



Cisco Expressway Registrar

Deployment Guide

First Published: July 2016

Last Updated: September 2018

Cisco Expressway X8.11

Preface

Change History

Table 1 Deployment Guide Change History

Date	Change
September 2018	Updated for Webex and Spark platform rebranding and X8.11.1 maintenance release.
July 2018	Updated for X8.11. Removed duplicate port reference information
December 2016	Updated for X8.9.
August 2016	Changed document title. From <i>Cisco Expressway Basic Configuration (Single Expressway-C) Deployment Guide</i> . To <i>Cisco Expressway Registrar Deployment Guide</i> .
July 2016	Initial release for X8.8.

Contents

Preface	3
Change History	3
Introduction	5
Example Network Deployment	6
Network Elements	6
Process Summary	7
Prerequisites	8
Run the Service Setup Wizard	9
Overview	9
Task 1: Accessing and Navigating the Wizard	9
Task 2: Running the Service Setup Wizard and Applying Licenses	11
Expressway System Configuration	12
Task 3: Setting the System Name	12
Task 4: Configuring DNS	12
Task 5: Replacing the Default Server Certificate	13
Task 6: Configuring NTP Servers	14
Task 7: Configuring SIP Domains	14
Routing Configuration	16
Pre-search Transforms	16
Search Rules	16
Task 8: Configuring Transforms	16
Task 9: Configuring Local Zone Search Rules	17
Endpoint Registration	19
System Checks	20
Registration Status	20
Call Signaling	20
Connectivity Test Tool	20
Maintenance Routine	21
Creating a System Backup	21
Optional Configuration Tasks	22
Task 10: Configuring Routes to a Neighbor Zone (Optional)	22
Task 11: Configuring Cisco TMS (Optional)	23
Task 12: Configuring Logging (Optional)	25
Task 13: Configuring Registration Restriction Policy (Optional)	25
Task 14: Configuring Device Authentication Policy (Optional)	26
Task 15: Restricting Access to ISDN Gateways (Optional)	27
Appendix 1: Configuration Details	29
Appendix 2: DNS Records	31
Obtaining Documentation and Submitting a Service Request	32
Cisco Legal Information	33
Cisco Trademark	33

Introduction

This document describes how to configure a single Cisco Expressway-C platform for use in a basic video infrastructure deployment. It takes you through the following tasks:

1. Using the Service Setup Wizard to select the services you want to use and to apply the corresponding keys (licenses).
2. Configuring system parameters and routing information.
3. Checking that the system is working as expected.
4. Configuring optional items such as Cisco TMS, system logging, and access restrictions.

If your deployment includes a Cisco Expressway-E, use the *Expressway-E and Expressway-C Basic Configuration Deployment Guide* on the [Expressway configuration guides page](#) instead.

The appendices to the document provide detailed reference information, as follows:

- Expressway configuration details used in this document are listed in [Appendix 1: Configuration Details, page 29](#).
- DNS records required for the example deployment used in this document are in [Appendix 2: DNS Records, page 31](#).

For descriptions of all system configuration parameters, see the *Expressway Administrator Guide* and the Expressway web application's online field help [🔍](#) and page help [📖](#).

Example configuration values used in this guide

For ease of reading this guide is based around an example deployment, which uses the following assumed configuration values throughout:

LAN1 IPv4 address	10.0.0.2
IPv4 gateway	10.0.0.1
LAN1 subnet mask	255.255.255.0
Domain name	<i>internal-domain.net</i>

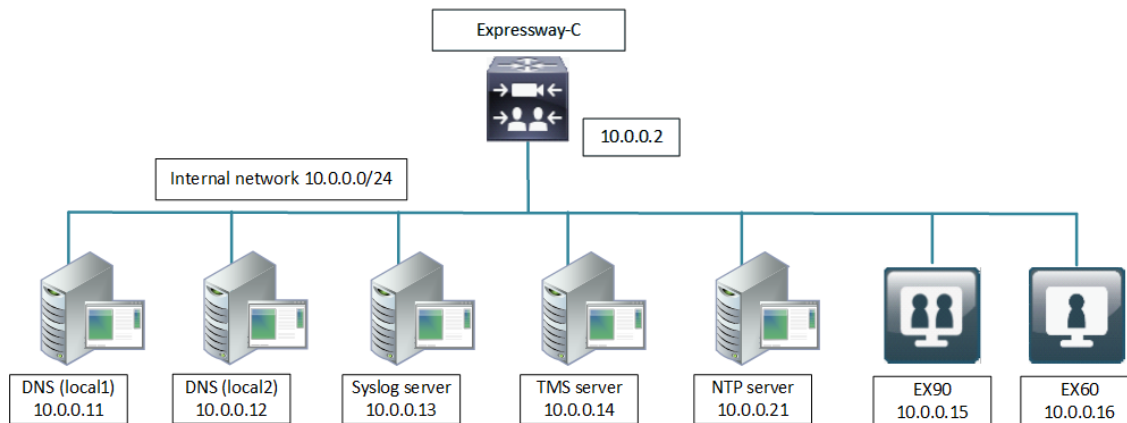
Information in other deployment guides

This document does not describe how to deploy a clustered system, or systems running device provisioning, device authentication, or FindMe applications, or how to configure the Expressway system for Unified Communications services. For more details about these features, see the following documents:

- *Expressway Cluster Creation and Maintenance Deployment Guide* on the [Expressway configuration guides page](#)
- *Cisco TMS Provisioning Extension Deployment Guide* on the [VCS configuration guides page](#) (includes instructions for deploying FindMe - note that this guide is on the VCS page and not on the Expressway page)
- *Cisco VCS Authenticating Devices* on the [VCS configuration guides page](#) (note that this guide is on the VCS page and not on the Expressway page)

Example Network Deployment

Figure 1 Example Network for the Deployment Described in this Document



Network Elements

Internal Network Elements

The internal network elements are devices which are hosted on your local area network. Elements on the internal network have an internal network domain name. This name is not resolvable by a public DNS. For example, the Cisco Expressway-C is configured with an internally resolvable name of `expc.internal-domain.net` (which resolves to an IP address of 10.0.0.2 by the internal DNS servers).

Element	Role
Cisco Expressway-C	SIP Registrar & Proxy, H.323 Gatekeeper for devices located on the internal network.
EX90 and EX60	Example endpoints hosted on the internal network which register to the Cisco Expressway-C.
DNS (local 1 & local 2)	DNS servers used by the Cisco Expressway-C to perform DNS lookups (resolve network names on the internal network).
DHCP Server	Provides host, IP gateway, DNS server, and NTP server addresses to endpoints located on the internal network.
Cisco TMS Server	Management and scheduling server. See Task 11: Configuring Cisco TMS (Optional) , page 23.
Syslog Server	Logging server for Syslog messages. See Task 12: Configuring Logging (Optional) , page 25.
NTP Server	Provides the clock source used to synchronize devices.

SIP and H.323 Domain

The example deployment is configured to route SIP (and H.323) signaling messages for calls made to URIs which use the domain `example.com`. The DNS SRV configurations are described in [Appendix 2: DNS Records](#), page 31.

Process Summary

Before You Begin

- [Prerequisites, page 8](#)

Run the Service Setup Wizard

- [Task 1: Accessing and Navigating the Wizard, page 9](#)
- [Task 2: Running the Service Setup Wizard and Applying Licenses, page 11](#)
- [Examples for Running the Service Setup Wizard, page 1](#)

Expressway system configuration tasks

- [Task 3: Setting the System Name, page 12](#)
- [Task 4: Configuring DNS, page 12](#)
- [Task 5: Replacing the Default Server Certificate, page 13](#)
- [Task 6: Configuring NTP Servers, page 14](#)
- [Task 7: Configuring SIP Domains, page 14](#)

Routing configuration tasks

- [Task 8: Configuring Transforms, page 16](#)
- [Task 9: Configuring Local Zone Search Rules, page 17](#)

Optional configuration tasks

- [Task 10: Configuring Routes to a Neighbor Zone \(Optional\), page 22](#)
- [Task 11: Configuring Cisco TMS \(Optional\), page 23](#)
- [Task 12: Configuring Logging \(Optional\), page 25](#)
- [Task 13: Configuring Registration Restriction Policy \(Optional\), page 25](#)
- [Task 15: Restricting Access to ISDN Gateways \(Optional\), page 27](#)

Prerequisites

Before you begin any of the tasks in this guide, make sure that the following prerequisites are complete.

General prerequisites

- We recommend that you use the Expressway web user interface to do the system configuration. This guide assumes that you are using a web browser running on a PC. The PC needs an Ethernet connection to a LAN which can route HTTP(S) traffic to the Expressway.
- Review the relevant release notes on the [Expressway release notes page](#).
- Have the *Expressway Administrator Guide* on the [Expressway maintenance and operation guides page](#) available for reference before you start.

IP address and password prerequisites

This guide also assumes that you have already configured a static IP address and changed the default passwords, as described in the appropriate installation guide:

Cisco Expressway Virtual Machine Installation Guide on the [Expressway installation guides page](#).

Cisco Expressway CE1100 Appliance Installation Guide on the [Expressway installation guides page](#).

Note: Expressway requires a static IP address. It doesn't use DHCP/SLAAC to get an IP address.

Run the Service Setup Wizard

Overview

The Service Setup Wizard makes it easier to configure and license the Expressway for its chosen purpose in your environment. It also simplifies the user interface. You select from a list of popular Expressway services and the wizard then prompts you with the licensing requirements for those services. You can also use the wizard to review and edit the Expressway basic network settings (typically already configured during initial installation).

When you restart the Expressway, the user interface is tailored to match your service selections. You only see menus and pages for the services you chose.

Note: Some services are incompatible and cannot be selected together. The [Expressway Administrator Guide](#) and the online help provide a matrix of compatible services. The matrix specifies which services you can use together on the same system or cluster.

What If I Don't Want to Use the Wizard?

A skip option exists if you don't want to use the wizard. If you change your mind later, you can go back and run it at any time (**Status > Overview** page; click **Run service setup**).

If you opt to skip the wizard, you need to deal with the Expressway licensing setup requirements manually before you start the configuration tasks in this guide. Also, the user interface isn't customized to reflect your specific service selections.

Task 1: Accessing and Navigating the Wizard

There are multiple ways to access the wizard:

- As of X8.8, you'll automatically see the Service Setup Wizard when you first log in to the Expressway user interface. You don't need to launch it.
- If you previously logged in or have upgraded, you'll see the **Status > Overview** page as usual. Click **Run service setup** to launch the wizard.
- If you've already run the wizard you can rerun it at any time. From the **Status > Overview** page, click **Return to service setup**.

To navigate the wizard:

- Click **Skip Service Setup Wizard** if you want to back out of the wizard completely, or **Back** to return to the previous page.
- Click **Continue** to save and move to the next wizard page.

Run the Service Setup Wizard

Figure 2 Service Setup Wizard Example - Selection Page

Welcome to Cisco Collaboration services ? Help Logout

Select Series

Expressway series	<input checked="" type="radio"/> <small>i</small>
VCS series	<input type="radio"/>

Select Type

Expressway-C	<input checked="" type="radio"/> <small>i</small>
Expressway-E	<input type="radio"/>

Select Services

After you select services, you get a simplified menu that is relevant to your selection. i

Cisco Spark Hybrid Services	<input type="checkbox"/>
Mobile and remote access	<input type="checkbox"/>
Jabber Guest services	<input type="checkbox"/>
Microsoft interoperability	<input type="checkbox"/>
Registrar	<input type="checkbox"/>
Collaboration Meeting Rooms (CMR) Cloud	<input type="checkbox"/>
Business to business calls	<input type="checkbox"/>
Proceed without selecting services	<input type="checkbox"/>

If you proceed without selecting services, you will get the full menu.

Task 2: Running the Service Setup Wizard and Applying Licenses

This guide applies to deployments with local networking only (with the Cisco Expressway-C but no Cisco Expressway-E). For these deployments, choose the *Registrar* service in the wizard. This is the core video conferencing service.

Note: If you try to add more than 65 option keys (licenses), they appear as normal on the **Option keys** page. However, only the first 65 keys take effect. Additional keys from 66 onwards appear to be added, but actually the Expressway does not process them. CDETS [CSCvf78728](#) refers.

Process

1. Choose *Expressway series*.
2. Choose *Expressway-C*.
3. Check the box for the *Registrar* service.
4. Click **Continue** to move to the **Option keys** page of the wizard.
5. On the **Option Keys** page, click the [Product License Registration Portal](#) link to go to the licensing portal. (For this step you need to work away from the wizard to obtain the necessary licenses, and you need the serial number of the system.) In the licensing portal, enter the necessary details for the required licenses. For example, to register desktop systems like the EX90, you'll need to add Desktop System registration licenses.

Detailed information about using the licensing portal is in the online help or the [Expressway Administrator Guide](#). An ordering guide for our products is available on the Cisco [Collaboration Ordering Guides page](#).
6. Wait for system-generated emails from the licensing portal with the release key and option key.
7. Back in the wizard, paste the text from the release key email into the first text area. The system reads the release key out of the pasted text and displays it next to the text area.
8. Paste the text from the option keys email into the second text area. The system reads the option keys out of the pasted text and displays them next to the text area.
9. Create a new paste area and paste in your room or desktop system registration license keys.
10. Click **Add Keys**.
11. Click **Continue**.
12. Review the network configuration and modify the settings if necessary. Save any changes before you continue the wizard.
13. Click **Finish**.
14. Restart the system when prompted.

Result: When you log in, the user interface is tailored to match your service selections. You only see menus and pages for the services you chose.

What to do next

The Service Setup Wizard part of the configuration process is now complete. Go to the next section in this guide "[Expressway System Configuration](#)."

Expressway System Configuration

Task 3: Setting the System Name

The **System name** defines the name of the Expressway. It appears in various places in the web interface and is also used by Cisco TMS. We recommend using a name that lets you easily and uniquely identify the Expressway.

To configure the **System name**:

1. Go to **System > Administration**.
2. Configure the **System name** as follows:

System name	Enter <code>expc</code>
--------------------	-------------------------

3. Click **Save**.

Task 4: Configuring DNS

System Host Name

The **System host name** defines the DNS hostname that this system is known by. Note that this is not the fully-qualified domain name, just the host label portion.

Note that **<System host name>.<Domain name>** = FQDN of this Expressway.

To configure the **System host name**:

1. Go to **System > DNS**.
2. Configure the **System host name** as follows:

System host name	Enter <code>expc</code>
-------------------------	-------------------------

3. Click **Save**.

Domain Name

The **Domain name** is the name to append to an unqualified host name before querying the DNS server.

To configure the **Domain name**:

1. Go to **System > DNS**.
2. Configure the **Domain name** as follows:

Domain name	Enter <code>internal-domain.net</code>
--------------------	--

3. Click **Save**.

The fully qualified domain name for the Cisco Expressway-C is now `expc.internal-domain.net`

DNS Servers

The DNS server addresses specify the IP addresses of up to five domain name servers to be used for resolving domain names. In either of the following cases you must specify at least one default DNS server for address resolution:

Expressway System Configuration

- To use fully qualified domain names instead of IP addresses when specifying external addresses. For example, for LDAP and NTP servers, neighbor zones and peers.
- To use features such as URI dialing or ENUM dialing.

The Expressway queries one server at a time. If that server is unavailable the Expressway tries another server from the list.

In the example deployment two DNS servers are configured for each Expressway, which provides a level of DNS server redundancy. The Cisco Expressway-C is configured with DNS servers which are located on the internal network.

To configure the **Default DNS server** addresses:

1. Go to **System > DNS**.
2. Configure the DNS server **Address** fields as follows:

Address 1	Enter 10.0.0.11
Address 2	Enter 10.0.0.12

3. Click **Save**.

Task 5: Replacing the Default Server Certificate

For extra security, you may want to have the Expressway communicate with other systems (such as LDAP servers, neighbor Expressways, or clients such as SIP endpoints and web browsers) using TLS encryption.

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

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

The Expressway lets you install a certificate that can represent the Expressway as either a client or a server in connections using TLS. The Expressway can also authenticate client connections (typically from a web browser) over HTTPS. You can also upload certificate revocation lists (CRLs) for the CAs used to verify LDAP server and HTTPS client certificates.

The Expressway can generate server certificate signing requests (CSRs). This removes the need to use an external mechanism to generate certificate requests.

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

Table 2 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.

TLS can be difficult to configure. For example, when using it with an LDAP server we recommend verifying that the system works correctly over TCP, before you attempt to secure the connection with TLS. We also recommend using a third-party LDAP browser to verify that your LDAP server is correctly configured for TLS.

Note: Be careful not to allow your CA certificates or CRLs to expire. This may cause certificates signed by those CAs to be rejected.

To load the trusted CA list, go to **Maintenance > Security > Trusted CA certificate**.

To generate a CSR and/or upload the Expressway's server certificate, go to **Maintenance > Security > Server certificate**.

Additional server certificate requirements apply when configuring your Expressway system for Unified Communications. For full information, see *Expressway Certificate Creation and Use Deployment Guide* on the [Expressway configuration guides page](#).

Task 6: Configuring NTP Servers

The **NTP server** address fields set the IP addresses or Fully Qualified Domain Names (FQDNs) of the NTP servers to be used to synchronize system time. The **Time zone** sets the local time zone of the Expressway.

To configure the NTP server address and time zone:

1. Go to **System > Time**.
2. Configure the fields as follows:

NTP server 1	Enter 10.0.0.21
Time zone	GMT in this example

3. Click **Save**.

Time You are here: [System](#) > [Time](#)

NTP servers

NTP server 1	Address: <input type="text" value="10.0.0.21"/>	Authentication: <input type="text" value="Disabled"/>
NTP server 2	Address: <input type="text"/>	Authentication: <input type="text" value="Disabled"/>
NTP server 3	Address: <input type="text"/>	Authentication: <input type="text" value="Disabled"/>
NTP server 4	Address: <input type="text"/>	Authentication: <input type="text" value="Disabled"/>
NTP server 5	Address: <input type="text"/>	Authentication: <input type="text" value="Disabled"/>

Time zone

Time zone:

Task 7: Configuring SIP Domains

The Expressway acts as a SIP Registrar for configured SIP domains, accepting registration requests for any SIP endpoints attempting to register with an alias that includes these domains.

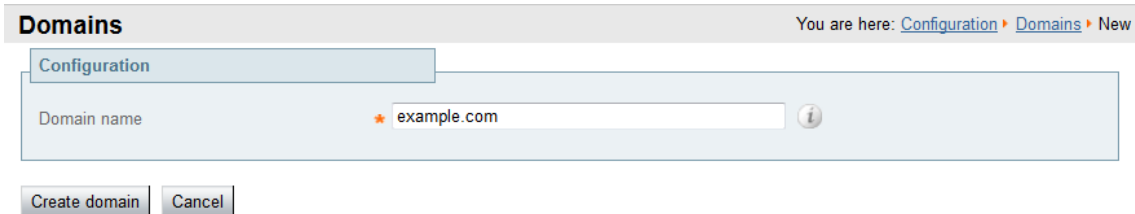
- Registration restriction (Allow or Deny) rules can be configured to limit acceptable registrations. See [Task 13: Configuring Registration Restriction Policy \(Optional\)](#), page 25.
- If authentication is enabled, only devices that can properly authenticate themselves will be allowed to register.

To configure a SIP domain:

1. Go to **Configuration > Domains**.
2. Click **New**.

Expressway System Configuration

3. Enter the domain name into the **Name** field, such as `example.com`.
4. Click **Create domain**.
5. The **Domains** page displays all configured SIP domain names.



The screenshot shows a web interface for configuring domains. At the top, there is a header bar with the title "Domains" on the left and a breadcrumb trail "You are here: Configuration > Domains > New" on the right. Below the header, there is a "Configuration" tab. The main content area contains a form with a label "Domain name" and a text input field containing "example.com". To the right of the input field is an information icon (a lowercase 'i' inside a circle). Below the form, there are two buttons: "Create domain" and "Cancel".

What To Do Next

The Expressway system configuration is now complete. Go to the next section, "*Routing Configuration*."

Routing Configuration

Pre-search Transforms

Pre-search transform configuration allows the destination alias (called address) in an incoming search request to be modified. The Expressway applies the transformation before any searches are sent to external zones.

The pre-search transform configuration described in this document is used to standardize destination aliases originating from both H.323 and SIP devices. This means that the same call searches work for calls from both H.323 and SIP endpoints.

For example, if the called address is an H.323 E.164 alias "01234", the Expressway automatically appends the configured domain name (in this case example.com) to the called address (that is, 01234@example.com making it into a URI), before attempting to set up the call.

- Use pre-search transforms with care. They apply to *all* incoming signaling messages, not just to call requests.
- Transformations can also be carried out in search rules. Consider whether it's best to use a pre-search transform or a search rule to modify the called address to be looked up.

Search Rules

Search rules define how the Expressway routes calls (to destination zones, such as to Unified CM, or another Expressway, or Meeting Server) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule.

The search rules described in this document are used to ensure that endpoints can dial H.323 devices that have registered E.164 numbers or H.323 IDs without a domain portion. The search rules first search for received destination aliases without the domain portion of the URI, and then search with the full URI.

The routing configuration in this document searches for destination aliases that have valid SIP URIs. That is, using a valid SIP domain, such as id@domain.

You can configure routing which enables calls to unregistered devices on an internal network (routing to the addresses of IP of the devices) by configuring a search rule with a mode of *Any IP address* with target Local Zone. However this is not recommended (and not described in this document). The best practice is to register all devices and route using destination aliases.

Task 8: Configuring Transforms

The pre-search transform configuration described in this document is used to standardize destination aliases originating from both H.323 and SIP devices.

The following transform modifies the destination alias of all call attempts made to destination aliases which do not contain an '@'. The old destination alias has @example.com appended to it, thus standardizing all called destination aliases into a SIP URI format.

To configure the transform:

1. Go to **Configuration > Dial plan > Transforms**.
2. Click **New**.

- Configure the transform fields as follows:

Priority	Enter 1
Description	Enter Transform destination aliases to URI format
Pattern type	<i>Regex</i>
Pattern string	Enter ([^@]*)
Pattern behavior	<i>Replace</i>
Replace string	Enter \1@example.com
State	<i>Enabled</i>

- Click **Create transform**.

Create transform You are here: [Configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform

Configuration

Priority	<input type="text" value="1"/> ⓘ
Description	<input type="text" value="Transform destination aliases to URI format"/> ⓘ
Pattern type	Regex ⓘ
Pattern string	* <input type="text" value="([^\@]*)"/> ⓘ
Pattern behavior	Replace ⓘ
Replace string	<input type="text" value="\1@example.com"/> ⓘ
State	Enabled ⓘ

Task 9: Configuring Local Zone Search Rules

To configure the search rules to route calls to the Local Zone (to locally registered endpoint aliases):

- Go to **Configuration > Dial plan > Search rules**.
- First disable the supplied default search rule (**LocalZoneMatch**), as follows:
 - Select the check box next to **LocalZoneMatch**.
 - Click **Disable**.
 - Click **OK**.
- Click **New**.

4. Configure the search rule fields as follows:

Rule name	Enter <code>Local zone - full URI</code>
Description	Enter <code>Search local zone for SIP devices with a domain</code>
Priority	Enter <code>50</code>
Protocol	<i>Any</i>
Source	<i>Any</i>
Request must be authenticated	<i>No</i>
Mode	<i>Alias pattern match</i>
Pattern type	<i>Regex</i>
Pattern string	Enter <code>(.+@example.com.*</code>
Pattern behavior	<i>Leave</i>
On successful match	<i>Continue</i>
Target	<i>LocalZone</i>
State	<i>Enabled</i>

5. Click **Create search rule**.

Endpoint Registration

The example network configuration diagram shows two endpoints.

Endpoint	IP address	Network
EX90	10.0.0.15	Internal network
EX60	10.0.0.16	Internal network

After system configuration, endpoint registration should be possible using these endpoint configuration details:

EX90 (uses SIP protocol)	
SIP URI	user.one.ex90@example.com
SIP Proxy1	expc.internal-domain.net
EX60 (uses H.323 and SIP protocol)	
H.323 ID	user.two.mxp@example.com
H.323 E.164	7654321
Gatekeeper IP Address	expc.internal-domain.net
SIP URI	user.two.mxp@example.com
SIP Proxy1	expc.internal-domain.net

What To Do Next

The Expressway routing configuration is now complete. Go to the next section, "*System Checks*."

System Checks

Registration Status

Check that all endpoints which are expected to be registered are actually registered to the relevant Expressway. And that they are registering the expected aliases. All successfully registered endpoints are listed on **Status > Registrations > By device**.

If the expected endpoints are not registered, review the following items:

- The SIP domains ([Task 7: Configuring SIP Domains, page 14](#)).
- Any registration restriction configuration applied to the Expressway (optional, [Task 13: Configuring Registration Restriction Policy \(Optional\), page 25](#)).

Call Signaling

If calls do not complete, despite the endpoints being successfully registered to a Expressway:

- Review the Cisco Expressway-C search rule configuration.
- Check the search history page for search attempts and failures (**Status > Search history**).
- Check the Event Log for call connection failure reasons (**Status > Logs > Event Log**).

Connectivity Test Tool

The SRV connectivity tester is a network utility that tests whether the Expressway can connect to particular services on a given domain. You can use this tool to proactively test your connectivity while configuring Expressway-based solutions such as Cisco Webex Hybrid Call Service or business-to-business video calling. You specify the DNS Service Record Domain and the Service Record Protocols you want to query for that domain. The Expressway does a DNS SRV query for each specified protocol, and then attempts TCP connections to the hosts returned by the DNS. If you specify TLS, the Expressway only attempts a TLS connection after the TCP succeeds. The Expressway connectivity test page shows the DNS response and the connection attempts. For any connection failures, the reason is provided along with advice to help with resolving specific issues. To troubleshoot connectivity, you can download the TCP data from your test in *.pcap* format. You can selectively download a dump of the DNS query, or a specific connection attempt, or you can get a single *.pcap* file showing the whole test.

What To Do Next

When you've completed the system checks and are satisfied that the system is working as expected, [create a system backup](#) and then go on to "*Optional Configuration Tasks*".

Maintenance Routine

Creating a System Backup

Before You Begin

- From X8.11, backup files are always encrypted. 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

- From X8.11, 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:

1. Go to **Maintenance > Backup and restore**.
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.
3. Click **Create system backup file**.
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.
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.)
6. Save the backup file to a secure location.

Optional Configuration Tasks

Task 10: Configuring Routes to a Neighbor Zone (Optional)

You can optionally set up neighbor zones and associated search rules on the Cisco Expressway-C if you want to route calls to other systems. To another Expressway for example, or to a Cisco VCS, Cisco Meeting Server, or Unified CM.

Example: Cisco VCS Neighbor Zone

This example assumes that you want to route calls toward devices that are registered to a Cisco VCS. The devices have an address (destination alias) in the format `<alias>@vcs.domain`.

Note: You may need more rules or transforms if any H.323 devices have registered E.164 numbers or H.323 IDs without a domain portion.

To configure a neighbor zone to the Cisco VCS:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows, and leave all other fields with their default values:

	Cisco Expressway-C
Name	Enter Neighbor zone to VCS
Type	<i>Neighbor</i>
H.323 Mode	<i>On</i>
H.323 Port	Enter 1719
SIP Mode	<i>On</i>
SIP Port	Enter 5061
SIP Transport	<i>TCP</i>
Location Peer 1 address	Enter the address of the Cisco VCS neighbor system

4. Click **Create zone**.

To configure the search rule to route calls to the Cisco VCS:

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.

Optional Configuration Tasks

3. Configure the search rule fields as follows:

	Cisco Expressway-C
Rule name	Enter <code>Route to VCS</code>
Description	Enter <code>Search VCS neighbor zone</code>
Priority	Enter <code>100</code>
Protocol	<i>Any</i>
Source	<i>Any</i>
Request must be authenticated	<i>No</i>
Mode	<i>Alias pattern match</i>
Pattern type	<i>Suffix</i>
Pattern string	Enter <code>@vcs.domain</code>
Pattern behavior	<i>Leave</i>
On successful match	<i>Continue</i>
Target	<i>Neighbor zone to VCS</i>
State	<i>Enabled</i>

4. Click **Create search rule**.

SIP Trunks to Unified CM

To configure a SIP trunk to Unified CM, see [Cisco Unified Communications Manager with Expressway Deployment Guide](#).

Task 11: Configuring Cisco TMS (Optional)

The following configuration enables the Expressway system to be integrated to a Cisco TelePresence Management Suite (Cisco TMS).

Points to note:

- Further configuration tasks are also required on Cisco TMS to fully integrate the Expressway with the TMS server. For details, see [Cisco TMS Administrator Guide](#) on the [TMS Maintain and Operate Guides](#) page.
- Enabling SNMP speeds up the Expressway - TMS integration process, but is not essential.

To enable and configure SNMP:

Optional Configuration Tasks

1. Go to **System > SNMP**.
2. Configure the SNMP fields as follows:

SNMP mode	<i>v3 plus TMS support</i>
Community name	Check that it is <code>public</code>
System contact	Enter <code>IT administrator</code>
Location	Enter <code>example.com head office</code>
Username	Enter <code>VCS</code>
Authentication mode	<i>On</i>
Type	<i>SHA</i>
Password	Enter <code>ex4mp13.c0m</code>
Privacy mode	<i>On</i>
Type	<i>AES</i>
Password	Enter <code>ex4mp13.c0m</code>

3. Click **Save**.

SNMP You are here: [System](#) > [SNMP](#)

Configuration

SNMP mode: ⓘ

Community name: ⓘ

System contact: ⓘ

Location: ⓘ

Username: ⓘ

Authentication

Authentication mode: ⓘ

Type: ⓘ

Password: ⓘ

Privacy

Privacy mode: ⓘ

Type: ⓘ

Password: ⓘ

To configure the necessary external manager (Cisco TMS) parameters:

Optional Configuration Tasks

1. Go to **System > External manager**.
2. Configure the fields as follows:

Address	Enter 10.0.0.14
Path	Enter tms/public/external/management/ SystemManagementService.asmx
Protocol	Select <i>HTTP</i> or <i>HTTPS</i>
Certificate verification mode	Select <i>On</i> or <i>Off</i> The certificate is only verified if the value is <i>On</i> and the protocol is set to <i>HTTPS</i> . If you switch this on then Cisco TMS and Expressway must have appropriate certificates.

3. Click **Save**.

The screenshot shows the 'External manager' configuration page. The breadcrumb trail indicates 'You are here: System > External manager'. The 'Configuration' tab is active. The fields are: Address (10.0.0.14), Path (tms/public/external/management/SystemManagementService.asmx), Protocol (HTTP), and Certificate verification mode (On). A 'Save' button is located at the bottom left.

Task 12: Configuring Logging (Optional)

The following configuration enables event logs to be sent to an external logging server using the SYSLOG protocol.

- The **Local event log verbosity** setting controls the granularity of event logging. 1 is the least verbose, 4 the most.
- We recommend a minimum level of 2. This provides both system and basic signaling message logging.

To configure a logging server:

1. Go to **Maintenance > Logging**.
2. Configure the fields as follows:

Local event log verbosity	2
Remote syslog server 1: Address	Enter 10.0.0.13
Remote syslog server 1: Message Format	<i>IETF syslog format</i>

3. Click **Save**.

Task 13: Configuring Registration Restriction Policy (Optional)

You can limit the aliases that endpoints can register, using either an Allow list or a Deny list. This is an example of how to configure Allow list registration restrictions:

Optional Configuration Tasks

1. Go to **Configuration > Registration > Allow List**.
2. Click **New**.
3. Create an allow pattern by configuring the following fields. This example limits registrations to endpoints which register with an identity that contains "@example.com".

Description	Enter Only allow registrations containing "@example.com"
Pattern type	Regex
Pattern string	Enter .*@example\.com

4. Click **Add Allow List pattern**.

Create allow pattern You are here: [Configuration](#) > [Registration](#) > [Allow List](#) > Create allow pattern

Configuration

Description

Pattern type

Pattern string

To activate the registration restriction:

1. Go to **Configuration > Registration > Configuration**.
2. Configure the **Restriction policy** as follows:

Restriction policy	Allow List
---------------------------	------------

3. Click **Save**.

Registration configuration You are here: [Configuration](#) > [Registration](#) > Configuration

Configuration

Restriction policy

Task 14: Configuring Device Authentication Policy (Optional)

Authentication policy is applied by the Expressway at the zone and subzone levels. It controls how the Expressway challenges incoming messages (for provisioning, registration, phone books, and calls) from that zone or subzone and whether those messages are rejected, treated as authenticated, or treated as unauthenticated within the Expressway.

Each zone and subzone can set its **Authentication policy** to *Check credentials*, *Do not check credentials*, or *Treat as authenticated*.

- Registration authentication is controlled by the Default Subzone configuration (or the relevant alternative subzone).
- Initial provisioning subscription request authentication is controlled by the Default Zone configuration.
- Call and phone book request authentication is controlled by the Default Subzone (or relevant alternative subzone) if the endpoint is registered, or by the Default Zone if the endpoint is not registered.

By default, zones and subzones are configured as *Do not check credentials*.

Task 15: Restricting Access to ISDN Gateways (Optional)

We recommend that you restrict unauthorized access to any ISDN gateway resources (also known as toll-fraud prevention). This section describes one way to achieve this.

In these examples, an ISDN gateway is registered to the Cisco Expressway-C with a prefix of 9. And / or it has a neighbor zone specified that routes calls starting with a 9.

This example describes how to configure the Cisco Expressway-C to stop calls that come in through the gateway, from being able to route calls back out of the gateway.

To do this, you load some specially constructed CPL onto the Cisco Expressway-C and configure its **Call policy mode** to use *Local CPL*.

Creating a CPL File

The CPL file can be created in a text editor.

Here are two example sets of CPL. In these examples:

- “GatewayZone” is the neighbor zone to the ISDN gateway.
- “GatewaySubZone” is the subzone to the ISDN gateway (required if the gateway registers the 9 prefix to the Expressway).
- Calls coming into the ISDN gateway and hitting a FindMe do not ring devices that use the gateway. So for example, calls forwarded to a mobile phone are disallowed.

This example CPL excludes any checking of whether the calling party is authenticated:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <taa:rule-switch>
      <!--Check that gateway is not hairpinning call - Neighbor zone -->
      <taa:rule originating-zone="GatewayZone" destination="9.*">
        <!-- Calls coming from the gateway may not send calls back out of this gateway -->
        <!-- Reject call with a status code of 403 (Forbidden) -->
        <reject status="403" reason="ISDN hairpin call denied"/>
      </taa:rule>
      <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
      <taa:rule originating-zone="GatewaySubZone" destination="9.*">
        <!-- Calls coming from the gateway may not send calls back out of this gateway -->
        <!-- Reject call with a status code of 403 (Forbidden) -->
        <reject status="403" reason="ISDN hairpin call denied"/>
      </taa:rule>
      <taa:rule origin=".*" destination=".*">
        <!-- All other calls allowed -->
        <proxy/>
      </taa:rule>
    </taa:rule-switch>
  </taa:routed>
</cpl>
```

This example CPL also ensures that the calling party is authenticated:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
```

Optional Configuration Tasks

```

<taa:routed>
  <taa:rule-switch>
    <!-- Check that calling party is authenticated -->
    <taa:rule authenticated-origin="" destination="9.*">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN call denied as unauthenticated caller"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Neighbor zone -->
    <taa:rule originating-zone="GatewayZone" destination="9.*">
      <!-- Calls coming from the gateway may not hairpin and send calls back out -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
    <taa:rule originating-zone="GatewaySubZone" destination="9.*">
      <!-- Calls coming from the gateway may not hairpin and send calls back out -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <taa:rule origin=".*" destination=".*">
      <!-- All other calls allowed -->
      <proxy/>
    </taa:rule>
  </taa:rule-switch>
</taa:routed>
</cpl>

```

Loading the CPL onto Cisco Expressway-C

To configure the Cisco Expressway-C to use the CPL:

1. Go to **Configuration > Call Policy > Configuration**.
2. Click **Browse....** Select the CPL file you created in the previous step from your file system.
3. Click **Upload file**.
 - If the file upload succeeds, you see a "File upload successful" message.
 - If you receive an "XML invalid" message, correct the problems with the CPL file and upload it again.
4. Select a **Call policy mode** of *Local CPL*.
5. Click **Save**.

Call Policy configuration You are here: [Configuration](#) > [Call Policy](#) > Configuration

Configuration

Call Policy mode Local CPL

Policy files

Call policy file CPL File

CPL XSD file XSD File

CPL extensions xsd file XSD File

Select the new Call Policy file

Appendix 1: Configuration Details

This appendix summarizes the configuration required for the Cisco Expressway-C.

Cisco Expressway-C System Configuration

Configuration item	Value	Expressway page
System configuration		
System name	EXPC	System > Administration
LAN1 IPv4 address	10.0.0.2	System > Network interfaces > IP
IPv4 gateway	10.0.0.1	System > Network interfaces > IP
LAN1 subnet mask	255.255.255.0	System > Network interfaces > IP
DNS server address 1	10.0.0.11	System > DNS
DNS server address 2	10.0.0.12	System > DNS
DNS Domain name	internal-domain.net	System > DNS
DNS System host name	expc	System > DNS
NTP server 1	10.0.0.21	System > Time
Time zone	GMT	System > Time
Protocol configuration		
SIP domain name	example.com	Configuration > Domains

Cisco Expressway-C transforms and search rules

Configuration item	Value	Expressway page
Transform		
Pattern string	([^\@]*)	Configuration > Dial plan > Transforms
Pattern type	Regex	Configuration > Dial plan > Transforms
Pattern behavior	Replace	Configuration > Dial plan > Transforms
Replace string	\1@example.com	Configuration > Dial plan > Transforms
Local search rule 1		
Rule name	Local zone - no domain	Configuration > Dial plan > Search rules
Priority	48	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	(.+)\@example\.com.*	Configuration > Dial plan > Search rules
Pattern behavior	Replace	Configuration > Dial plan > Search rules

Appendix 1: Configuration Details

Configuration item	Value	Expressway page
Replace string	\1	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	LocalZone	Configuration > Dial plan > Search rules
Local search rule 2		
Rule name	Local zone - full URI	Configuration > Dial plan > Search rules
Priority	50	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	(.+@example\..com.*	Configuration > Dial plan > Search rules
Pattern behavior	Leave	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	LocalZone	Configuration > Dial plan > Search rules

Appendix 2: DNS Records

The following records are required in the local DNS which hosts the internally routable domain: internal-domain.net to allow internal messages to be routed to the Cisco Expressway-C.

Local DNS A Record

Host	Host IP address
expc.internal-domain.net	10.0.0.2

Local DNS SRV Records

Name	Service	Protocol	Priority	Weight	Port	Target host
internal-domain.net.	h323cs	tcp	10	10	1720	expc.internal-domain.net.
internal-domain.net.	h323ls	udp	10	10	1719	expc.internal-domain.net.
internal-domain.net.	h323rs	udp	10	10	1719	expc.internal-domain.net.
internal-domain.net.	sip	tcp	10	10	5060	expc.internal-domain.net.
internal-domain.net.	sip	udp *	10	10	5060	expc.internal-domain.net.
internal-domain.net.	sips	tcp	10	10	5061	expc.internal-domain.net.

* SIP UDP is disabled on Expressway by default.

For example, the DNS records would be:

```
_h323cs._tcp.internal-domain.net. 86400 IN SRV 10 10 1720 expc.internal-domain.net.
_h323ls._udp.internal-domain.net. 86400 IN SRV 10 10 1719 expc.internal-domain.net.
_h323rs._udp.internal-domain.net. 86400 IN SRV 10 10 1719 expc.internal-domain.net.
_sip._tcp.internal-domain.net. 86400 IN SRV 10 10 5060 expc.internal-domain.net.
_sip._udp.internal-domain.net. 86400 IN SRV 10 10 5060 expc.internal-domain.net.
_sips._tcp.internal-domain.net. 86400 IN SRV 10 10 5061 expc.internal-domain.net.
expc.internal-domain.net. 86400 IN A 10.0.0.2
```

Obtaining Documentation and Submitting a Service Request

Use the [Cisco Notification Service](#) to create customized flexible notification alerts to be sent to you via email or by RSS feed.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

© 2016, 2018 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)