Maintenance

Enable Maintenance Mode

Maintenance mode is typically used when you need to upgrade or take out of service an Expressway peer that is part of a cluster. It allows the other cluster peers to continue to operate normally while the peer that is in maintenance mode is upgraded or serviced. Putting a peer into maintenance mode provides a controlled method of stopping any further registrations or calls from being managed by that peer.

An alarm is raised while the peer is in maintenance mode. You can monitor the **Resource usage** page (**Status** > **System** > **Resource usage**) to check how many registrations and calls are currently being handled by that peer.

When a peer is in maintenance mode, its workload is handled by the other cluster nodes. For large multitenant deployments or MRA deployments therefore, we recommend that you only enable maintenance mode on one peer at a time, to avoid overloading the other nodes.

Impact on Active Calls and Registrations

Standard Expressway sessions (not MRA)

- New calls and registrations will be handled by another peer in the cluster.

- Existing registrations are allowed to expire and then should reregister to another peer (see *Expressway Cluster Creation and Maintenance Deployment Guide* for more information about endpoint configuration and setting up DNS SRV records).
- Existing calls continue until the call is terminated.

Unified CM MRA sessions

Expressway stops accepting new calls or proxy (MRA) traffic. Existing calls and chat sessions are not affected.

As users end their sessions normally, the system comes to a point when it is not processing any traffic of a certain type, and then it shuts that service down.

If users try to make new calls or start new chat sessions while the Expressway is in maintenance mode, the clients will receive a service unavailable response, and they might then choose to use another peer (if they are capable). This fail-over behavior depends on the client, but restarting the client should resolve any connection issues if there are active peers in the cluster.

The Unified Communications status pages also show (*Maintenance Mode*) in any places where MRA services are affected.

Process to Enable Maintenance Mode

1. Log to in the relevant peer.
2. Go to the **Maintenance mode** page **Maintenance** > **Maintenance mode**.
3. Set **Maintenance mode** to *On*.
4. Click **Save** and Click **Ok** on the confirmation dialog.

Note Maintenance mode is automatically disabled if the peer is restarted.

How to Manually Remove Calls or Registrations

To manually remove any calls or registrations that don't clear automatically:

- Go to **Status** > **Calls**, click **Select all** and then click **Disconnect** (SIP calls may not disconnect immediately).
- Go to **Status** > **Registrations** > **By device**, click **Select all** and then click **Unregister**.

You can leave the Conference Factory registration. This will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration (if enabled).

Enabling SSH Access to Expressway

You may want to enable SSH access to the Expressway so that you can access it securely without requiring password-based login. One common reason for this is to improve the efficiency of monitoring and logging. You will need to repeat this procedure on each Expressway that you want to access in this way.

Caution You will use root access to authorize your public key. Take care not to increase your security exposure or cause any unsupported configuration. We strongly discourage using `root`.

Step 1 Use SSH to log in as `root`.

Step 2 Enter `mkdir /tandberg/.ssh` to create `.ssh` directory if it is not already present.

Step 3 Copy your public key to `/tandberg/.ssh`.

Step 4 Append your public key to the `authorized_keys` file with `cat /tandberg/.ssh/ id_rsa.pub >> /tandberg/.ssh/authorized_keys`.

Where *id_rsa.pub* is substituted with the name of your public key. Do not place your key anywhere else because the key could be lost on upgrade (`authorized_keys` file does persist)

Step 5 Log off and test SSH access using your own key

If you cannot access the Expressway with your key, you may need to connect as `root` and restart the SSH daemon with `/etc/init.d/sshd restart`.

Upgrading Expressway Software

This section describes how to install new releases of Expressway software components onto an existing system. Component upgrades can be performed in one of two ways:

- **Using the Web Interface** - Recommended approach using the **Maintenance** > **Upgrade** page.
- **Using Secure Copy** (SCP/PSCP) - Alternative approach. This method may be useful in specific cases such as with a slow or unstable network connection.
- **Using APIs** – Only single node upgrade is supported as of now. So, we are introducing another alternative approach which is useful in specific cases of automated deployment. For upgrading a clustered system, start with the primary peer.

Downgrading Support

Downgrading to an older version is NOT supported.

Upgrading Using Web Interface

Upgrading Expressway

This section describes how to install the software on Expressway using the web user interface, which is the method we recommend. If you prefer to use a secure copy program such as SCP or PSCP to do the install, please use the *Cisco Expressway Administrator Guide* instead.

Summary

Table 1: Summary of tasks in a typical upgrade process

Stage	Task	Where
1	Review the *Prerequisites and Software Dependencies* and *Before You Begin* sections below	Release Notes
2	Back up the system	**Maintenance** > **Backup and restore**
3	Enable maintenance mode and wait for current calls and registrations to end	**Maintenance** > **Maintenance mode**
4	Upload the new software image (**"Upgrade"** option)	**Maintenance** > **Upgrade**
5	Install the new software ("**Continue with upgrade**" option)	**Maintenance** > **Upgrade**
6	Reboot	From the **Upgrade** page
7	In clustered deployments repeat for each peer in sequence	-

Prerequisites and Software Dependencies

This section has important information about issues that may prevent the system working properly after an upgrade. Before you upgrade, please review this section and complete any tasks that apply to your deployment.

Expressway and Cisco VCS systems before X8.11.4 need a two-stage upgrade

If you are upgrading a system which is running software earlier than version X8.11.4, you must first upgrade to an **intermediate release** before you install X14.2 software (this requirement applies to all upgrades X8.11.x and later versions). Depending on the existing system version, the upgrade will fail. We recommend upgrading to X8.11.4 as the intermediate release.

All deployments

If you are upgrading from X12.6 or X12.6.1 and use the alarm-based email notifications feature

Note In X12.6.2 the email ID length is limited to 254 characters maximum. Before you upgrade make sure that all destination email IDs are no longer than 254 characters.

We do not support downgrades. Do not install a previous Expressway/Cisco VCS version onto a system that is running a newer version; the system configuration will be lost.

Note From X8.11.x, when the system restarts after the upgrade it uses a new encryption mechanism. This is due to a unique root of trust for every software installation that was introduced in that release.

X8.8 and later versions are more secure than earlier versions. Upgrading could cause your deployments to stop working as expected, and you must check for the following environmental issues before you upgrade to X8.8 or later:

- **Certificates**: Because certificate validation was tightened up in X8.8, you must verify the following items to avoid validation failures:
  - Try the secure traversal test before and after upgrade (**Maintenance** > **Security** > **Secure traversal test**) to validate TLS connections.
  - If Unified Communications nodes are deployed, do they use valid certificates that were issued by a CA in the Expressway-C/Cisco VCS Control trust list?
  - If you use self-signed certificates, are they unique? Does the trusted CA list on Expressway/Cisco VCS have the self-signed certificates of all the nodes in your deployment?
  - Are all entries in the Expressway/Cisco VCS trusted CA list unique? Remove any duplicates.
  - If **TLS verify mode** is enabled on connections to other infrastructure (always on by default for Unified Communications traversal zone, and optional for zones to Unified Communications nodes), make sure that the hostname is present in the CN or SAN field of the host's certificate. We do not recommend disabling TLS verify mode, even though it may be a quick way to resolve a failing deployment.
- **DNS entries**: Do you have forward and reverse DNS lookups for all infrastructure systems that the Expressway/Cisco VCS interacts with? From X8.8, you need forward and reverse DNS entries for all Expressway-E/Cisco VCS Expressway systems, so that systems making TLS connections to them can resolve their FQDNs and validate their certificates. If the Expressway/Cisco VCS cannot resolve system hostnames and IP addresses, complex deployments like MRA may not work as expected after the upgrade.
- **Cluster peers**: Do they have valid certificates? If they are using default certificates you should replace them with (at least) internally generated certificates and update the peers trust lists with the issuing CA. From X8.8, clustering communications use TLS connections between peers instead of IPSec. By default, TLS verification is not enforced after the upgrade, and an alarm will remind you to enforce it.

How and when rebooting is necessary as part of the upgrade

Upgrading the *System platform* component is a two-stage process. First, the new software image is uploaded onto the Expressway/Cisco VCS. At the same time, the current configuration of the system is recorded, so that this can be restored after the upgrade. During this initial stage the system will continue running on its existing software version, and all normal system processes will continue.

The second part of the upgrade involves rebooting the system. It is only during the reboot that the Expressway/Cisco VCS installs the new software version and restores the previous configuration. Rebooting causes all current calls to terminate, and all current registrations to be ended. This means that you can upload the new software at any time, and then wait until a convenient moment (for example, when no calls are taking place) to switch to the new version by rebooting the system. Any **configuration changes made between the software upload and the reboot will be lost when the system restarts** with the new software version.

Upgrades for components other than the *System platform* do not involve a system reboot, although the services provided by that component are temporarily stopped while the upgrade process completes.

Deployments that use MRA

This section only applies if you use the Expressway/Cisco VCS for MRA (mobile and remote access with Cisco Unified Communications products).

- Minimum versions of Unified Communications infrastructure software apply - some versions of Unified CM, IM and Presence Service, and Cisco Unity Connection have been patched with CiscoSSL updates. Before you upgrade Expressway/Cisco VCS check that you are running the minimum versions listed in the *Mobile and Remote Access Through Expressway Deployment Guide*.

  IM and Presence Service 11.5 is an exception. You must upgrade Expressway/Cisco VCS to X8.8 or later before you upgrade IM and Presence Service to 11.5.

- Expressway-C/Cisco VCS Control and Cisco Expressway-E/VCS Expressway **should both be upgraded** in the same upgrade "window"/timescale (this is also a general recommendation for non-MRA deployments). We don't recommend operating with Expressway-C/Cisco VCS Control and Expressway-E/Cisco VCS Expressway on different versions for an extended period.

- This item applies if you are upgrading a Expressway/Cisco VCS that is used for MRA, with clustered Unified CMs and endpoints running TC or Collaboration Endpoint (CE) software. In this case you must install the relevant TC or CE maintenance release listed below (or later) before you upgrade the Expressway/Cisco VCS. This is required to avoid a known problem with failover. If you do not have the recommended TC/CE maintenance release, an endpoint will not attempt failover to another Unified CM if the original Unified CM to which the endpoint registered fails for some reason. Bug ID CSCvh97495 refers.

  - TC7.3.11
  - CE8.3.3
  - CE9.1.2

From X8.10.x, the MRA authentication (access control) settings are configured on Expressway-C/Cisco VCS Control and not on Expressway-E/Cisco VCS Expressway as in earlier releases, and default values are applied if it is not possible to retain the existing settings. To ensure correct system operation, after the upgrade reconfigure the access control settings on the Expressway/Cisco VCS, as described later in these instructions.

Deployments that use FIPS mode cryptography

If the Expressway/Cisco VCS has FIPS mode enabled, after the upgrade, manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater, as described later in these instructions.

Deployments that use X8.7.x or earlier with Cisco Unified Communications Manager IM and Presence Service 11.5(1)

X8.7.x (and earlier versions) of Expressway/Cisco VCS are not interoperable with Cisco Unified Communications Manager IM and Presence Service 11.5(1) and later. This is caused by a deliberate change in that version of IM and Presence Service, which has a corresponding change in Expressway/Cisco VCS X8.8 and later. To ensure continuous interoperability, upgrade the Expressway/Cisco VCS systems before you upgrade the IM and Presence Service systems. The following error on Expressway/Cisco VCS is a symptom of this issue: `Failed Unable to Communicate with <IM&P node address>. AXL query HTTP error "'HTTPError:500'"`

Deployments that use Cisco Webex Hybrid Services

The Management Connector must be up to date before you upgrade Expressway/Cisco VCS. Authorize and accept any Management Connector upgrades advertised by the Cisco Webex cloud before you try to upgrade Expressway/Cisco VCS. Failure to do so may cause issues with the connector after the upgrade. For details about which versions of Expressway/Cisco VCS are supported for hybrid connector hosting, see Connector Host Support for Cisco Webex Hybrid Services.

Upgrade Instructions

Before You Begin

- Do the upgrade when the system has low levels of activity.
- A system upgrade needs a system reboot to complete the process. The reboot will terminate any active calls and registrations.
- For clustered systems, allocate enough time to upgrade all peers in the same upgrade "window". The cluster will not re-form correctly until the software versions match on all peers.
- Check the **Alarms** page (**Status** > **Alarms**) and make sure that all alarms are acted upon and cleared. Do this for each peer if you are upgrading a cluster.
- If you are upgrading a VM-based system, use the standard *.tar.gz* software image file. The *.ova* file is only needed for the initial install of Expressway software onto VMware.
- If you use the Expressway for MRA and you upgrade from X8.9.x or earlier to X8.10 or later, note your MRA authentication settings before you upgrade. From version X8.10 the MRA authentication (access control) settings moved from the Expressway-E to the Expressway-C. The upgrade does not preserve the existing Cisco Expressway-E settings, so after the upgrade you need to review them on the Expressway-C and adjust as necessary for your deployment. To access existing MRA authentication settings:

  a. On the Expressway-E, go to **Configuration** > **Unified Communications** > **Configuration** and locate **Single Sign-on support**.

  Note The existing value (On, Exclusive, or Off)

  b. If **Single Sign-on support** is set to *On* or *Exclusive*.

  Note The current values of these related fields:
  - Check for internal authentication availability.
  - Allow Jabber iOS clients to use embedded Safari.

- Make sure that all relevant tasks in Prerequisites and Software Dependencies are complete.

Upgrading Expressway-C and Expressway-E systems connected over a traversal zone

In all cases we recommend that Expressway-C (traversal client) and Expressway-E (traversal server) systems that are connected over a traversal zone **both run the same software version**. For some services such as Mobile and Remote Access, we *require* both systems to run the same version.

However, we do support a traversal zone link from one Expressway system to another that is running the previous feature release of Expressway (for example, from an X12.6 system to an X12.5 system). This means that you do not have to simultaneously upgrade your Expressway-C and Expressway-E systems.

Process to Upgrade a Standalone System

Note Do not use this process if you are upgrading a clustered Expressway/Cisco VCS; instead use the Process to Upgrade a Clustered System.

Step 1 Sign in to the Expressway/Cisco VCS web user interface as *admin*.

Step 2 Back up the Expressway/Cisco VCS system before you upgrade (**Maintenance** > **Backup and restore**).

Step 3 Enable maintenance mode so that Expressway/Cisco VCS does not process any new incoming calls (**Maintenance** > **Maintenance mode**). Existing calls continue until the call is terminated.

Step 4 Wait for all calls to clear and registrations to timeout.

To manually remove any calls or registrations that don't clear automatically, use the **Status** > **Calls** page or the **Status** > **Registrations** > **By device** page respectively (SIP calls may not clear immediately).

Note You can leave the registration for Conference Factory (if enabled) – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration.

Step 5 Go to **Maintenance** > **Upgrade** to access the **Upgrade** page.

Step 6 Click **Browse** and select the software image file for the component you want to upgrade.

The Expressway/Cisco VCS automatically detects which component you are upgrading based on the selected software image file.

Step 7 Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.

Step 8 For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:

a. Check the following details:

- **New software version** number is as expected.
- **MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you downloaded the software image file.

b. Click **Continue with upgrade**. This step installs the new software.

The **System upgrade** page opens and displays a progress bar while the software installs.

A summary of any active calls and registrations is displayed when the software completes installing (the calls and registrations will be lost when you reboot the system in the next step).

c. Click **Reboot system**. Any configuration changes made between uploading the software tar file and rebooting, will be lost when the system restarts.

   Sometimes the web browser interface times out during the restart process, after the progress bar reaches the end. This may occur if the Expressway/Cisco VCS carries out a disk file system check – approximately once every 30 restarts.

   After the reboot is complete the **Login** page is displayed.

Step 9 For upgrades to other components (not System platform) the software is automatically installed and no reboot is required.

What Next?

If you don't use MRA, the upgrade is now complete, and the Expressway configuration should be as expected. The **Overview** and **Upgrade** pages show the upgraded software version numbers.

If you do use MRA, and you are upgrading from X8.9.x or earlier, reconfigure your MRA access control settings as described in "Appendix 2: Post-Upgrade Tasks for MRA Deployments" in the *Mobile and Remote Access Deployment Guide*.

If you have components that require option keys to enable them, do this from the **Maintenance** > **Option keys** page.

If the Expressway has FIPS mode enabled (that is, it's a FIPS140-2 cryptographic system) then from X12.6 you must manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater. 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"***

This step does **not** apply to most systems. It only affects systems with advanced account security configured and FIPS enabled.

Process to Upgrade a Clustered System

Caution To avoid the risk of configuration data being lost and to maintain service continuity, UPGRADE THE PRIMARY PEER FIRST and then upgrade the subordinate peers ONE AT A TIME in sequence.

We recommend upgrading the Expressway-E cluster first, followed by the Expressway-C (in each case start with the primary peer). This ensures that when Expressway-C starts a new traversal session toward Expressway-E, the Expressway-E is ready to process it. Starting with the primary peer, upgrade the cluster peers in sequence as follows:

Step 1 Sign in to the Expressway/Cisco VCS web user interface as *admin*.

Step 2 Back up the Expressway/Cisco VCS before you upgrade (**Maintenance** > **Backup and restore**).

Note If the cluster peers are running different versions of the Expressway/Cisco VCS, do not make any configuration changes other than the settings required to upgrade. The cluster does not replicate any configuration changes to the subordinate peers that are running on different versions from the primary Expressway/Cisco VCS.

Step 3 Enable maintenance mode so that the peer does not process any new incoming calls (**Maintenance** > **Maintenance mode**). Existing calls continue until the call is terminated. Other peers in the cluster continue to process calls.

Step 4 Wait for all calls to clear and registrations to timeout.

To manually remove any calls or registrations that don't clear automatically, use the **Status** > **Calls** page or the **Status** > **Registrations** > **By device** page respectively (SIP calls may not clear immediately).

Note You can leave the registration for Conference Factory (if enabled) – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration.

Step 5 Go to **Maintenance** > **Upgrade** to access the **Upgrade** page.

Step 6 Click **Browse** and select the software image file for the component you want to upgrade. The Expressway/Cisco VCS automatically detects which component you are upgrading based on the selected software image file.

Step 7 Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.

Step 8 For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:

a. Check the following details:

- **New software version** number is as expected.
- **MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you downloaded the software image file.

b. Click **Continue with upgrade**. This step installs the new software.

The **System upgrade** page opens and displays a progress bar while the software installs.

A summary of any active calls and registrations is displayed when the software completes installing (the calls and registrations will be lost when you reboot the system in the next step).

c. Click **Reboot system**. Any configuration changes made between uploading the software tar file and rebooting, will be lost when the system restarts.

Sometimes the web browser interface times out during the restart process, after the progress bar reaches the end. This may occur if the Expressway/Cisco VCS carries out a disk file system check – approximately once every 30 restarts.

Ignore any cluster-related alarms and warnings that occur during the upgrade process, such as cluster communication failures or cluster replication errors. These are expected and will resolve when all cluster peers are upgraded and after cluster data synchronization (typically within 10 minutes of the complete upgrade).

After the reboot is complete the **Login** page displays.

Step 9 For upgrades to other components (not the System platform) the software is automatically installed and no reboot is required.

Step 10 Repeat the previous steps for each peer in sequence until all peers are on the new software version.

What Next?

1. Verify the new status of each Expressway (including the primary):
   a. Go to **System** > **Clustering** and check that the cluster database status reports as **Active**.

b. Check the configuration for items from the System, Configuration, and Application menus.

2. Backup the Expressway again (**Maintenance** > **Backup and restore**).
3. If you use MRA, and you are upgrading from X8.9.x or earlier, reconfigure the MRA access control settings as described in "Appendix 2: Post-Upgrade Tasks for MRA Deployments" in the *Mobile and Remote Access Deployment Guide*.
4. If you have components that require option keys to enable them, do this from the **Maintenance** > **Option keys** page.
5. If the Expressway has FIPS mode enabled (that is, it's a FIPS140-2 cryptographic system) then from X12.6 you must manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater. 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"***

   This step does **not** apply to most systems. It only affects systems with advanced account security configured and FIPS enabled.
6. (Optional) If for any reason you want to change the default TLS version, the *Cisco Expressway Certificate Creation and Use Deployment Guide* explains how to set the TLS version on each peer.

The software upgrade on the Expressway cluster is now complete.

Upgrading Using Secure Copy (SCP/PSCP)

Optionally use this process to upgrade using a secure copy program such as SCP or PSCP (part of the PuTTY free package) to transfer the file containing the software image onto the system.

Before you begin

The process requires the software image file to be manually renamed to the filename expected by the system. We recommend that you upload the file with its default name (similar to *s42700xXX_XX_XX.tar.gz*) and rename it only when you are ready to start (install) the upgrade. This provides better control of the process and also lets you check the file size before you proceed.

Depending on the software version, you may also need to install the *release-key* file.

Step 1 Upload the software image file.

- For the **System platform** component, upload to the /tmp folder on the system. For example: *scp s42700x12_5_7.tar.gz root@10.0.0.1:/tmp/s42700x12_5_7.tar.gz*
- For other components, upload to the */tmp/pkgs/new/* folder on the system, keeping the file name and extension unchanged. For example: *scp root@10.0.0.1:/tmp/pkgs/new/vcs-lang-es-es_8.1_amd64.tlp*

Step 2 Wait for the file upload to complete and then check the file size.

Note The default */tmp/tandberg-image.tar.gz* file entry in */tmp* will be 0 bytes.

Step 3 When you are ready to start the upgrade, rename (or move) the file to the required filename of */tmp/tandberg-image.tar.gz* (this will start the upgrade process).

For example: *mv /tmp/s42700x12_5_7.tar.gz /tmp/tandberg-image.tar.gz*

Step 4 Enter the root password when prompted. The software installation begins automatically and you see "*Software upgrade in progress*" on the SSH/console.

Step 5 Wait until the software has installed completely and you see "*Upgrade complete! The new software will be used on the next reboot*".

Step 6 We recommend that you reboot the system immediately, because any further configuration changes made before the reboot **will be lost when the system restarts**.

Upgrading Using APIs

Before you begin

The process requires the software image file to be placed manually in a SFTP server.

For request parameters and more information, refer to *REST API Summary Guide*.

Step 1 Add SFTP details with the following API

PUT https://<Expressway FQDN or IPaddress>/api/v1/provisioning/common/sftpconfig

Step 2 Trigger Upgrade with the following API

POST https://<Expressway FQDN or IPaddress>/api/v1/provisioning/common/upgrade

Step 3 Check UpgradeStatus with the following API

GET https://<Expressway FQDN or IPaddress>/api/v1/status/common/upgradestatus

Upgrading Firmware (Physical Appliances Only)

This section applies if Expressway is deployed on a physical appliance, and you need to upgrade the firmware for some reason.

Use the Cisco Host Upgrade Utility (HUU) to perform the upgrade. This is Cisco's dedicated tool for upgrading firmware components on a UCS C-Series server. Detailed instructions about using the HUU are available in the latest *Cisco Host Upgrade Utility User Guide* on the Cisco UCS C-Series Rack Servers documentation page.

Known Issues and Workarounds

Upgrade failure due to "Unique index collision" error

From X14.2.1 release, duplicate entries are not allowed in the CDB table **serviceConfiguration**. Due to this, upgrades from a previous version (which have duplicate entries in 'serviceConfiguration' table) fail with the below error.

Error: Upgrade fails with the following error in developer logs.

```
"Unique index collision: The value already exists in the table"
Table="serviceConfiguration""
```

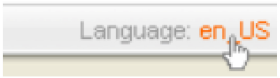
Cause: A 'UNIQUE' qualifier is introduced on the 'name' field of the table.

Due to this, upgrades from any previous version (which have duplicate entries in the 'serviceConfiguration' table) to a version higher or equal to X14.2.1 fails with a unique index collision error.

Solution: For technical assistance, contact Cisco Technical Assistance Center (TAC) team for a workaround script to delete duplicate entries before retrying the upgrade (bug ID CSCwd38155 refers).

Configuring Language Settings

The **Language** page (**Maintenance** > **Language**) controls which language is used for text displayed in the web user interface.

 453657	You can also get to the **Language** page by clicking on the **Language** link at the bottom of every page.

Changing the Language

You can configure both the default language and the language to use on an individual browser:

Field	Description	Usage tips
System default language	The default language used on the web interface.	This applies to administrator and user (FindMe) sessions. You can select from the set of installed language packs.
This browser	The language used by the current browser on the current client computer. It can be set to use either the system default language or a specific alternative language.	This setting applies to the browser currently in use on the client computer. If you access the Expressway user interface using a different browser or a different computer, a different language setting may be in place.

Installing Language Packs

You can install new language packs or install an updated version of an existing language pack.

Language packs are downloaded from the same area on cisco.com from where you obtain your Expressway software files. All available languages are contained in one language pack zip file. Download the appropriate language pack version that matches your software release.

After downloading the language pack, unzip the file to extract a set of .tlp files, one per supported language.

For the list of available languages, see the relevant release notes for your software version.

Note

- English (en_us) is installed by default and is always available.
- You cannot create your own language packs. Language packs can be obtained only from Cisco.
- If you upgrade to a later version of Expressway software you will see a "Language pack mismatch" alarm. You may need to install a later version of the associated language pack to ensure that all text is available in the chosen language.

To install a .tlp language pack file:

Step 1 Go to **Maintenance** > **Language**.

Step 2 Click **Browse** and select the **.tlp** language pack you want to upload.

Step 3 Click **Install**.

The selected language pack is then verified and uploaded. This may take several seconds.

Step 4 Repeat steps 2 and 3 for any other languages you want to install.

Removing Language Packs

To remove a language pack:

Step 1 Go to the **Language** page (**Maintenance** > **Language**).

Step 2 From the list of installed language packs, select the language packs you want to remove.

Step 3 Click **Remove**.

Step 4 Click **Yes** when asked to confirm.

The selected language packs are then removed. This may take several seconds.

Backing Up and Restoring Expressway Data

Use the **Backup and restore** page (**Maintenance** > **Backup and restore**) to create backup files of Expressway data and to restore the Expressway to a previous, saved configuration.

When to Create a Backup

We recommend creating regular backups, and always in the following situations:

- Before performing an upgrade.
- Before performing a system restore.

- In demonstration and test environments, if you want to be able to restore the Expressway to a known configuration.

What Gets Backed Up

The data saved to a backup file includes:

- Bootstrap key (from X8.11)
- System configuration settings
- Clustering configuration
- Local authentication data (but not Active Directory credentials for remotely managed accounts):
  - User account and password details
  - Server security certificate **and** private key
- Call detail records (if the CDR service on Expressway is enabled)

Log files are not included in backup files.

For detailed backup and restore procedures, see Creating a System Backup, and Restoring a Previous Backup.

Clustered Systems

For more details about backing up and restoring peers in a cluster, see

Cluster Upgrades, Backup, and Restore.

Creating a System Backup

Before you Begin

- Backup files are always encrypted (from X8.11). In particular because they include the bootstrap key, and authentication data and other sensitive information.
- Backups can only be restored to a system that is running the **same version of software from which the backup was made**.
- You can create a backup on one Expressway and restore it to a different Expressway. For example if the original system has failed. Before the restore, you must install the same option keys on the new system that were present on the old one.

  If you try to restore a backup made on a different Expressway, you receive a warning message, but you will be allowed to continue.

  (If you use FIPS140-2 cryptographic mode) You can't restore a backup made on a non-FIPS system, onto a system that's running in FIPS mode. You can restore a backup from a FIPS-enabled system onto a non-FIPS system.

- Do not use backups to copy data between Expressways. If you do so, system-specific information will be duplicated (like IP addresses).
- Because backup files contain sensitive information, you should not send them to Cisco in relation to technical support cases. Use snapshot and diagnostic files instead.

Passwords

- All backups must be password protected.
- If you restore to a previous backup, and the administrator account password has changed since the backup was done, you must also provide the old account password when you first log in after the restore.
- Active Directory credentials are **not** included in system backup files. If you use NTLM device authentication, you must provide the Active Directory password to rejoin the Active Directory domain after any restore.
- For backup and restore purposes, emergency account passwords are handled the same as standard administrator account passwords.

Process

To create a backup of Expressway system data:

Step 1 Go to **Maintenance** > **Backup and restore**.

Step 2 Enter an **Encryption password** to encrypt the backup file.

Caution The password will be required in future if you ever want to restore the backup file.

Step 3 Click **Create system backup file**.

Step 4 Wait for the backup file to be created. This may take several minutes. Do not navigate away from this page while the file is being prepared.

Step 5 When the backup is ready, you are prompted to save it. The default filename uses format: **<software version>_<hardware serial number>_<date>_<time>_backup.tar.gz.enc**. Or if you use Internet Explorer, the default extension is **.tar.gz.gz**. (These different filename extensions have no operational impact, and you can create and restore backups using any supported browser.)

Step 6 Save the backup file to a secure location.

Restoring a Previous Backup

Before you Begin

Caution When you restore an Expressway-E onto a CE1200 appliance from a CE1100 or earlier appliance backup, the CE1200 appliance may restore as Expressway-C. This issue occurs if the service setup wizard was used in the CE1100 or earlier appliance to change the type to Expressway-C and you skipped the wizard without completing the entire configuration. To avoid this issue, before you back up the appliance, run the service setup wizard, change the type to Expressway-E, and ensure that you complete the wizard.

- You need the password for the backup file from which you intend to restore.
- If you are restoring a backup file from a different Expressway, you need to apply the same set of license keys as exist on the system from which you intend to restore.
- We recommend that you take the Expressway unit out of service before doing a restore.
- The restore process involves **doing a factory reset** back to the original software version. Then upgrading to the **same software version that was running when you took the backup**.
- If the backup is out of date (made on an earlier version than the version you want) these extra steps are needed after the restore:
  1. Upgrade the software version to the required later version.
  2. Manually redo any configuration changes made since the backup was taken.
- (If you use FIPS140-2 cryptographic mode) You can't restore a backup made on a non-FIPS system, onto a system that's running in FIPS mode. You can restore a backup from a FIPS-enabled system onto a non-FIPS system.
- You can't restore data to a Expressway while it's part of a cluster. You must first remove it from the cluster. For details, see Cluster Upgrades, Backup, and Restore.

Passwords

- Backups must be password protected.
- If you restore to a previous backup, and the administrator account password has changed since the backup was done, you must also provide the old account password when you first log in after the restore.
- Active Directory credentials are **not** included in system backup files. If you use NTLM device authentication, you must provide the Active Directory password to rejoin the Active Directory domain after any restore.
- For backup and restore purposes, emergency account passwords are handled the same as standard administrator account passwords.

Process

To restore the Expressway to a previous configuration of system data:

Step 1 First do a factory reset, as described in Restoring the Default Configuration (Factory Reset). This removes your configuration data, and reverts the system back to its original state. The reset maintains your current software version if you've upgraded since the system was first set up.

Step 2 Upgrade the system to the software version that was running when you made the backup.

- For standalone systems, see *Upgrade instructions*.
- For clustered systems, see the *Expressway Cluster Creation and Maintenance Deployment Guide*.

Step 3 Now you can restore the system from the backup, as follows:

a. Go to **Maintenance** > **Backup and restore**.

b. In the **Restore** section, click **Browse** and navigate to the backup file that you want to restore.

c. In the **Decryption password** field, enter the password used to create the backup file.

d. Click **Upload system backup file**.

e. The Expressway checks the file and takes you to the **Restore confirmation** page.

- If the backup file is invalid or the decryption password was entered incorrectly, an error message is displayed at the top of the **Backup and restore** page.
- The current software version and the number of calls and registrations is displayed.

f. Read the warning messages that appear, before you continue.

g. Click **Continue with system restore** to proceed with the restore.

This will restart the system, so make sure that no active calls exist.

h. When the system restarts, the **Login** page is displayed.

Step 4 This step only applies if the backup file is out of date. That is, the software version was upgraded, or system configuration changes were made after the backup was done. In this case:

a. Upgrade the system again, this time to the required software version for the system.

b. Redo any configuration changes made after the backup (assuming you still need them on the restored system).

Checking the Effect of Pattern

The **Check pattern** tool (**Maintenance** > **Tools** > **Check pattern**) lets you test whether a pattern or transform you intend to configure on the Expressway will have the expected result.

Patterns can be used when configuring:

- Transforms to specify aliases to be transformed before any searches take place

- Search rules to filter searches based on the alias being searched for, and to transform an alias before the search is sent to a zone

To use this tool:

Step 1 Enter an **Alias** against which you want to test the transform.

Step 2 In the **Pattern** section, enter the combination of **Pattern type** and **Pattern behavior** for the **Pattern string** being tested.

- If you select a **Pattern behavior** of *Replace*, you also need to enter a **Replace string**.
- If you select a **Pattern behavior** of *Add prefix* or *Add suffix*, you also need to enter an **Additional text** string to append/prepend to the **Pattern string**.
- The Expressway has a set of predefined pattern matching variables that can be used to match against certain configuration elements.

Step 3 Click **Check pattern** to test whether the alias matches the pattern.

The **Result** section shows whether the alias matched the pattern, and displays the resulting alias (including the effect of any transform if appropriate).

Locating an Alias

The **Locate** tool (**Maintenance** > **Tools** > **Locate**) lets you test whether the Expressway can find an endpoint identified by the given alias, within the specified number of "hops", without actually placing a call to that endpoint.

This tool is useful when diagnosing dial plan and network deployment issues.

Step 1 Enter the **Alias** you want to locate.

Step 2 Enter the **Hop count** for the search.

Step 3 Select the **Protocol** used to initiate the search, either *H.323* or *SIP*. The search may be interworked during the search process, but the Expressway always uses the native protocol first to search those target zones and policy services associated with search rules at the same priority, before searching those zones again using the alternative protocol.

Step 4 Select the **Source** from which to simulate the search request. Choose from the *Default Zone* (an unknown remote system), the *Default Subzone* (a locally registered endpoint) or any other configured zone or subzone.

Step 5 Select whether the request should be treated as **Authenticated** or not (search rules can be restricted so that they only apply to authenticated messages).

Step 6 Optionally, you can enter a **Source alias**. Typically, this is only relevant if the routing process uses CPL that has rules dependent on the source alias. (If no value is specified a default alias of `xcom-locate` is used.)

Step 7 Click **Locate** to start to search.

The status bar shows **Searching...** followed by **Search completed**. The results include the list of zones that were searched, any transforms and Call Policy that were applied, and if found, the zone in which the alias was located.

The locate process performs the search as though the Expressway received a call request from the selected **Source zone**. For more information, see the Call Routing Process section.

Port Usage

The pages under the **Maintenance** > **Tools** > **Port usage** menu show, in table format, all the IP ports that have been configured on the Expressway.

The information shown on these pages is specific to that particular Expressway and varies depending on the Expressway's configuration, the option keys that have been installed and the features that have been enabled.

The information can be sorted according to any of the columns on the page, so for example you can sort the list by IP port, or by IP address.

Each page contains an **Export to CSV** option. This lets you save the information in a CSV (comma separated values) format file suitable for opening in a spreadsheet application.

Note that IP ports cannot be configured separately for IPv4 and IPv6 addresses, nor for each of the two LAN interfaces. In other words, after an IP port has been configured for a particular service, for example SIP UDP, this will apply to all IP addresses of that service on the Expressway. Because the tables on these pages list all IP ports and all IP addresses, a single IP port may appear on the list up to 4 times, depending on your Expressway configuration.

The port information is split into the following pages:

- Local Inbound Ports
- Local Outbound Ports
- Remote Listening Ports

On Expressway-E you can also configure the specific listening ports used for firewall traversal via **Configuration** > **Traversal** > **Ports**.

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

Local Inbound Ports

The **Local inbound ports** page (**Maintenance** > **Tools** > **Port usage** > **Local inbound ports**) shows the listening IP ports on the Expressway that are used to receive inbound communications from other systems.

For each port listed on this page, if there is a firewall between the Expressway and the source of the inbound communications, your firewall must allow:

- Inbound traffic to the IP port on the Expressway from the source of the inbound communications, and
- Return traffic from that same Expressway IP port back out to the source of the inbound communication.

Note This firewall configuration is particularly important if this Expressway is a traversal client or traversal server, in order for Expressway firewall traversal to function correctly.

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

Local Outbound Ports

The **Local outbound ports** page (**Maintenance** > **Tools** > **Port usage** > **Local outbound ports**) shows the source IP ports on the Expressway that are used to send outbound communications to other systems.

For each port listed on this page, if there is a firewall between the Expressway and the destination of the outbound communications, your firewall must allow:

- Outbound traffic out from the IP port on the Expressway to the destination of the outbound communications, and
- Return traffic from that destination back to the same Expressway IP port.

Note This firewall configuration is particularly important if this Expressway is a traversal client or traversal server, in order for Expressway firewall traversal to function correctly.

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

Remote Listening Ports

The **Remote listening ports** page (**Maintenance** > **Tools** > **Port usage** > **Remote listening ports**) shows the destination IP addresses and IP ports of remote systems with which the Expressway communicates.

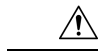
Your firewall must be configured to allow traffic originating from the local Expressway to the remote devices identified by the IP addresses and IP ports listed on this page.

Note There are other remote devices not listed here to which the Expressway will be sending media and signaling, but the ports on which these devices receive traffic from the Expressway is determined by the configuration of the destination device, so they cannot be listed here. If you have opened all the ports listed in the Local Outbound Ports page, the Expressway will be able to communicate with all remote devices. You only need to use the information on this page if you want to limit the IP ports opened on your firewall to these remote systems and ports.

See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

Restarting, Rebooting, and Shutting Down

The **Restart options** page (**Maintenance** > **Restart options**) allows you to restart, reboot, or shut down the Expressway without having physical access to the hardware.



Caution Do not restart, reboot or shut down the Expressway while the red ALM LED on the front of the unit is on. This indicates a hardware fault. Contact your Cisco customer support representative.

Restarting

The restart function shuts down and restarts the Expressway application software, but not the operating system or hardware. A restart takes approximately 3 minutes.

A restart is typically required in order for some configuration changes to take effect, or when the system is being added to, or removed from, a cluster. In these cases a system alarm is raised and will remain in place until the system is restarted.

If the Expressway is part of a cluster and other peers in the cluster also require a restart, we recommend that you wait until each peer has restarted before restarting the next peer.

Rebooting

The reboot function shuts down and restarts the Expressway application software, operating system and hardware. A reboot takes approximately 5 minutes.

Reboots are normally only required after software upgrades and are performed as part of the upgrade process. A reboot may also be required when you are trying to resolve unexpected system errors.

Shutting down

A shutdown is typically required if you want to unplug your unit, prior to maintenance or relocation for example. The system must be shut down before it is unplugged. Avoid uncontrolled shutdowns, in particular the removal of power to the system during normal operation.

Effect on active calls

Any of these restart options will cause all active calls to be terminated. (If the Expressway is part of a cluster, only those calls for which the Expressway is taking the signaling will be terminated.)

For this reason, the **System status** section displays the number of current calls so you can check these before you restart the system. If you do not restart the system immediately, you should refresh this page before restarting to check the current status of calls.

If **Mobile and remote access** is enabled, the number of currently provisioned sessions is displayed (Expressway-C only).

Restarting, rebooting or shutting down using the web interface

To restart the Expressway using the web interface:

1. Go to **Maintenance** > **Restart options**.
2. Check the number of calls currently in place.
3. Click **Restart**, **Reboot**, or **Shutdown** as appropriate and confirm the action.

   Sometimes only one of these options, such as **Restart** for example, may be available. This typically occurs when you access the **Restart options** page after following a link in an alarm or a banner message.

   - Restart/reboot: the **Restarting/Rebooting** page appears, with an orange bar indicating progress.

After the system has successfully restarted or rebooted, you are automatically taken to the **Login** page.

- Shutdown: the **Shutting down** page appears.

  This page remains in place after the system has successfully shut down but any attempts to refresh the page or access the Expressway will be unsuccessful.