Managing Security

This section describes security concepts and configuration for Expressway. (Information about managing user accounts, device authentication, and registration access control is provided in separate chapters later in this guide.)

Security Basics

Data at Rest

Every software installation (from X8.11) has a unique root of trust. Each Expressway system has a unique key that is used to encrypt data local to that system. This improves the security of data at rest in the following ways:

- The new key is created when you upgrade a pre-X8.11 version to X8.11 or later, and is used to encrypt all data on the first restart.
- Only this key can be used to decrypt data from this system. No other Expressway key can decrypt this system's data.
- The key is never exposed on the UI, and it is never logged--locally or remotely.

TLS and Certificates

For TLS encryption to work successfully in a connection between a client and server:

- The server must have a certificate installed that verifies its identity, which is signed by a Certificate Authority (CA).
- The client must trust the CA that signed the certificate used by the server.

Expressway lets you install a certificate that can represent the Expressway as either a client or a server in TLS connections. Expressway can also authenticate client connections (typically from a web browser) over HTTPS. You can upload certificate revocation lists (CRLs) for the CAs used to verify LDAP server and HTTPS client certificates. Expressway can generate server certificate signing requests (CSRs), so there is no need to use an external mechanism to do this.

Note For all secure communications (HTTPS and SIP/TLS), we recommend that you replace the Expressway default certificate with a certificate generated by a trusted CA.

Table 1: Expressway Role in Different Connection Types

In connections...	The Expressway acts as...
To an endpoint.	TLS server.
To an LDAP server.	Client.
Between two Expressway systems.	Either Expressway may be the client. The other Expressway is the TLS server.
Over HTTPS.	Web browser is the client. Expressway is the server.

Note We also recommend using a third-party LDAP browser to verify that your LDAP server is correctly configured for TLS.

TLS can be difficult to configure. So if using it with an LDAP server, for example, we recommend verifying that the system works correctly over TCP, before you attempt to secure the connection with TLS.

Caution Certificates must be RFC-compliant. Do not allow CA certificates or CRLs to expire, as this may cause certificates signed by those CAs to be rejected.

Certificate and CRL files are managed via the web interface, and cannot be installed using the CLI.

Configuring Certificate-Based Authentication

The **Certificate-based authentication configuration** page (**Maintenance** > **Security** > **Certificate-based authentication configuration**) is used to configure how the Expressway retrieves authorization credentials (the username) from a client browser's certificate.

This configuration is required if **Client certificate-based security** (defined on the System page) is set to *Certificate-based authentication*. This setting means that the standard login mechanism is no longer available and that administrators (and FindMe accounts, if accessed via the Expressway) can log in only if they present a valid browser certificate - typically provided via a smart card (also referred to as a Common Access Card or CAC) - and the certificate contains appropriate credentials that have a suitable authorization level.

Enabling Certificate-Based Authentication

The recommended procedure for enabling certificate-based authentication is described below:

Procedure

Step 1 Add the Expressway's trusted CA and server certificate files (on the **Trusted CA certificate** and **Server certificate** pages, respectively).

Step 2 Configure certificate revocation lists (on the **CRL management** page).

Step 3 Use the **Client certificate testing** page to verify that the client certificate you intend to use is valid.

Step 4 Set **Client certificate-based security** to *Certificate validation* (on the **System administration** page).

Step 5 Restart the Expressway.

Step 6 Use the **Client certificate testing** page again to set up the required regex and format patterns to extract the username credentials from the certificate.

Step 7 Only when you are sure that the correct username is being extracted from the certificate, set **Client certificate-based security** to *Certificate-based authentication*.

Authentication Versus Authorization

When the Expressway is operating in certificate-based authentication mode, user authentication is managed by a process external to the Expressway.

When a user attempts to log in to the Expressway, the Expressway will request a certificate from the client browser. The browser may then interact with a card reader to obtain the certificate from the smart card (or alternatively the certificate may already be loaded into the browser). To release the certificate from the card/browser, the user will typically be requested to authenticate themselves by entering a PIN. If the client certificate received by the Expressway is valid (signed by a trusted certificate authority, in date and not revoked by a CRL) then the user is deemed to be authenticated.

To determine the user's authorization level (read-write, read-only and so on) the Expressway must extract the user's authorization username from the certificate and present it to the relevant local or remote authorization mechanism.

Note If the client certificate is not protected (by a PIN or some other mechanism) then unauthenticated access to the Expressway may be possible. This lack of protection may also apply if the certificates are stored in the browser, although some browsers do allow you to password protect their certificate store.

Obtaining the Username from the Certificate

The username is extracted from the client browser's certificate according to the patterns defined in the **Regex** and **Username format** fields on the **Certificate-based authentication configuration** page:

- In the **Regex** field, use the (**?<name>regex**) syntax to supply names for capture groups so that matching sub-patterns can be substituted in the associated **Username format** field, for example,

  /(Subject:.*, CN=(?<Group1>.*))/m.

  The regex defined here must conform to *PHP regex guidelines*.

- The **Username format** field can contain a mixture of fixed text and the capture group names used in the **Regex**. Delimit each capture group name with **#**, for example, **prefix#Group1#suffix**. Each capture group name will be replaced with the text obtained from the regular expression processing.

You can use the Testing Client Certificates page to test the outcome of applying different **Regex** and **Username format** combinations to a certificate.

Emergency Account and Certificate-Based Authentication

Advanced account security mode requires that you use only remote authentication, but also mandates that you have an emergency account in case the authentication server is unavailable. See Configuring Advanced Account Security Mode.

If you are using certificate-based authentication, the emergency account must be able to authenticate by presenting a valid certificate with matching credentials.

You should create a client certificate for the emergency account, make sure that the CN matches the **Username format**, and load the certificate into the emergency administrator's certificate store.

Managing the Trusted CA Certificate List

The **Trusted CA certificate** page (**Maintenance** > **Security** > **Trusted CA certificate**) allows you to manage the list of certificates for the Certificate Authorities (CAs) trusted by this Expressway. When a TLS connection to Expressway mandates certificate verification, the certificate presented to the Expressway must be signed by a trusted CA in this list and there must be a full chain of trust (intermediate CAs) to the root CA.

- To upload a new file containing one or more CA certificates, **Browse** to the required PEM file and click **Append CA certificate**. This will append any new certificates to the existing list of CA certificates. If you are replacing existing certificates for a particular issuer and subject, you have to manually delete the previous certificates.
- To replace all of the currently uploaded CA certificates with the system's original list of trusted CA certificates, click **Reset to default CA certificate**.

- To view the entire list of currently uploaded trusted CA certificates, click **Show all (decoded)** to view it in a human-readable form, or click **Show all (PEM file)** to view the file in its raw format.
- To view an individual trusted CA certificate, click on **View (decoded)** in the row for the specific CA certificate.
- To delete one or more CA certificates, tick the box(es) next to the relevant CA certificate(s) and click **Delete**.

Note If you have enabled certificate revocation list (CRL) checking for TLS encrypted connections to an LDAP server (for account authentication), you must add the PEM encoded CRL data to your trusted CA certificate file.

Root CAs included by default

Expressway X12.6 and later includes these trusted root CAs, which are installed as part of the *Cisco Intersection CA Bundle*:

- O=Internet Security Research Group, CN=ISRG Root X1
- O=Digital Signature Trust Co., CN=DST Root CA X3

Managing the Expressway Server Certificate

Use the **Server certificate** page (**Maintenance** > **Security** > **Server certificate**) to manage the Expressway server certificate, which identifies Expressway when it communicates with client systems using TLS encryption and with web browsers over HTTPS.

You can view details of the currently loaded certificate, generate a CSR, upload a new certificate, and configure the ACME service. These tasks are described in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway Configuration Guides page.

Note We strongly recommend using certificates based on RSA keys.

Other types of certificate, such as those based on DSA keys, are not tested and may not work with Expressway in all scenarios.

Using the ACME Service

From X12.5 the Cisco Expressway Series supports the ACME protocol (Automated Certificate Management Environment) which enables automatic certificate signing and deployment to the Expressway-E from a certificate authority such as Let's Encrypt.

Server Certificates and Clustered Systems

When a CSR is generated, a single request and private key combination is generated for that peer only. If you have a cluster of Expressways, you must generate a separate signing request on each peer. Those requests must then be sent to the certificate authority and the returned server certificates uploaded to each relevant peer.

Make sure that the correct server certificate is uploaded to the appropriate peer, otherwise the stored private key on each peer will not correspond to the uploaded certificate.

Server Certificates and Unified Communications

If you deploy Mobile and Remote Access, details about the Unified Communication and Expressway certificate requirements are in the *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway Configuration Guides page.

Managing Certificate Revocation Lists (CRLs)

Certificate revocation list files (CRLs) are used by the Expressway to validate certificates presented by client browsers and external systems that communicate with the Expressway over TLS/HTTPS. A CRL identifies those certificates that have been revoked and can no longer be used to communicate with the Expressway.

We recommend that you upload CRL data for the CAs that sign TLS/HTTPS client and server certificates. When enabled, CRL checking is applied for every CA in the chain of trust.

Certificate Revocation Sources

The Expressway can obtain certificate revocation information from multiple sources:

- Automatic downloads of CRL data from CRL distribution points.
- Through OCSP (Online Certificate Status Protocol) responder URIs in the certificate to be checked (SIP TLS only).
- Manual upload of CRL data.
- CRL data embedded within the Expressway's **Trusted CA certificate** file.

Limitations and Usage Guidelines

The following limitations and usage guidelines apply:

- When establishing SIP TLS connections, the CRL data sources are subject to the **Certificate revocation checking** settings on the **SIP** configuration page.
- Automatically downloaded CRL files override any manually loaded CRL files (except for when verifying SIP TLS connections, when both manually uploaded or automatically downloaded CRL data may be used).
- When validating certificates presented by external policy servers, the Expressway uses manually loaded CRLs only.

- When validating TLS connections with an LDAP server for remote login account authentication, the Expressway only uses CRL data that has been embedded into the **Trusted CA certificate** (**Tools** > **Security** > **Trusted CA certificate**).

  For LDAP connections, Expressway does not download the CRL from Certificate Distribution Point URLs in the server or issuing CA certificates. Also, it does not use the manual or automatic update settings on the **CRL management** page.

Automatic CRL Updates

Note We recommend that you configure the Expressway to perform automatic CRL updates. This ensures that the latest CRLs are available for certificate validation.

Procedure

Step 1 Go to **Maintenance** > **Security** > **CRL management**.

Step 2 Set **Automatic CRL updates** to *Enabled*.

Step 3 Enter the set of **HTTP(S) distribution points** from where the Expressway can obtain CRL files.

Note
- You must specify each distribution point on a new line
- Only HTTP(S) distribution points are supported; if HTTPS is used, the distribution point server itself must have a valid certificate
- PEM and DER encoded CRL files are supported
- The distribution point may point directly to a CRL file or to ZIP and GZIP archives containing multiple CRL files
- The file extensions in the URL or on any files unpacked from a downloaded archive do not matter as the Expressway will determine the underlying file type for itself; however, typical URLs could be in the format:
  - http://example.com/crl.pem
  - http://example.com/crl.der
  - http://example.com/ca.crl
  - https://example.com/allcrls.zip
  - https://example.com/allcrls.gz

Step 4 Enter the **`Daily update time`** (in UTC). This is the approximate time of day when the Expressway will attempt to update its CRLs from the distribution points.

Step 5 Click **Save**.

Manual CRL Updates

You can upload CRL files manually to the Expressway. Certificates presented by external policy servers can only be validated against manually loaded CRLs.

Procedure

Step 1 Go to **Maintenance** > **Security** > **CRL management**.

Step 2 Click **Browse** and select the required file from your file system. It must be in PEM encoded format.

Step 3 Click **Upload CRL file**.

This uploads the selected file and replaces any previously uploaded CRL file.

Click **Remove revocation** list if you want to remove the manually uploaded file from the Expressway.

If a certificate authority's CRL expires, all certificates issued by that CA will be treated as revoked.

Online Certificate Status Protocol (OCSP)

The Expressway can establish a connection with an OCSP responder to query the status of a particular certificate.The Expressway determines the OCSP responder to use from the responder URI listed in the certificate being verified. The OCSP responder sends a status of “good”, “revoked” or “unknown” for the certificate.

The benefit of OCSP is that there is no need to download an entire revocation list. OCSP is supported for SIP TLS connections only. See below for information on how to enable OCSP.

Outbound communication from the Expressway-E is required for the connection to the OCSP responder. Check the port number of the OCSP responder you are using (typically this is port 80 or 443) and ensure that outbound communication is allowed to that port from the Expressway-E.

Configuring Revocation Checking for SIP TLS Connections

You must also configure how certificate revocation checking is managed for SIP TLS connections.

1. Go to **Configuration** > **SIP**.
2. Scroll down to the **Certificate revocation checking** section and configure the settings accordingly:

Field	Description	Usage Tips
Certificate revocation checking mode	Controls whether revocation checking is performed for certificates exchanged during SIP TLS connection establishment.	We recommend that revocation checking is enabled.

Field	Description	Usage Tips
Use OCSP	Controls whether the Online Certificate Status Protocol (OCSP) may be used to perform certificate revocation checking.	To use OCSP: • The X.509 certificate to be checked must contain an OCSP responder URI. • The OCSP responder must support the SHA-256 hash algorithm. If it is not supported, the OCSP revocation check and the certificate validation will fail.
Use CRLs	Controls whether Certificate Revocation Lists (CRLs) are used to perform certificate revocation checking.	CRLs can be used if the certificate does not support OCSP. CRLs can be loaded manually onto the Expressway, downloaded automatically from preconfigured URIs (see Managing Certificate Revocation Lists (CRLs)), or downloaded automatically from a CRL distribution point (CDP) URI contained in the X.509 certificate.
Allow CRL downloads from CDPs	Controls whether the download of CRLs from the CDP URIs contained in X.509 certificates is allowed.	
Fallback behavior	Controls the revocation checking behavior if the revocation status cannot be established, for example if the revocation source cannot be contacted. *Treat as revoked*: Treat the certificate as revoked (and thus do not allow the TLS connection). *Treat as not revoked*: Treat the certificate as not revoked. Default: *Treat as not revoked*	*Treat as not revoked* ensures that your system continues to operate in a normal manner if the revocation source cannot be contacted, however it does potentially mean that revoked certificates will be accepted.

Managing mTLS Client Certificate Verification for MRA Onboarding

The **CA certificate page for mTLS** is accessed from the **Trusted CA certificate** page (**Maintenance** > **Security** > **Trusted CA certificate**). This page only applies if you use Expressway for Mobile and Remote Access (MRA) with Cisco Unified Communications products, and onboarding with activation codes is enabled for MRA.

Testing Client Certificates

The **Client certificate testing** page (**Maintenance** > **Security** > **Client certificate testing**) is used to check client certificates before enabling client certificate validation. You can:

- Test whether a client certificate is valid when checked against the Expressway's current trusted CA list and, if loaded, the revocation list (see Managing Certificate Revocation Lists (CRLs)).
- Test the outcome of applying the regex and template patterns that retrieve a certificate's authorization credentials (the username).

You can test against a certificate on your local file system or the browser's currently loaded certificate.

To test if a certificate is valid

Procedure

Step 1 Select the **Certificate source**. You can choose to:

- Upload a test file from your file system in either PEM or plain text format; if so click **Browse** to select the certificate file you want to test
- Test against the certificate currently loaded into your browser (only available if the system is already configured to use *Certificate validation* and a certificate is currently loaded)

Step 2 Ignore the **Certificate-based authentication pattern** section - this is only relevant if you are extracting authorization credentials from the certificate.

Step 3 Click **Check certificate**.
The results of the test are shown in the **Certificate test results** section.

To retrieve authorization credentials (username) from the certificate

Procedure

Step 1 Select the **Certificate source** as described above.

Step 2 Configure the **Regex and Username format** fields as required. Their purpose is to extract a username from the nominated certificate by supplying a regular expression that will look for an appropriate string pattern within the certificate. The fields default to the currently configured settings on the **Certificate-based authentication configuration** page but you can change them as required.

- In the **Regex** field, use the (**?<name>regex**) syntax to supply names for capture groups so that matching sub patterns can be substituted in the associated **Username format** field, for example,

  /(Subject:.*, CN=(?<Group1>.*))/m.

  The regex defined here must conform to PHP regex guidelines.

- The **Username format** field can contain a mixture of fixed text and the capture group names used in the **Regex**. Delimit each capture group name with #, for example, **prefix#Group1#suffix**. Each capture group name will be replaced with the text obtained from the regular expression processing.

Step 3 Click **Check certificate**.
The results of the test are shown in the **Certificate test results** section. The **Resulting string** item is the username credential that would be checked against the relevant authorization mechanism to determine that user's authorization (account access) level.

Step 4 If necessary, you can modify the **Regex** and **Username format** fields and repeat the test until the correct results are produced.

Note If the **Certificate source** is an uploaded PEM or plain text file, the selected file is temporarily uploaded to the Expressway when the test is first performed:

- If you want to keep testing different **Regex** and **Username format** combinations against the same file, you do not have to reselect the file for every test.
- If you change the contents of your test file on your file system, or you want to choose a different file, you must click **Browse** again and select the new or modified file to upload.

Step 5 If you have changed the **Regex** and **Username format** fields from their default values and want to use these values in the Expressway's actual configuration (as specified on the **Certificate-based authentication configuration** page) then click **Make these settings permanent**.

Note
- Any uploaded test file is automatically deleted from the Expressway at the end of your login session.
- The regex is applied to a plain text version of an encoded certificate. The system uses the command **openssl x509 -text -nameopt RFC2253 -noout** to extract the plain text certificate from its encoded format.

Testing Secure Traversal

This utility tests whether a secure connection can be made from the Expressway-C to the Expressway-E. A secure connection is required for a Unified Communications traversal zone, and is optional (recommended) for a normal traversal zone.

If the secure traversal test fails, the utility raises a warning with appropriate resolution where possible.

Procedure

Step 1 On the Expressway-C, go to **Maintenance** > **Security** > **Secure traversal test**.

Step 2 Enter the FQDN of the Expressway-E that is paired with this Expressway-C.

Step 3 Enter the TLS verify name of this Expressway-C, as it appears on the paired Expressway-E.

This setting is in the SIP section of the Expressway-E's traversal zone configuration page.

Step 4 Click **Test connection**.

The secure traversal test utility checks whether the hosts on either side of the traversal zone recognize each other and trust each others' certificate chains.

Note You must select the version of **HTTPS minimum TLS version** to test the applicability of a secure connection that enables the minimum supported TLS version by Expressway. Also, select the **HTTPS ciphers** for the same. This selection of *HTTPTLSversion* is required for connection establishment towards Unified Communication servers like VCSE, CUCM, CUP, and UCXN. These settings are configured on the **Ciphers** page (**Maintenance** > **Security** > **Ciphers**).

Managing the Expressway Server Certificate with HSM

Important HSM functionality support on Expressway may be a **Preview feature only**, depending on the Expressway software version. For example, it is a Preview feature in version X12.6. Please check the release notes for your Expressway version before you use HSM and if its status is Preview for your software version, **only enable HSM if you are willing to implement it as a Preview feature and subject to the Preview disclaimer contained in the Expressway Release Notes**. Instructions for how to configure and enable HSM are currently provided only in the Expressway Release Notes.

These instructions assume that HSM is already enabled on Expressway (**Maintenance** > **Security** > **HSM configuration**).

Procedure

Step 1 Go to **Maintenance** > **Security** > **Server certificate**.

Step 2 Click **Generate CSR**. You are navigated to the **Generate CSR** page.

The **Server certificate type** section displays at the top of the **Generate CSR** page. If HSM usage is not configured, the section does not display.

If you have an Expressway cluster, issues may arise if the CSR fields are incorrectly completed. For details on how to fill these fields, see the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide* on the Cisco Expressway Series Configuration Guides page.

Step 3 After generating as HSM private key and CSR, you are returned to the **Server certificate** page.

Step 4 You can view and download the generated HSM CSR from the **Certificate signing request (CSR)** section.

Step 5 Click **Download** to download the certificate.

Step 6 Sign the certificate using certificate signing authority.

Install the HSM private key and certificate

Note Only use these instructions if you use Hardware Security Module (HSM) functionality.

Procedure

Step 1 To upload a signed certificate, click **Choose File** to navigate to the location and choose the certificate.

Step 2 Select a certificate file and corresponding certificate type, and click **Upload server certificate** data to upload the certificate.

For more information, see the section about managing the Expressway's server certificate.

Download the HSM key handle across a cluster

After deploying an HSM certificate and private key to an Expressway, the HSM certificate and private key can be deployed to other Expressways in a cluster. To do this:

Procedure

Step 1 On the primary peer. Download the HSM private key from the first Expressway. After deploying an HSM certificate and private key, a **Download HSM key handle** button displays on the **Server certificate data** section.

Step 2 On the cluster peers. Upload the HSM private key with HSM certificate to other peers in the cluster from the **Upload new certificate** section. Browse to and select the signed HSM certificate and private key.

Restart Expressway

After an HSM certificate is installed on Expressway, a banner on the **Server certificate** page prompts you to restart Expressway. An alarm is also raised to restart. Although the certificate is now installed, the restart is required for the Expressway to begin using it.

After the restart, the alarm disappears and all services on the Expressway use the new HSM certificate.

Configuring Hardware Security Module Functionality

The **HSM configuration** page (**Maintenance** > **Security** > **HSM configuration**) is used to manage HSM devices with Expressway.

Important HSM functionality may be a **Preview feature only**, depending on the Expressway software version. For example, it is a Preview feature in version X12.6. Please check the release notes for your Expressway version before you use HSM and if its status is Preview for your software version, only enable HSM if you are willing to implement it as a Preview feature. Instructions for how to configure HSM are currently provided only in the Expressway release notes and not in this section.

Configuring Minimum TLS Version and Cipher Suites

The **Maintenance** > **Security** > **Ciphers** page is used to manage the minimum TLS version for services on Expressway, and their associated cipher suites.

Note For improved security, TLS version 1.2 or later is recommended for all encrypted sessions.

Expressway defaults to TLS 1.2 when establishing secure connections for the following:

- HTTPS
- Certificate checker
- Cisco Meeting Server discovery
- SIP
- XMPP
- UC server discovery
- Reverse proxy
- LDAP
- SMTP mail server
- TMS Provisioning Service

Restart required in some cases

A restart is required after changing the cipher suite configuration or TLS protocol version for the following:

- SIP
- XCP

Minimum TLS Version

On upgrade of an existing system, the previous behavior and defaults persist so you won't be defaulted to TLS 1.2.

For new installations, check that all browsers and other equipment that must connect to Expressway support TLS 1.2.

If required--typically for compatibility reasons with legacy equipment--the minimum TLS versions can be configured per service to use versions 1.0 or 1.1.

Cipher Suites

You can configure the cipher suite and minimum supported TLS version for services on the Expressway. The cipher suites are shown in the table (cipher strings are in OpenSSL format):

For services where the Expressway can act as a client, such as HTTPS, the same minimum TLS version and cipher suites will be negotiated.

Services	Cipher Suite Values (Defaults)
HTTPS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
Reverse proxy TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
SIP TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH
UC server discovery TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
XMPP TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
LDAP TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
TMS TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
SMTP ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL

SIP behavior—disable ADH recommendation

Some endpoints, for example the E20, only support Anonymous Diffie-Hellman (ADH) when you connect to them, so ADH is enabled in the default cipher suites. However, if it's an inbound connection, for security reasons you should always add `!ADH` to disable it.

Be aware that removing the ADH from SIP will cause the outbound connections to some legacy endpoints to fail.

Configuring SSH

Tunnel Configuration

The Expressway pair uses SSH tunnels to securely transfer data from the Expressway-E to the Expressway-C without requiring Expressway-E to open the connection. The Expressway-C opens a TCP session with the Expressway-E which is listening on a fixed TCP port. The pair then use the selected cipher and algorithms to establish an encrypted tunnel for securely sharing data.

The cipher and algorithms that the pair use to encrypt SSH tunnels are configured as follows:

1. Go to **Maintenance** > **Security** > **SSH configuration**.
2. Modify the following settings, if necessary:

Setting	Description
Ciphers	*aes256-ctr*: Advanced Encryption Standard using the CTR (counter) mode to encipher 256-bit blocks. (Default)
Public Key Algorithms	*X509v3-sign-rsa* (Default) *X509v3-ssh-rsa*
Key Exchange Algorithms	*ecdh-sha2-nistp256* *ecdh-sha2-nistp384*(Default)

3. Click **Save**.

Remote Access Configuration

The cipher and algorithms that the pair use to encrypt remote access between a SSH client and server are configured as follows:

1. Go to **Maintenance** > **Security** > **SSH configuration**.
2. Modify the following settings, if necessary:

Setting	Description
Ciphers	*"aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr"*
Key Exchange Algorithms	*"ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1"*
MAC Algorithms	*"hmac-sha2-512,hmac-sha2-256,hmac-sha1"*

3. Click **Save**.

Advanced Security

The **Advanced security** page (**Maintenance** > **Advanced security**) is used to configure the Expressway for use in highly secure environments. You need to install the **Advanced Account Security** option key to see this page.

You can configure the system for:

- Configuring Advanced Account Security Mode
- Configuring FIPS140-2 Cryptographic Mode

Configuring Advanced Account Security Mode

Enabling advanced account security limits login access to remotely authenticated users using the web interface only, and also restricts access to some system features. To indicate that the Expressway is in advanced account security mode, any text specified as the **Classification banner** message is displayed on every web page.

A system reboot is required for changes to the advanced account security mode to take effect.

HTTP methods

The Expressway web server allows the following HTTP methods:

Method	Used by Web UI?	Used by API?	Used to...
GET	Yes	Yes	Retrieve data from a specified resource. For example, to return a specific page in the Expressway web interface.
POST	Yes	Yes	Apply data to a web resource. For example, when an administrator saves changes to a setting using the Expressway web interface.
OPTIONS	No	Yes	For a specified URL, returns the HTTP methods supported by the server. For example, the Expressway can use OPTIONS to test a proxy server for HTTP/1.1 compliance.
PUT	No	Yes	Send a resource to be stored at a specified URI. Our REST API commands use this method to change the Expressway configuration.
DELETE	No	Yes	Delete a specified resource. For example, the REST API uses DELETE for record deletion.

How to disable user access to the API

Administrators have API access by default. This can be disabled in two ways:

- If the Expressway is running in advanced account security mode, then API access is automatically disabled for all users.

- API access for individual administrators can be disabled through their user configuration options.

Prerequisites

Before you can enable advanced account security mode, the following items are required:

- The system must be configured to use remote account authentication for administrator accounts.
- The **Advanced Account Security** option key must be installed.
- You must create a local administrator account and nominate it as the emergency account, so that you can get in if remote authentication is unavailable. You cannot use a remote account for this purpose.

  Do not use the built in *admin* account.

Caution The Expressway will disallow local authentication by all accounts except the emergency account. Ensure that the remote directory service is working properly before you enable the mode.

You are also recommended to configure your system so that:

- SNMP is disabled.
- The session time out period is set to a non-zero value.
- HTTPS client certificate validation is enabled.
- User account LDAP server configuration uses TLS encryption and has certificate revocation list (CRL) checking set to *All*.
- Remote logging is disabled.
- Incident reporting is disabled.
- Any connection to an external manager uses HTTPS and has certificate checking enabled.

Alarms are raised for any non-recommended configuration settings.

Enabling Advanced Account Security

To enable advanced account security:

Procedure

Step 1 Go to **Maintenance** > **Advanced security**.

Step 2 Enter a `Classification banner`.

The text entered here is displayed on every web page.

Step 3 Set **Advanced account security mode** to *On*.

Step 4 Click **Save**.

Step 5 Reboot the Expressway (**Maintenance** > **Restart options**).

Expressway Functionality: Changes and Limitations

When in secure mode, the following changes and limitations to standard Expressway functionality apply:

- Access over SSH and through the serial port is disabled and cannot be turned on (the pwrec password recovery function is also unavailable).
- Access over HTTPS is enabled and cannot be turned off.
- The command line interface (CLI) and API access are unavailable.
- Administrator account authentication source is set to *Remote only* and cannot be changed.
- Local authentication is disabled. There is no access using the root account or any local administrator account except the emergency account.
- Only the emergency account may change the emergency account.
- If you are using certificate-based authentication, the emergency account must be authenticated by credentials in the client's certificate. See Emergency Account and Certificate-Based Authentication.
- If there are three consecutive failed attempts to log in (by the same or different users), login access to the Expressway is blocked for 60 seconds.
- Immediately after logging in, the current user is shown statistics of when they previously logged in and details of any failed attempts to log in using that account.
- Administrator accounts with read-only or read-write access levels cannot view the Event Log, Configuration Log and Network Log pages. These pages can be viewed only by accounts with *Auditor* access level.
- The **Upgrade** page only displays the **System platform** component.

The Event Log, Configuration Log, Network Log, call history, search history and registration history are cleared whenever the Expressway is taken out of advanced account security mode.

Note If intrusion protection is enabled, this will cause any existing blocked addresses to become unblocked.

Disabling Advanced Account Security

Note This operation wipes all configuration. You cannot maintain any configuration or history when exiting this mode. The system returns to factory state.

Procedure

Step 1 Sign in with the emergency account.

Step 2 Disable Advanced Account Security mode (**Maintenance** > **Advanced security**).

Step 3 Sign out.

Step 4 Connect to the console.

Step 5 Sign in as **root** and run **factory-reset**.

See Restoring the Default Configuration (Factory Reset) for details.

Configuring FIPS140-2 Cryptographic Mode

FIPS140 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. FIPS140-1 became a mandatory standard for the protection of sensitive data in 1994 and was superseded by FIPS140-2 in 2001. Expressway X8.8 or later implements FIPS140-2 compliant features.

When in FIPS140-2 cryptographic mode, system performance may be affected due to the increased cryptographic workload.

You can cluster Expressways that have FIPS140-2 mode enabled.

Prerequisites

Before you enable FIPS140-2 mode:

- Ensure that the system is not using NTLM protocol challenges with a direct Active Directory Service connection for device authentication; NTLM cannot be used while in FIPS140-2 mode.
- If login authentication via a remote LDAP server is configured, ensure that it uses TLS encryption if it is using SASL binding.
- The **Advanced Account Security** option key must be installed.

FIPS140-2 compliance also requires the following restrictions:

- System-wide SIP transport mode settings must be TLS: *On*, TCP: *Off* and UDP: *Off*.
- All SIP zones must use TLS.
- SNMP and NTP server connections should use strong hashing and encryption. Use these settings:

  System > **SNMP** > **v3 Authentication** > **Type** = *SHA*

  System > **SNMP** > **v3 Privacy** > **Type** = *AES*

  System > **Time** > **NTP server *n*** > **Authentication=** *Symmetric key*

  System > **Time** > **NTP server *n*** > **Hash=** *SHA-1*

If your system is running as a virtualized application and has never been through an upgrade process, perform a system upgrade before you continue. You can upgrade the system to the same software release version that it is currently running. If you do not complete this step, the activation process described below will fail.

Enable FIPS 140-2 Cryptographic Mode

Caution The transition to FIPS 140-2 cryptographic mode requires a system reset to be performed. This will remove all existing configuration data. To preserve your data you should take a backup immediately prior to performing the reset, and then restore the backup file when the reset has completed.

The reset removes all administrator account information and reinstates the default security certificates. To log in after the reset has completed you will have to first complete the Install Wizard.

To turn your system into a compliant FIPS 140-2 cryptographic system:

Procedure

Step 1 Enable FIPS 140-2 cryptographic mode:

a. Go to **Maintenance** > **Advanced security**.

b. Set **FIPS 140-2 cryptographic mode** to *On*.

c. Click **Save**.

Step 2 Fix any alarms that have been raised that report non-compliant configuration.

Note When you enable FIPS in a Mobile and Remote Access scenario, if alarm #40042 (some SIP configuration is not using TLS transport; FIPS 140-2 compliance requires TLS) is raised you can disable and enable this feature to clear the alarm.

Step 3 Take a system backup if you want to preserve your current configuration data.

Note Ensure that all backups require password protection.

Step 4 Reset the system and complete the activation of FIPS140-2 mode:

a. Log in to Expressway as **root**.

b. Type **`fips-activate`**.

The reset takes up to 30 minutes to complete.

Step 5 Follow the prompts to complete the Install Wizard.

Step 6 When the system has applied the configuration and restarted, log in as **`admin`** using the password you set.

You may see alarms related to non-compliance with FIPS 140-2. Ignore these alarms if you intend to restore the backup taken prior to the reset. You must take action if they persist after restoring the backup.

Step 7 Restore your previous data, if required.

Note While in FIPS 140-2 mode, you can only restore backup files that were taken when **FIPS 140-2 cryptographic mode** is set to *On*. Any previous administrator account information and passwords will be restored however, the previous **root** account password is not restored. If the data you are restoring contains untrusted security certificates, the restart that occurs as part of the restore process may take up to 6 minutes to complete.

Step 8 From X12.6 you must manually change the SIP TLS Diffie-Hellman key size from the default 1024 bits, to at least 2048. To do this type the following command in the Expressway command line interface (change the value in the final element if you want a key size higher than 2048): *xconfiguration SIP Advanced SipTlsDhKeySize: "2048"*

FIPS140-2 Compliant Features

The following Expressway features are FIPS140-2 compliant / use FIPS140-2 compliant algorithms:

- Administration over the web interface
- Clustering
- XML and REST APIs
- SSH access (restricted to only use AES or 3DES ciphers)
- Login authentication via a remote LDAP server (must use TLS if using SASL binding)
- Client certificate verification
- SIP certificate revocation features
- SNMP (SNMPv3 authentication is restricted to SHA1, and SNMPv3 privacy is restricted to AES)
- NTP (NTP server authentication using symmetric key is restricted to SHA1)
- Device authentication against the local database
- SIP connections to/from the Expressway providing they use TLS
- H.323 connections to/from the Expressway
- Delegated credential checking
- SRTP media encryption
- SIP/H.323 interworking
- Unified Communications Mobile and Remote Access (MRA)
- TURN server authentication
- Backup/restore operations
- Connections to an external manager
- Connections to external policy services
- Remote logging
- Incident reporting
- CSR generation

Other Expressway features are not FIPS140-2 compliant, including:

- SIP authentication over NTLM / Active Directory
- SIP/H.323 device authentication against an H.350 directory service

- Microsoft Interoperability service
- Use of Cisco TMSPE