL accelerated service configuration. When an SSL accelerated service is configured with a wildcard domain name such as *.webex.com, the SSL Application Optimizer, upon receiving an SSL connection request from the client, performs a reverse DNS lookup on the destination server IP address; if the IP address resolves to a host with webex.com domain name, then the appropriate SSL accelerated service policy is applied to this connection (refer to Figure 19 and Table 6).

Figure 19. Simplified Deployment for SaaS Optimization

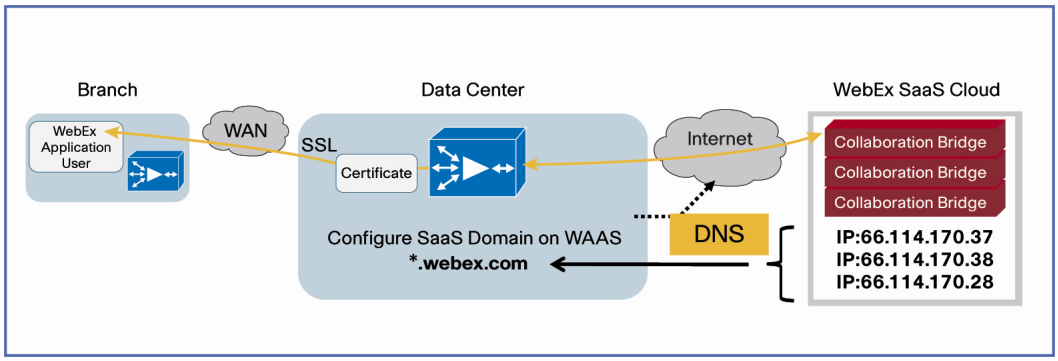


Table 6. Simplified SSL Application Optimizer Configuration Workflow for Cloud-Based SaaS Optimization

Step	Configuration Task
Step 1	• Admin configures single SaaS domain on WAAS: "*.webex.com" • Optionally could use SaaS server hostname also
Step 2	• Provides wildcard certificate with Common Name "*.webex.com" • Options: Self-signed or Enterprise CA signed certificate
Step 3	• Cisco WAAS performs DNS lookup on destination IP addresses automatically (using DNS) ◦ Identifies and optimizes connections to SaaS servers ◦ Tracks SaaS server IP address changes

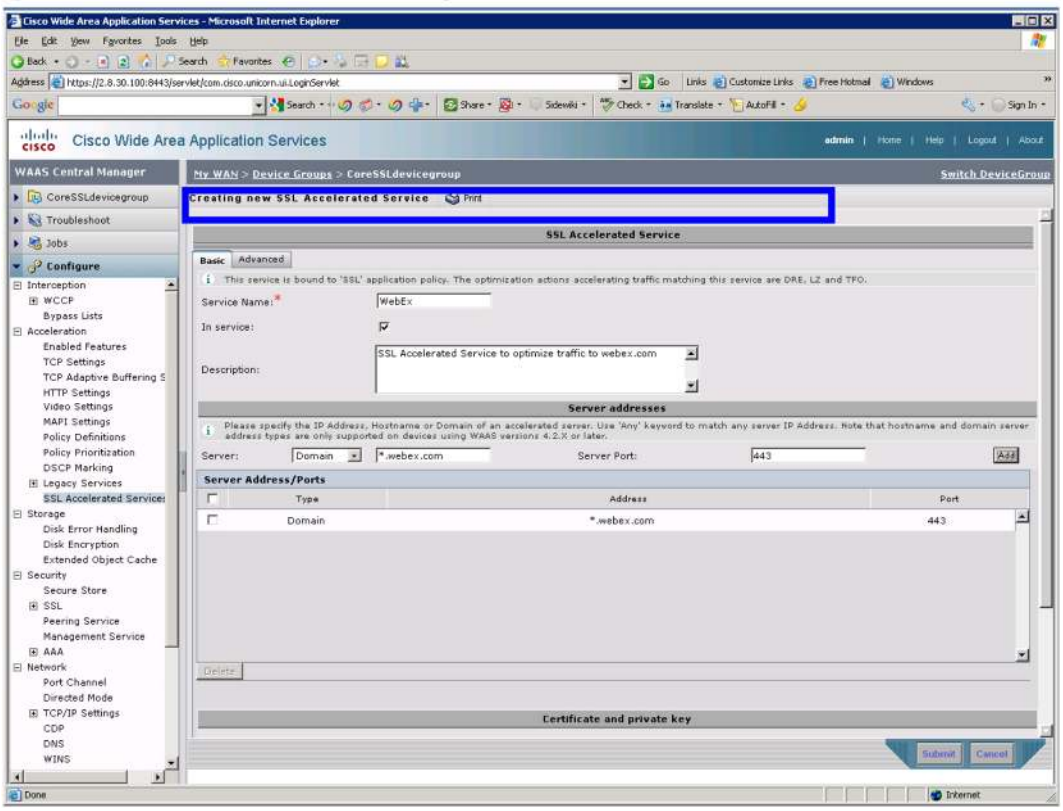
Cisco WAAS provides flexible options to choose from when selecting which SSL server certificate to associate with the SaaS services to be accelerated and optimized. Cisco WAAS can support the original SSL server certificate and private key if that is available from the service provider. If not, a self-signed wildcard domain certificate or an Enterprise CA signed wildcard domain certificate can be used to substitute the original SSL server certificate. A

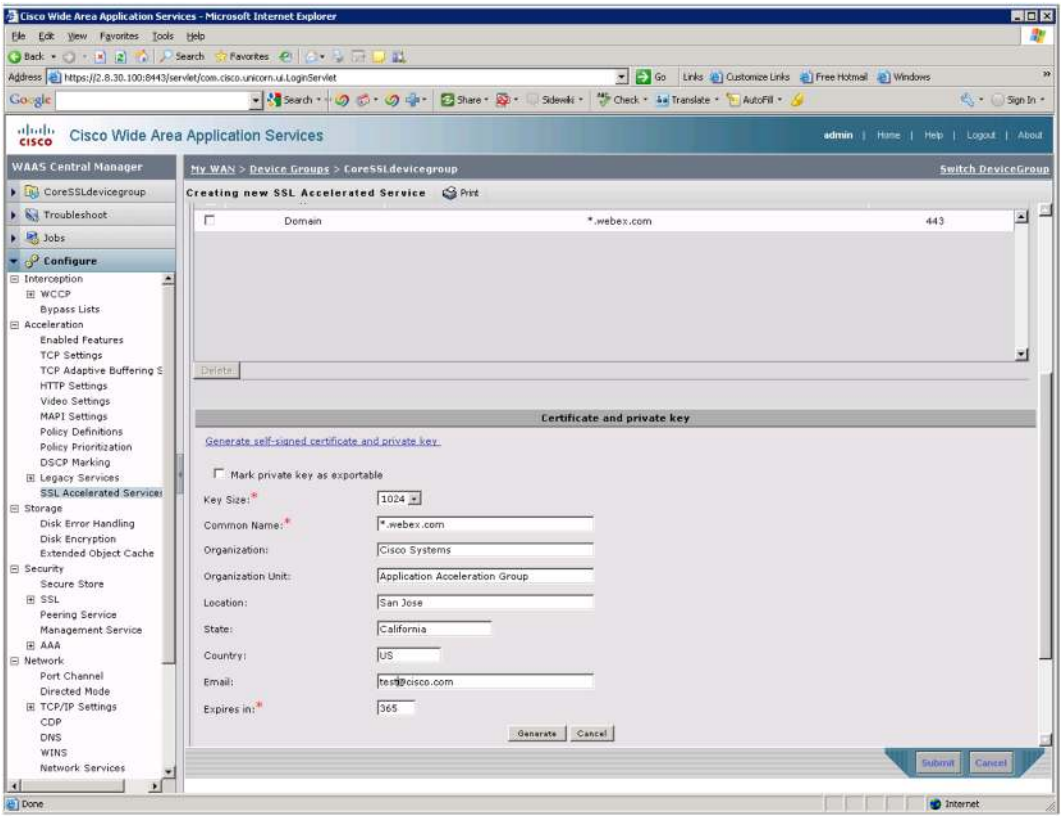
wildcard certificate is valid for the entire domain and has an asterisk instead of hostname in the Common Name field. An example of a wildcard certificate would be one with CN (common name) = *.webex.com, which is valid for any host in the domain webex.com.

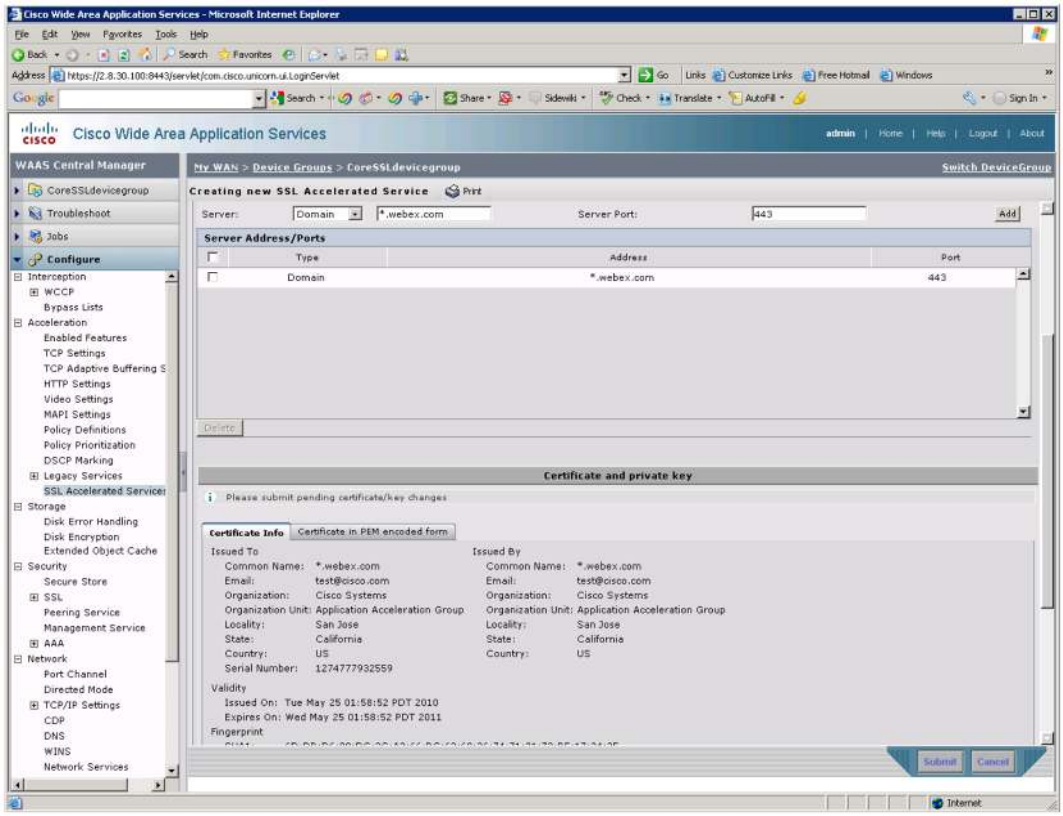
In the sample configuration example here, a new core device group has been created for SSL accelerated service configuration. This device group is named coreSSLdevicegroup.

In this example we will show how to configure an SSL accelerated service using the self-signed certificate option to accelerate remote branch-office user connections to webex.com SaaS provider services. First log in to the Cisco WAAS Central Manager; then from the Cisco WAAS Central Manager GUI, choose **My WAN > Managed Device Groups** and select the coreSSLdevicegroup Cisco WAE. On the selected coreSSLdevicegroup device group navigation pane, choose **Configure > Acceleration > SSL Accelerated Services** and then click the **Create** button. Figure 20 shows how to create a new SSL accelerated service named WebEx on coreSSLdevicegroup using the Cisco WAAS Central Manager GUI.

Figure 20. Cisco WAAS SSL Accelerated Service Configuration for WebEx







Appendix A

Exporting the Server Private Key and SSL Certificate from Microsoft IIS Server

You can export the SSL certificate and private key used to secure a Microsoft SharePoint Server and IIS server by using the IIS Certificate Export Wizard. The Microsoft IIS server allows you to export server private keys only if they were marked as exportable at the time of import. Cisco WAAS requires the SSL certificate and private key associated with the SSL server in the data center to accelerate client connections from the branch-office users to the SSL server.

The SSL certificate and private key associated with a website under the Microsoft IIS server or SharePoint Server can be exported in PKCS#12 (.pfx extension) format. To export the server private key and certificate, start the Microsoft IIS Manager. Choose **IIS Site Properties > Directory Security > View Certificate** and launch the **IIS Certificate Export Wizard**.

Figures 21 and 22 show how to export the private key and certificate from a Microsoft IIS web server.

Figure 21. Generating a Self-Signed Wild Card Domain Certificate

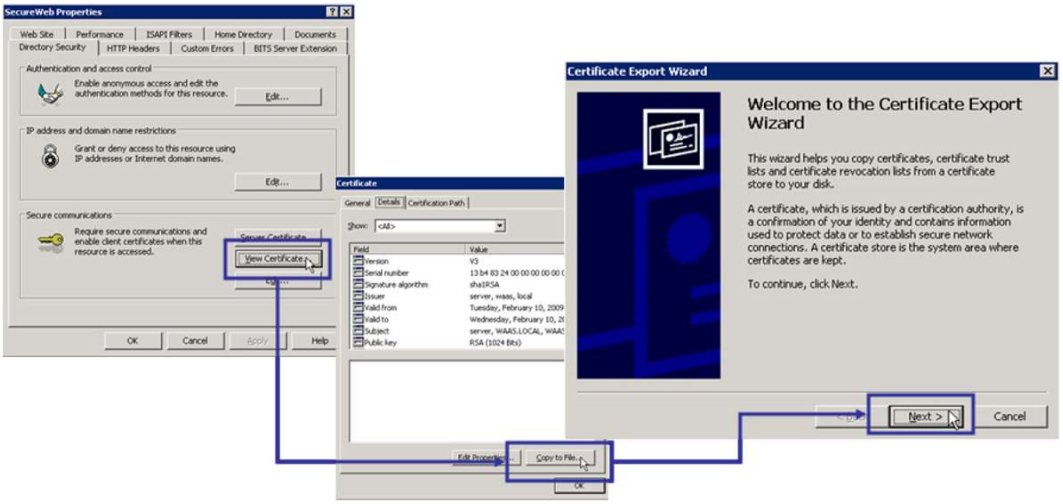
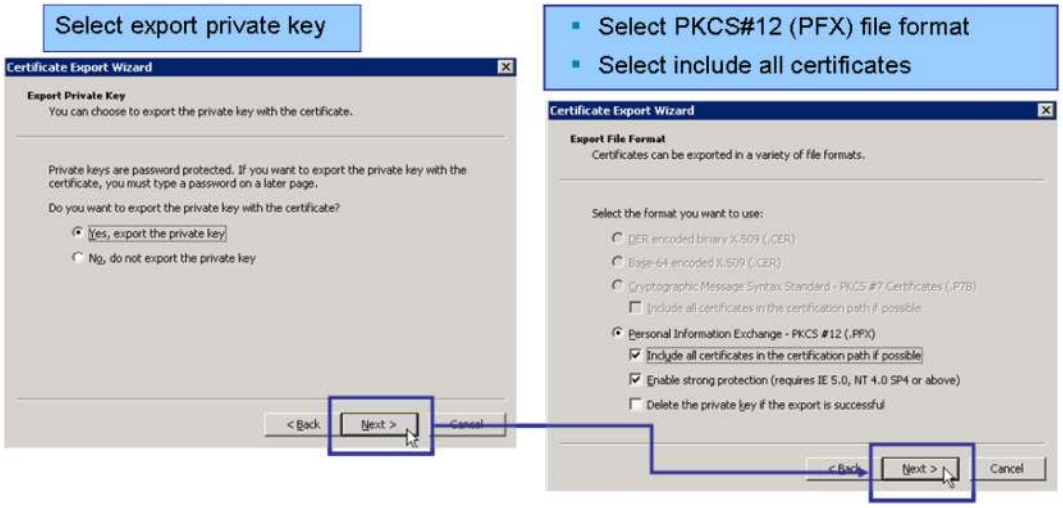


Figure 22. Self-Signed Wild Card Domain Certificate for WebEx.com



If the option to export a private key with the SSL server certificate is not available, or if the SSL certificate and private key cannot otherwise be obtained because of other constraints, the following other choices are available:

- Generate a self-signed certificate and key pair in the Cisco WAAS SSL accelerated service configuration. The client browser will display a security warning stating that the certificate could not be verified.
- Create a CSR by generating a new key pair and submit the CSR to an Enterprise CA server to obtain a new X.509 SSL certificate.

Generating a Self-Signed Certificate and Private Key

A self-signed certificate is an identity certificate that is signed by itself. Typically, a digital certificate is signed by a third-party trusted CA that the client web browsers are configured to trust.

When an SSL server presents a self-signed certificate to a web browser, the browser will display a warning stating that the certificate could not be verified. You can either accept the certificate and allow the SSL handshake to continue or stop the SSL connection from being established.

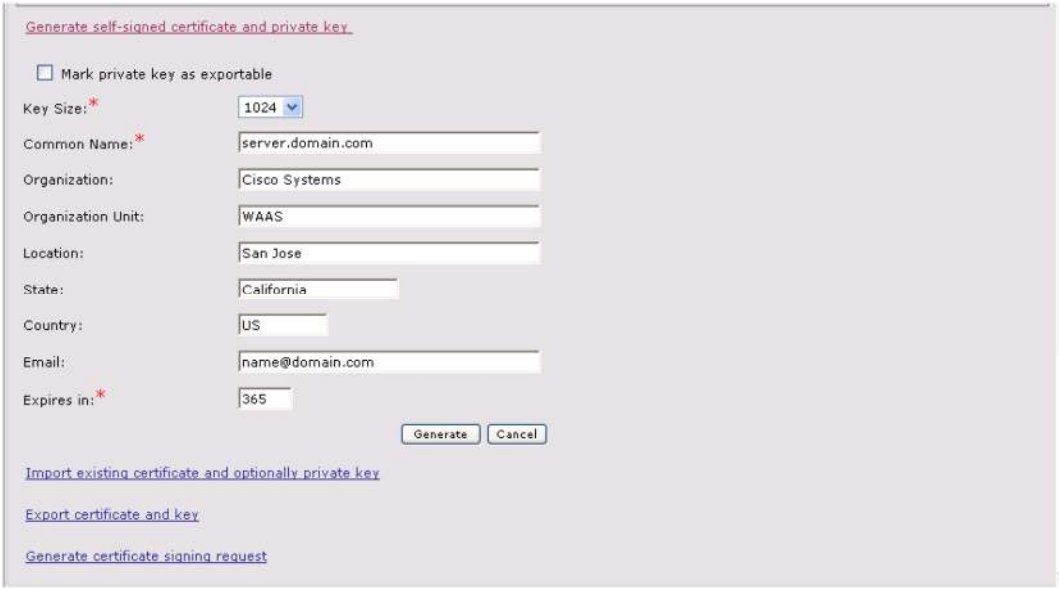
Self-signed certificates are useful in proof-of-concept testing or small pilot designs when access to an actual SSL server certificate and private key is restricted. Cisco WAAS provides an option to generate a self-signed certificate for use with an SSL accelerated service.

To generate a self-signed certificate and private key for an SSL accelerated service, follow these steps:

- Select the **Mark private key as exportable** check box to export this certificate or key in the Cisco WAAS Central Manager and device CLI later.
- Fill in the fields for the certificate and private key.

Figure 23 shows how to generate a self-signed certificate.

Figure 23. Generating a Self-Signed Certificate



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C07-541981-01 06/10