Install and Deploy Cisco Jabber Guest

Cisco Jabber Guest is deployed as a virtual server and requires a VMware server to act its host. The server operating system is CentOS. Cisco Jabber Guest is an on-premises deployment: all services are set up, managed, and maintained on your corporate network.

Cisco Jabber Guest is delivered as an OVA image and deployed manually.

Install Cisco Jabber Guest Server

Install Server to vCenter Server

Procedure

Step 1 Download `JabberGuest-10.x.x.x.iso` or access the file from the physical media you receive.

Step 2 Extract the contents from the ISO file.

Step 3 Copy the .OVA to a location on your drive that is accessible to vSphere.

Step 4 Open the vSphere Client.

Step 5 Choose **File** > **Deploy OVF Template**.

Step 6 In the **Source** screen, browse to location of the OVA package, and then click **Next**.
You can enter the URL in the text field if you know it.

Step 7 Verify the details in the **OVF Template Details** screen, and then click **Next**.

Step 8 In the **Name and Location** screen, enter a name for the virtual machine, select its location, and then click **Next**.

Step 9 In the **Host / Cluster** screen, select the virtual machine deployment cluster, and then click **Next**.

Step 10 In the **Storage** screen, select the virtual machine storage usage, and then click **Next**.

Step 11 In the **Disk Format** screen, select a Virtual Machine Disk (VMDK) provisioning format, and then click **Next**.

Step 12 In the **Networking Mapping** screen, select the appropriate Destination Networks for OVA deployment, and then click **Next**.

Step 13 In the **Properties** screen, enter the network settings, and then click **Next**.
The virtual machine is set up with DHCP by default. Provide the following to configure the virtual machine with a static IP address:

- IP address
- Network mask
- Hostname
- Gateway IP address
- At least one DNS server IP address

Important Do not add leading zeros to the IP addresses or the addresses will not resolve as intended.

Step 14 Click **Finish**.

What to Do Next

To turn on the virtual machine after it has been created, in the console window select **Power On**.

Configure the appropriate SIP trunk in Cisco Unified Communications Manager or zones in Cisco TelePresence Video Communication Server depending on the type of server deployed in your network.

Note If the virtual machine cannot acquire the IP address of your VLAN, it shows a bootup failure related to network `eth0`.

Install Server to ESXi, UC Virtualization Foundation, or UC Virtualization Hypervisor

Procedure

Step 1 Download `JabberGuest-10.x.x.x.iso` or access the file from the physical media you receive.

Step 2 Extract the contents from the ISO file.

Step 3 Copy the .OVA to a location on your drive that is accessible to vSphere.

Step 4 Open the vSphere Client.

Step 5 Choose **File** > **Deploy OVF Template**.

Step 6 In the **Source** screen, browse to location of the OVA package, and then click **Next**.
You can enter the URL in the text field if you know it.

Step 7 Verify the details in the **OVF Template Details** screen, and then click **Next**.

Step 8 In the **Name and Location** screen, enter a name for the virtual machine, select its location, and then click **Next**.

Step 9 In the **Disk Format** screen, select a Virtual Machine Disk (VMDK) provisioning format, and then click **Next**.

Step 10 Click **Finish**.

What to Do Next

To turn on the virtual machine after it has been created, in the console window, select **Power On**.

Note The virtual machine is set up with DHCP by default. If you want to configure the virtual machine with a static IP address, edit the following properties: IP address, network mask, hostname, gateway IP address, and at least one DNS server IP address.

Configure the appropriate SIP trunk in Cisco Unified Communications Manager or zones in Cisco TelePresence Video Communication Server depending on the type of server deployed in your network.

Note If the virtual machine cannot acquire the IP address of your VLAN, it shows a boot up failure related to network `eth0`.

Related Topics

Change Virtual Machine Properties of a UC Virtualization Foundation, UC Virtualization Hypervisor, or ESXi-hosted Server

Sign In to Cisco Jabber Guest Administration

The Cisco Jabber Guest server is set up with default credentials.

Before You Begin

You can access Cisco Jabber Guest Administration on Windows with:

- Google Chrome 18 or later
- Microsoft Internet Explorer 8 or later (32-bit, or 64-bit running 32-bit tabs only)
- Mozilla Firefox 10 or later

You can access Cisco Jabber Guest Administration on Mac with:

- Apple Safari 5 or later
- Google Chrome 18 or later
- Mozilla Firefox 10 or later

Your session times out after 30 minutes of inactivity.

Procedure

Step 1 From a compatible browser, navigate to the IP address or host name of your Cisco Jabber Guest server and append `/admin/` to the URL.

Step 2 For **Alias**, enter admin.

Step 3 For **Password**, enter jabbercserver.
The first time that you sign in you must change your password.

Step 4 Enter a new password.

Sign In to Cisco Jabber Guest Server CLI

The Cisco Jabber Guest server command-line interface (CLI) is set up with default credentials.

Procedure

Step 1 For the user ID, enter root.

Step 2 For the password enter jabbercserver. The first time that you sign in, you must change the password.

Step 3 Enter a new password.

Install Certificate

When you install Cisco Jabber Guest, a self-signed certificate is installed by default. If you want, you can:

- Install a certificate that is signed by a third party (a trusted certificate authority).
- Install a certificate with additional distinguished name information.

- Install a certificate that includes the intermediate certificate or the entire certificate trust chain.

Cisco Jabber Guest supports installing DER encoded certificates and PEM encoded certificates.

Important The certificate signing request must be generated on the server on which you install the certificate. For this reason, we recommend that you obtain a new CA-signed certificate for your new install of Cisco Jabber Guest or use a self-signed certificate.

If you choose to use the certificate that is installed by default, you must generate a new self-signed certificate if the hostname of the server changes.

Install Certificate Signed by a Certificate Authority

The following procedure creates a certificate signing request in which the Distinguished Name (DN) information is composed of Common Name=<*ip address*> only. If your organization requires you to include additional DN information in your request, follow the instructions in the procedure, *Install Certificate with Additional Distinguished Name Information*.

If you have deployed a Cisco Jabber Guest cluster, you must install a certificate on each server in the cluster.

When you create the new certificate signing request, the current certificate becomes invalid.

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Local SSL Certificate**.

Step 3 Under **Certificate Signing Request Options**, click **Create a New Certificate Signing Request**.

Step 4 Click **Download a certificate signing request**.
A 4096-bit certificate signing request named `csr.pem` downloads.

Step 5 Send the certificate signing request to a trusted certificate authority.

Step 6 After you receive the signed certificate from the certificate authority:

a) Click **Choose File**.
b) Open the signed certificate.
c) Click **Install a Certificate Authority Signed Certificate**.

Under **Certificate Status**, the following message appears:

```
This system has a certificate authority signed certificate
```

Step 7 Restart the virtual machine:

a) Open vSphere Client.
b) In the virtual machines and templates inventory tree, right-click the virtual machine.
c) Choose **Power** > **Restart Guest**.

Related Topics

Install Certificate with Additional Distinguished Name Information, on page 6

Install Certificate with Additional Distinguished Name Information

If you use Cisco Jabber Guest Administration to create a certificate signing request, the Distinguished Name (DN) information in the request is composed only of Common Name=<*ip address*>. If your organization requires you to include additional DN information, such as organization name and locality name, use the following procedure.

If you have deployed a Cisco Jabber Guest cluster, you must install a certificate on each server in the cluster.

When you create the new certificate signing request, the current certificate becomes invalid.

Procedure

Step 1 Sign in to the server as root.

Step 2 Change directory to `/opt/cisco/webcommon/scripts`:

```
/opt/cisco/webcommon/scripts
```

Step 3 Execute the `createcsr` script:

```
./createcsr.sh
```

Step 4 Follow the instructions on the screen to enter additional DN information, including country name, state or province name, locality name, organization name, organizational unit name, and common name.
After you enter the information, the `csr` file is saved in a location from which you download it in Step 7.

Step 5 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 6 Click **Settings**, and then click **Local SSL Certificate**.

Step 7 Under **Certificate Signing Request Options**, click **Download a certificate signing request**.
A 4096-bit certificate signing request named `csr.pem` downloads.

Step 8 Send the certificate signing request to a trusted certificate authority.

Step 9 After you receive the signed certificate from the certificate authority:

a) Click **Choose File**.
b) Open the signed certificate.
c) Click **Install a Certificate Authority Signed Certificate**.

Under **Certificate Status**, the following message appears:

```
This system has a certificate authority signed certificate
```

Step 10 Restart the virtual machine:

a) Open vSphere Client.
b) In the virtual machines and templates inventory tree, right-click the virtual machine.
c) Choose **Power** > **Restart Guest**.

Install Certificate That Includes the Intermediate Certificate or the Entire Certificate Trust Chain

You can upload a combined certificate file that includes the Cisco Jabber Guest server certificate and your intermediate certificate or that includes the Cisco Jabber Guest server certificate, your intermediate certificate, and your root certificate.

If you have deployed a Cisco Jabber Guest cluster, you must install a certificate on each server in the cluster.

When you create the new certificate signing request, the current certificate becomes invalid.

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Local SSL Certificate**.

Step 3 Under **Certificate Signing Request Options**, click **Create a New Certificate Signing Request**.

Step 4 Click **Download a certificate signing request**.
A 4096-bit certificate signing request named `csr.pem` downloads.

Step 5 Send the certificate signing request to a trusted certificate authority.

Step 6 After you receive the signed certificate from the certificate authority, open it in a text editor, such as Notepad.

Step 7 Download your intermediate certificate.

Step 8 In the Cisco Jabber Guest certificate, after `-----END CERTIFICATE-----`, paste the entire body of your intermediate certificate.

Note Make sure that you include the beginning and end tags of both certificates. The result should look like this:

```
----BEGIN CERTIFICATE-----
(Cisco Jabber Guest certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your intermediate certificate)
-----END CERTIFICATE-----
```

Step 9 (Optional) If you want to include the root certificate in the combined certificate file:

a) Download your root certificate.

b) In the Cisco Jabber Guest certificate, after `-----END CERTIFICATE-----` for the intermediate file, paste the entire body of your root certificate.

Note Make sure that you include the beginning and end tags of all three certificates. The result should look like this:

```
----BEGIN CERTIFICATE-----
(Cisco Jabber Guest certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your intermediate certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your root certificate)
-----END CERTIFICATE-----
```

Step 10 Make sure that there is no additional formatting in the file.

Step 11 Save the combined certificate file.

Step 12 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 13 Click **Settings**, and then click **Local SSL Certificate**.

Step 14 Click **Choose File**, open the combined certificate file, and click **Install a Certificate Authority Signed Certificate**.
Under **Certificate Status**, the following message appears:

```
This system has a certificate authority signed certificate
```

Step 15 Restart the virtual machine:

a) Open vSphere Client.
b) In the virtual machines and templates inventory tree, right-click the virtual machine.
c) Choose **Power** > **Restart Guest**.

Generate New Self-Signed Certificate

If you are using the self-signed certificate that is installed by default and the hostname of the server changes, you must generate a new self-signed certificate.

When you generate a new self-signed certificate, the current certificate becomes invalid.

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Local SSL Certificate**.

Step 3 Click **Generate a New Self-Signed Certificate**.
The message `Update successful` appears.

Step 4 Restart the virtual machine:

a) Open vSphere Client.
b) In the virtual machines and templates inventory tree, right-click the virtual machine.
c) Choose **Power** > **Restart Guest**.

Change Time Zone on Server

By default, the server time zone is set to Coordinated Universal Time (UTC). To change the time zone, use the following procedure.

The time zone change takes effect immediately.

Procedure

Step 1 Sign in to the server as root.

Step 2 Check the current time zone by executing the command: `date`.
The date and time appear in the format: *`ddd mmm dd hh`*`:`*`mm`*`:`*`ss`*` UTC `*`yyyy`*. For example: `Fri Dec 20 16:57:18 UTC 2013`.

Step 3 Change directory to `/opt/cisco/webcommon/scripts`:

```
cd /opt/cisco/webcommon/scripts
```

Step 4 Execute the `timezone` script:

```
./timezone
```

Step 5 Follow the on-screen instructions.

Step 6 At the confirmation message, type 1 for Yes.

Step 7 Verify that the server is set to your time zone by executing the command: `date`.

Step 8 Restart Tomcat:

```
service tomcat-as-standalone.sh restart
```

Deploy Cisco Jabber Guest

Cisco Jabber Guest must be configured to work with the other elements in your network after the server is deployed.

Deployment Options

Cisco Jabber Guest supports two deployments:

- Cisco Expressway-E with a single NIC—SIP traffic goes to the Cisco Expressway-C and media flows over a port range between the Cisco Expressway-E and the Cisco Expressway-C.
- Cisco Expressway-E with dual NIC—SIP traffic goes to the Cisco Expressway-E and media flows through the traversal zone between the Cisco Expressway-E and the Cisco Expressway-C.

Important Only the Cisco Expressway-E with dual NIC deployment supports NAT/PAT between the Cisco Expressway-E and the Cisco Expressway-C.

Lab Deployment

Cisco Jabber Guest can be pointed directly to Cisco Unified Communications Manager for lab deployments only; configure a SIP trunk on Cisco Unified Communications Manager for this deployment. This option is best suited to a lab deployment in which the goal is to familiarize yourself with Cisco Jabber Guest without the additional overhead of configuring Expressway. However, without configuring Expressway, Cisco Jabber Guest is not supported in a production environment.

Network Topology

Overview of Cisco Expressway-E with Single NIC Deployment

- SIP traffic is sent to the Cisco Expressway-C.
- Cisco Expressway-E is single NIC only.
- Cisco Expressway-E in static NAT mode is optional and requires additional configuration on the Cisco Jabber Guest server.
- Cisco Expressway-E is used for TURN services and reverse proxy, not call control.

- Media flows between the Cisco Expressway-E and the Cisco Expressway-C over port range, not a traversal zone.

Overview of Cisco Expressway-E with Dual NIC Deployment

- SIP traffic is sent to the Cisco Expressway-E.
- Cisco Expressway-E is dual NIC only.
- Cisco Expressway-E in static NAT mode is optional and requires additional configuration on the Cisco Jabber Guest server.
- Cisco Expressway-E is used for TURN services, reverse proxy, and call control.
- Media flows between the Cisco Expressway-E and the Cisco Expressway-C through a traversal zone.

In a production environment, Cisco Jabber Guest requires that your Cisco Unified Communications Manager be configured to work with Cisco Expressway.

Note If Cisco Expressway-E is used for reverse proxy functionality, the Cisco Jabber Guest URL looks like `https://`*`expressway-e.example.com`*`/call` where *expressway-e.example.com* is the FQDN of Cisco Expressway-E.

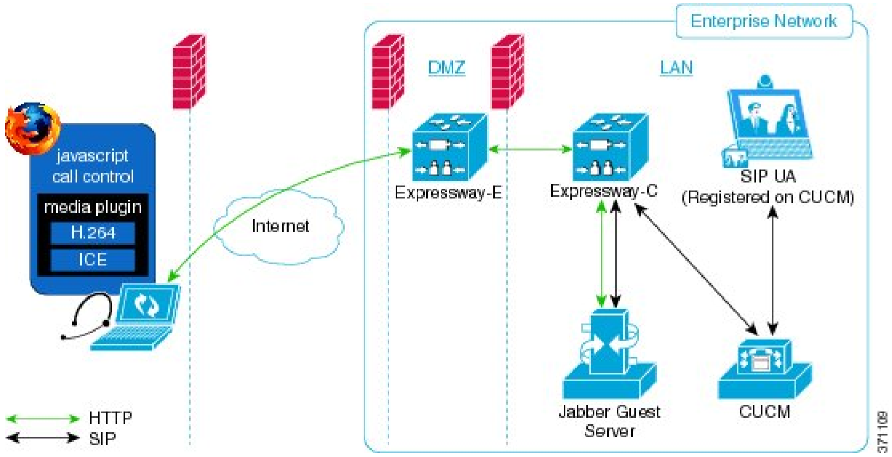
Call Control Flow

Note The mobile and web clients use the same interfaces when interacting with Cisco Expressway/Cisco VCS and Cisco Jabber Guest. To simplify the documentation, we reference only the web client throughout this guide.

Call Control Flow: Cisco Expressway-E with Single NIC Deployment

The following is an example of the call control flow for a Cisco Expressway-E with single NIC deployment of Cisco Jabber Guest Server.

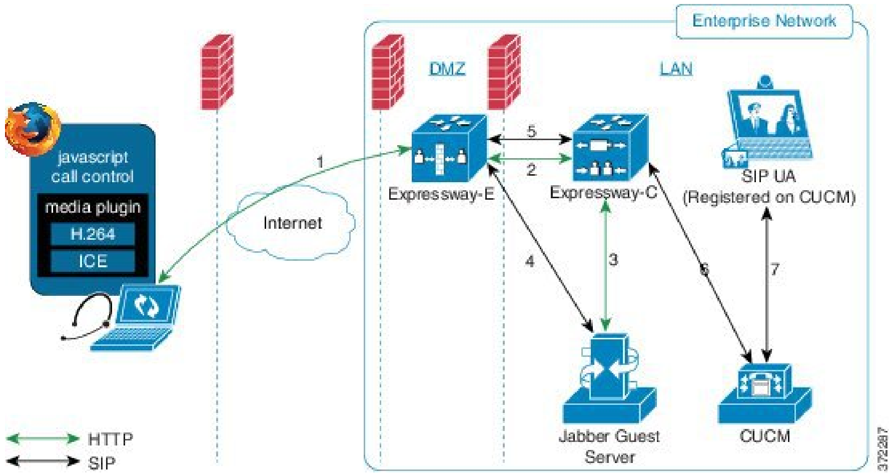
Figure 1: Cisco Jabber Guest Call Control: Cisco Expressway-E with Single NIC Deployment



Call Control Flow: Cisco Expressway-E with Dual NIC Deployment

The following is an example of the call control flow for a Cisco Expressway-E with dual NIC deployment of Cisco Jabber Guest Server.

Figure 2: Cisco Jabber Guest Call Control: Cisco Expressway-E with Dual NIC Deployment



SIP flows between the Cisco Jabber Guest server and the Cisco Expressway-E. This requires bi-directional TCP traffic between the two servers over 5060 (SIP over TCP) or 5061 (SIP over TLS). The SIP traffic then goes over the traversal zone to the Cisco Expressway-C.

We recommend that you disable SIP and H.323 application-level gateways on routers/firewalls carrying network traffic to or from a Cisco Expressway-E.

Important Because media hairpins between the two Cisco Expressway-E NICs, the TURN traffic and SIP traffic must reside on the same Cisco Expressway-E server. You must configure the static NAT address, DMZ external address, and DMZ internal address of the Cisco Expressway-E on the Cisco Jabber Guest server.

Related Topics

Configure Signaling and Media: Cisco Expressway-E with Dual NIC Deployment, on page 26

Media Flow

The web client uses TURN relays allocated on the Cisco Expressway-E to tunnel media into the enterprise. Media is sent and received in STUN encapsulated packets to the TURN server through UDP port 3478.

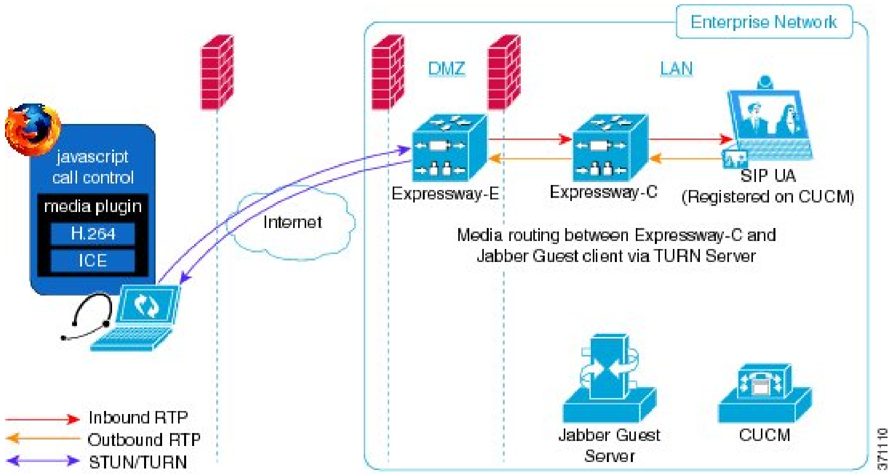
TURN relay credentials are acquired and used as follows:

- The Cisco Jabber Guest client allocates a call resource through HTTP to the Cisco Jabber Guest server.
- The Cisco Jabber Guest server requests short-term TURN credentials from the Cisco Expressway-C through a secure HTTP request. Administrator credentials are used for authentication. The configured domain must be on the Cisco Expressway-C with Jabber Guest service enabled.
- The Cisco Expressway-C creates the TURN credential and passes it to the Cisco Jabber Guest server.
- The Cisco Expressway-C propagates the TURN credential to the Cisco Expressway-E through the SSH tunnel (port 2222).
- The Cisco Jabber Guest server responds to the Cisco Jabber Guest client with the TURN credential and TURN server (Cisco Expressway-E) address (DNS or IP).
- The Cisco Jabber Guestclient uses the TURN credential to allocate the TURN relay on the TURN server.

Media Flow: Cisco Expressway-E with Single NIC Deployment

The following diagram is an example of the media flow for a Cisco Expressway-E with single NIC deployment of Cisco Jabber Guest.

Figure 3: Cisco Jabber Guest Media Flow: Cisco Expressway-E with Single NIC Deployment



Cisco Jabber Guest media does not go through the traversal link between Cisco Expressway-E and Cisco Expressway-C.

Important If the Cisco Expressway-E is behind a NAT, additional configuration is required on the Cisco Jabber Guest server to avoid the media flowing to the static NAT address. Turn on **Static NAT mode** and configure the static NAT address and DMZ external address of the Cisco Expressway-E on the Cisco Jabber Guest server. This allows media to be sent to the DMZ external address of the Cisco Expressway-E, avoiding NAT reflection on the outside firewall.

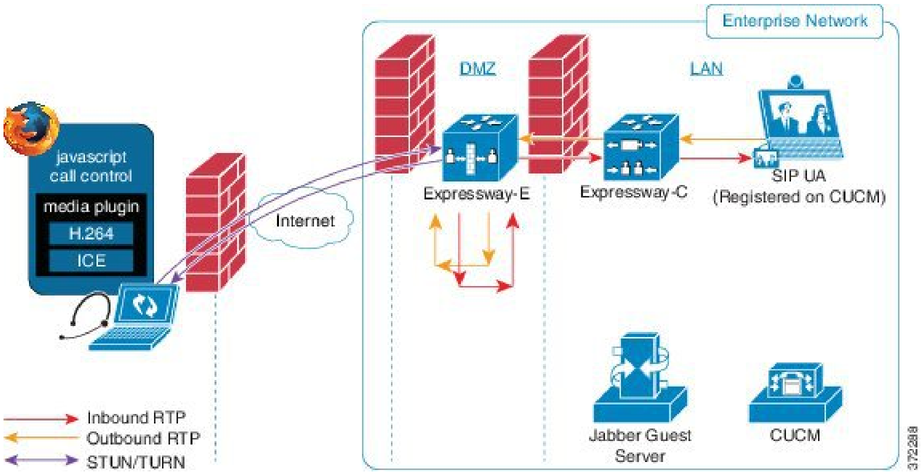
Related Topics

Configure Static NAT Mode on Cisco Expressway-E, on page 27

Media Flow: Cisco Expressway-E with Dual NIC Deployment

The following diagram is an example of the media flow for a Cisco Expressway-E with dual NIC deployment of Cisco Jabber Guest.

Figure 4: Cisco Jabber Guest Media Flow: Cisco Expressway-E with Dual NIC Deployment



Media flows through the traversal zone between the Cisco Expressway-C and the internal NIC of the Cisco Expressway-E. It hairpins on the Cisco Expressway-E to the external NIC of the Cisco Expressway-E, and then is STUN/TURN wrapped before being sent to the client browser.

Important If the Cisco Expressway-E is behind a NAT, additional configuration is required on the Cisco Jabber Guest server to avoid the media flowing to the static NAT address. Turn on **Static NAT mode** and configure the static NAT address, DMZ external address, and DMZ internal address of the Cisco Expressway-E on the Cisco Jabber Guest server. This allows media to be sent to the DMZ external address of the Cisco Expressway-E, avoiding NAT reflection on the outside firewall.

Related Topics

Configure Static NAT Mode on Cisco Expressway-E, on page 27

Ports and Protocols

Important

- HTTP and HTTPS traffic from Cisco Jabber Guest clients in the Internet is sent to ports 80 and 443 TCP respectively. Therefore the firewall between the Cisco Expressway-E and the public Internet must translate destination port 80 to 9980 and destination port 443 to 9443 for all TCP traffic that targets the Cisco Expressway-E address.
- The Cisco Expressway-E redirects HTTP requests on port 9980 to HTTPS on 9443.
- 80/443 TCP are the standard HTTP/S administration interfaces on the Expressway. If the Cisco Expressway-E is administered from systems located in the Internet, then the firewall translation must also distinguish by source address and must not translate the destination port of traffic arriving from those management systems.
- You also need to ensure that appropriate DNS records exist so that the Cisco Jabber Guest client can reach the Cisco Expressway-E. The FQDN of the Cisco Expressway-E in DNS must include the Cisco Jabber Guest domain. The Cisco Jabber Guest domain is the domain that is configured on the Cisco Expressway-C.

Ports and Protocols: Cisco Expressway-E with Single NIC Deployment

Table 1: Inbound from Public Internet to Cisco Expressway-E (DMZ)

Purpose	Protocol	Internet Endpoint (Source)	Cisco Expressway-E (Listening)
HTTP	TCP	TCP source port	9980 (read the following *Important* note)
HTTPS proxy	TLS	TCP source port	9443 (read the following *Important* note)
TURN server control/media	UDP	UDP source port	3478–3483 (control and media sent to this port)

Important

- The Cisco Expressway-E administrator currently uses port 80 and therefore, incoming requests from the Cisco Jabber Guest client to Cisco Expressway-E on port 80 must be remapped to port 9980 using a firewall (or similar) in front of Cisco Expressway-E. For the mobile client, using `9980` in call links is not supported; you must use port remapping on your firewall to remap port 80 to port 9980.
- The Cisco Expressway-E administrator currently uses port 443 and therefore, incoming requests from the Cisco Jabber Guest client to Cisco Expressway-E on port 443 must be remapped to port 9443 using a firewall (or similar) in front of Cisco Expressway-E. For the mobile client, using `9443` in call links is not supported; you must use port remapping on your firewall to remap port 443 to port 9443.

Table 2: Outbound from Cisco Expressway-C (Private) to Cisco Expressway-E (DMZ)

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Expressway-E (Destination)
SSH (HTTP/S tunnels)	TCP	Ephemeral port	2222 (not configurable)
Traversal zone SIP signaling	TLS	25000–29999	7001
Media[1]	UDP	36000–59999	24000–29999[2] 60000–61799[3]

[1] By default, media is sent to the NAT interface unless the Cisco Jabber Guest server is configured for static NAT mode.

[2] For fresh installs of Cisco Expressway-E 8.*x*.

[3] If you upgraded Cisco Expressway-E from 7.*x*.

Table 3: Inbound from Cisco Expressway-E (DMZ) to Cisco Expressway-C (Private)

Purpose	Protocol	Cisco Expressway-E (Source)	Cisco Expressway-C (Destination)
Media	UDP	24000–29999[4] 60000–61799[5]	36000–59999

[4] For fresh installs of Cisco Expressway-E 8.*x*.

[5] If you upgraded Cisco Expressway-E from 7.*x*.

Important

- Inbound firewall rules are required to allow media to flow from the Cisco Expressway-E to Cisco Expressway-C.
- You may find that two-way media can still be established even if the inbound from Cisco Expressway-E (DMZ) to Cisco Expressway-C (private) firewall rules are not applied. This is because the outbound media creates a pinhole in the firewall; however, these rules are required to support uni-directional media (that is, only from outside to inside).

Table 4: From Cisco Expressway-C to Cisco Jabber Guest

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Jabber Guest (Destination)
HTTP	TCP	Ephemeral port	80
HTTPS	TLS	Ephemeral port	443
SIP	TCP/TLS	Ephemeral port	5060 (SIP over TCP) 5061 (SIP over TLS)

Table 5: From Cisco Jabber Guest to Cisco Expressway-C

Purpose	Protocol	Cisco Jabber Guest (Source)	Cisco Expressway-C (Destination)
HTTPS	TLS	Ephemeral port	443
SIP	TCP/TLS	Ephemeral port	5060 (SIP over TCP) 5061 (SIP over TLS)

Ports and Protocols: Cisco Expressway-E with Dual NIC Deployment

Table 6: Inbound from Public Internet to Cisco Expressway-E (DMZ)

Purpose	Protocol	Internet Endpoint (Source)	Cisco Expressway-E (Listening)
HTTP	TCP	TCP source port	9980 (read the following *Important* note)
HTTPS proxy	TLS	TCP source port	9443 (read the following *Important* note)

Purpose	Protocol	Internet Endpoint (Source)	Cisco Expressway-E (Listening)
TURN server control/media	UDP	UDP source port	3478–3483 (control and media sent to this port)

Important

- The Cisco Expressway-E administrator currently uses port 80 and therefore, incoming requests from the Cisco Jabber Guest client to Cisco Expressway-E on port 80 must be remapped to port 9980 using a firewall (or similar) in front of Cisco Expressway-E. For the mobile client, using `9980` in call links is not supported; you must use port remapping on your firewall to remap port 80 to port 9980.
- The Cisco Expressway-E administrator currently uses port 443 and therefore, incoming requests from the Cisco Jabber Guest client to Cisco Expressway-E on port 443 must be remapped to port 9443 using a firewall (or similar) in front of Cisco Expressway-E. For the mobile client, using `9443` in call links is not supported; you must use port remapping on your firewall to remap port 443 to port 9443.

Table 7: Outbound from Cisco Expressway-C (Private) to Cisco Expressway-E (DMZ)

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Expressway-E (Destination)
SSH (HTTP/S tunnels)	TCP	Ephemeral port	2222 (not configurable)
Traversal zone SIP signaling	TLS	25000–29999	7001
Media **Note** If the internal > DMZ firewall rules allow outgoing traffic, no rules are needed for media.	UDP	36002–59999[6] 36002–59999[7] 50000–54999[8]	36000–36001[9] 36000–36011[10]

[6] For Cisco Expressway-C 8.1 or later.

[7] For large deployments of Cisco Expressway-C 8.1 or later.

[8] If Cisco Expressway-C is upgraded from 7.1.

[9] For Cisco Expressway-E 8.1 or later.

[10] For large deployments of Cisco Expressway-E 8.1 or later.

Table 8: Outbound from Cisco Jabber Guest (Private) to Cisco Expressway-E (DMZ)

Purpose	Protocol	Cisco Jabber Guest (Source)	Cisco Expressway-E (Destination)
SIP	TCP/TLS	Ephemeral port	5060 (SIP over TCP) 5061 (SIP over TLS)

Table 9: Inbound from Cisco Expressway-E (DMZ) to Cisco Jabber Guest (Private)

Purpose	Protocol	Cisco Expressway-E (Source)	Cisco Jabber Guest (Destination)
SIP	TCP/TLS	Ephemeral port	5060 (SIP over TCP) 5061 (SIP over TLS)

Table 10: From Cisco Expressway-C to Cisco Jabber Guest

Purpose	Protocol	Cisco Expressway-C (Source)	Cisco Jabber Guest (Destination)
HTTP	TCP	Ephemeral port	80
HTTPS	TLS	Ephemeral port	443

Table 11: From Cisco Jabber Guest to Cisco Expressway-C

Purpose	Protocol	Cisco Jabber Guest (Source)	Cisco Expressway-C (Destination)
HTTPS	TLS	Ephemeral port	443

Configure Cisco Expressway-E and Cisco Expressway-C

Do one of the following:

- Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Single NIC Deployment, on page 20
- Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Dual NIC Deployment, on page 22

Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Single NIC Deployment

Cisco Expressway-E and Cisco Expressway-C provide the following functionality:

- Both provide reverse proxy for HTTPS traffic.
- Cisco Expressway-E provides TURN relays.
- Cisco Expressway-C routes calls to Cisco Unified Communications Manager through a SIP trunk.

Before You Begin

Follow the instructions in the Cisco Expressway documentation to set up Cisco Expressway security certificates and a Unified Communications traversal zone. Configure the traversal zone type between the Cisco Expressway-C and Cisco Expressway-E as *Unified Communications traversal*.

Procedure

Step 1 On the Cisco Expressway-E, enable Cisco Jabber Guest support:

a) Choose **Configuration** > **Unified Communications** > **Configuration**.
b) From the **Unified Communications mode** drop-down list, select **Jabber Guest services**.
c) Click **Save**.

Step 2 On the Cisco Expressway-E, enable TURN service:

a) Choose **Configuration** > **Traversal** > **TURN**.
b) From the **TURN services** drop-down list, select **On**.
c) Click **Save**.

Step 3 On the Cisco Expressway-C, enable Cisco Jabber Guest support:

a) Choose **Configuration** > **Unified Communications** > **Configuration**.
b) From the **Unified Communications mode** drop-down list, select **Jabber Guest services**.
c) Click **Save**.

Step 4 On the Cisco Expressway-C, configure the domain for which HTTP traffic will be routed to the Cisco Jabber Guest server:
This domain is the outward-facing domain that is used to route the call on the Internet when users click a link.

a) Choose **Configuration** > **Domains**.
b) Create a new domain if none exist or, in the row of the target domain, click **View/Edit**.
c) From the **Jabber Guest** drop-down list, select **On**.
d) Click **Save**.
e) Repeat Step 5.a. through Step 5.d. for each domain.

Step 5 Make sure that the domain has an associated DNS record that resolves to the Cisco Expressway-E. The domain information is propagated from the Cisco Expressway-C to the Cisco Expressway-E through the SSH tunnel (port 2222). It is used by the Cisco Expressway-E to validate incoming HTTP requests for the Cisco Jabber Guest service.

Step 6 On the Cisco Expressway-C, associate the Cisco Jabber Guest servers with the domain:
This allows the Cisco Expressway-C to route HTTP requests with this domain to the appropriate Cisco Jabber Guest server.

a) Choose **Configuration** > **Unified Communications** > **Configuration**.
b) In the **Advanced** section, click **Configure Jabber Guest servers**.
c) Click **New**.
d) For **Server hostname**, enter the FQDN of the Cisco Jabber Guest server.
e) For **Priority**, enter the priority of the Cisco Jabber Guest server. Lower numbers have higher priority. Make sure that all Cisco Jabber Guest servers have a different priority so that calls are only sent to one Cisco Jabber Guest server in the deployment at a time.
f) From the **Domain** drop-down list, select the Cisco Jabber Guest HTTP domain.
g) Click **Create entry**.
h) Repeat Step 6.c. through Step 6.g. for each Cisco Jabber Guest server in the cluster.

Step 7 Verify that the SSH tunnel is active:

a) On either the Cisco Expressway-C or the Cisco Expressway-E, choose **Status** > **Unified Communications**.
b) Click **View ssh tunnel status**.
c) Make sure that the Cisco Jabber Guest domain is listed and that the SSH tunnel is active.

Step 8 On the Cisco Expressway-C, create a neighbor zone for each Cisco Jabber Guest server:

a) Choose **Configuration** > **Zones** > **Zones**.
b) Click **New**.
c) Enter the details. From the **Type** drop-down list, select **Neighbor**.
d) In the **H.323** section, from the **Mode** drop-down list, select **Off**
e) In the **SIP** section, from the **Mode** drop-down list, select **On**.
f) For **Port**, enter 5061.
g) From the **Transport** drop-down list, select TLS.

Note To enable TLS, you must also upload the Cisco Expressway-C certificate to Cisco Jabber Guest Administration. For more information, see Configure Signaling and Media: Cisco Expressway-E with Single NIC Deployment, on page 24.

h) From the **Media encryption mode** drop-down list, select **Best effort**.

Important Selecting *Best effort* forces media from the Cisco Expressway-E to terminate on the Cisco Expressway-C.

i) From the **ICE support** drop-down list, select **Off**.
j) In the **Location** section, for **Peer 1 address**, enter the IP address or FQDN of the Cisco Jabber Guest server.
k) In the **Advanced** section, from the **Zone profile** drop-down list, select **Default**.
l) Click **Create zone**.
m) Repeat Step 7.b. through 7.l. for each Cisco Jabber Guest server in a Cisco Jabber Guest cluster.
Do not configure any search rules for these neighbor zones. These zones are used to receive traffic only.

Step 9 Set up a connection between the Cisco Expressway-C and Cisco Unified Communications Manager:

a) On Cisco Unified Communications Manager, set up a non-secure or secure SIP trunk and point it to the Cisco Expressway-C.
b) On Cisco Expressway-C, set up a neighbor zone and point it to Cisco Unified Communications Manager.

Follow the steps in the *Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide*.

Step 10 Create a search rule on Cisco Expressway-C to route calls to Cisco Unified Communications Manager.

Step 11 Force the protocol between the Cisco Jabber Guest server and the Cisco Expressway-C to be http:

a) Sign in to the Cisco Expressway-C command-line interface as an administrator. In a clustered Cisco Expressway-C deployment, sign in to the master Cisco Expressway-C.
b) Enter the following command:

```
xconf CollaborationEdge JabbercProxyProtocol: http
```

HTTP request goes from the Cisco Expressway-E to the Cisco Expressway-C to the Cisco Jabber Guest server.

Related Topics

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html
Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide

Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Dual NIC Deployment

Cisco Expressway-E and Cisco Expressway-C provide the following functionality:

- Both provide reverse proxy for HTTPS traffic.
- Cisco Expressway-E provides TURN relays.
- Cisco Expressway-C routes calls to Cisco Unified Communications Manager through a SIP trunk.

Before You Begin

Follow the instructions in the Cisco Expressway documentation to set up Cisco Expressway security certificates and a Unified Communications traversal zone. Configure the traversal zone type between the Cisco Expressway-C and Cisco Expressway-E as *Unified Communications traversal*.

Procedure

Step 1 On the Cisco Expressway-E, enable Cisco Jabber Guest support:

a) Choose **Configuration** > **Unified Communications** > **Configuration**.
b) From the **Unified Communications mode** drop-down list, select **Jabber Guest services**.
c) Click **Save**.

Step 2 On the Cisco Expressway-E, enable TURN service:

a) Choose **Configuration** > **Traversal** > **TURN**.
b) From the **TURN services** drop-down list, select **On**.
c) Click **Save**.

Step 3 On the Cisco Expressway-C, enable Cisco Jabber Guest support:

a) Choose **Configuration** > **Unified Communications** > **Configuration**.
b) From the **Unified Communications mode** drop-down list, select **Jabber Guest services**.
c) Click **Save**.

Step 4 On the Cisco Expressway-C, configure the domain for which HTTP traffic routes to the Cisco Jabber Guest server:
This domain is the outward-facing domain that is used to route the call on the Internet when users click a link.

a) Choose **Configuration** > **Domains**.
b) Create a new domain if none exist or, in the row of the target domain, click **View/Edit**.
c) From the **Jabber Guest** drop-down list, select **On**.
d) Click **Save**.
e) Repeat Step 5.a. through Step 5.d. for each domain.

Step 5 Make sure that the domain has an associated DNS record that resolves to the Cisco Expressway-E. The domain information is propagated from the Cisco Expressway-C to the Cisco Expressway-E through the SSH tunnel (port 2222). The information is used by the Cisco Expressway-E to validate incoming HTTP requests for the Cisco Jabber Guest service.

Step 6 On the Cisco Expressway-C, associate the Cisco Jabber Guest servers with the domain:
This allows the Cisco Expressway-C to route HTTP requests with this domain to the appropriate Cisco Jabber Guest server.

a) Choose **Configuration** > **Unified Communications** > **Configuration**.
b) In the **Advanced** section, click **Configure Jabber Guest servers**.
c) Click **New**.
d) For **Server hostname**, enter the FQDN of the Cisco Jabber Guest server.
e) For **Priority**, enter the priority of the Cisco Jabber Guest server. Lower numbers have higher priority. Give each Cisco Jabber Guest server a different priority so that calls are only sent to one Cisco Jabber Guest server in the deployment at a time.
f) From the **Domain** drop-down list, select the Cisco Jabber Guest HTTP domain.
g) Click **Create entry**.
h) Repeat Step 6.c. through Step 6.g. for each Cisco Jabber Guest server in the cluster.

Step 7 Verify that the SSH tunnel is active:

a) On either the Cisco Expressway-C or the Cisco Expressway-E, choose **Status** > **Unified Communications**.
b) Click **View ssh tunnel status**.
c) Make sure that the Cisco Jabber Guest domain is listed and that the SSH tunnel is active.

Step 8 On the Cisco Expressway-E, create a neighbor zone for each Cisco Jabber Guest server so that you can verify that the zone between the Cisco Expressway-E and the Cisco Jabber Guest server is active:

a) Choose **Configuration** > **Zones** > **Zones**.
b) Click **New**.
c) Enter the details. From the **Type** drop-down list, select **Neighbor**.
d) In the **H.323** section, from the **Mode** drop-down list, select **Off**
e) In the **SIP** section, from the **Mode** drop-down list, select **On**.
f) For **Port**, enter 5061.
g) From the **Transport** drop-down list, select TLS.

Note To enable TLS, you must also upload the Cisco Expressway-C certificate to Cisco Jabber Guest Administration. For more information, see Configure Signaling and Media: Cisco Expressway-E with Dual NIC Deployment, on page 26.

h) From the **Media encryption mode** drop-down list, select **Best effort**.
i) From the **ICE support** drop-down list, select **Off**.
j) In the **Location** section, for **Peer 1 address**, enter the IP address or FQDN of the Cisco Jabber Guest server.
k) In the **Advanced** section, from the **Zone profile** drop-down list, select **Default**.
l) Click **Create zone**.
m) Repeat Step 7.b. through 7.l. for each Cisco Jabber Guest server in a Cisco Jabber Guest cluster.

Do not configure any search rules for these neighbor zones. These zones are used to receive traffic only.

Step 9 Create a search rule for the traversal zone between the Cisco Expressway-E and the Cisco Expressway-C servers.

Important For proper call routing, the SIP domain that you specify (click **Settings**, click **Call Control and Media**) and the domain that you optionally specify for **Destination** when you create a link (click **Links**, click **New**) must be configured on the Cisco Expressway-E search rule to point to the traversal zone.

Step 10 Set up a connection between the Cisco Expressway-C and Cisco Unified Communications Manager:

a) On Cisco Unified Communications Manager, set up a non-secure or secure SIP trunk and point it to the Cisco Expressway-C.

b) On Cisco Expressway-C, set up a neighbor zone and point it to Cisco Unified Communications Manager.

Follow the steps in the *Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide*.

Step 11 Create a search rule on Cisco Expressway-C to route calls to Cisco Unified Communications Manager.

Step 12 Force the protocol between the Cisco Jabber Guest server and the Cisco Expressway-C to be http:

a) Sign in to the Cisco Expressway-C command-line interface as an administrator. In a clustered Cisco Expressway-C deployment, you must sign in to the master Cisco Expressway-C.

b) Enter the following command:

```
xconf CollaborationEdge JabbercProxyProtocol: http
```

HTTP request goes from the Cisco Expressway-E to the Cisco Expressway-C to the Cisco Jabber Guest server.

Related Topics

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html

Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide

Configure Cisco Jabber Guest

Configure Signaling and Media

Do one of the following:

- Configure Signaling and Media: Cisco Expressway-E with Single NIC Deployment, on page 24
- Configure Signaling and Media: Cisco Expressway-E with Dual NIC Deployment, on page 26

Configure Signaling and Media: Cisco Expressway-E with Single NIC Deployment

We recommend enabling Session Initiation Protocol (SIP) over Transport Layer Security (TLS) for call control signaling and enabling Secure Real-Time Transfer Protocol (SRTP) for secure media. Secure media requires secure signaling.

Before You Begin

On Cisco Expressway-C, make sure that you have created a neighbor zone for each Cisco Jabber Guest server. For more information, see Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Single NIC Deployment, on page 20.

Procedure

Step 1 To enable SIP over TLS, obtain the Cisco Expressway-C server certificate or the Cisco Expressway-C certificate authority certificate:

- If you have a single Cisco Expressway-C, obtain the Cisco Expressway-C server certificate.
- If Cisco Expressway-C is a cluster of servers, obtain the Cisco Expressway-C certificate authority certificate. This certificate must be uploaded to the Cisco Jabber Guest server so that Cisco Jabber Guest can communicate with all nodes in the Cisco Expressway-C cluster.

Step 2 Upload the certificate to Cisco Jabber Guest Administration:

a) Sign in to Cisco Jabber Guest Administration as an administrator.
b) Click **Settings**, and then click **Secure SIP Trust Certificate**.
c) Under **Secure SIP Trust Certificate**, click **Choose File**.
d) Select the certificate that you obtained, and then click **Upload**.

Step 3 Configure the **Call Control and Media** settings in Cisco Jabber Guest Administration:

a) Click **Call Control and Media**.
b) Select **Route calls using Cisco Expressway**.
c) Check **Enable SIP over TLS**.
d) Check **Enable SRTP**.
e) For **SIP port**, enter 5061.
f) For **SIP domain**, enter the SIP domain. This setting is used if the Cisco Jabber Guest link does not contain a SIP domain. In most cases, this is the enterprise SIP domain as configured in Cisco Unified Communications Manager.
g) For **SIP server**, enter the IP address or FQDN of the Cisco Expressway-C.
h) Specify whether SIP is sent to the Cisco Expressway-C that originated the HTTP call control or to the server entered above.

Step 4 Click **Update**.
The message `Update successful` appears.

Step 5 Restart Tomcat:

```
service tomcat-as-standalone.sh restart
```

Step 6 On the Cisco Expressway-C, verify that the neighbor zones for each Cisco Jabber Guest server are active:

a) Choose **Configuration** > **Zones** > **Zones**.
b) View the **SIP status** column.

Configure Signaling and Media: Cisco Expressway-E with Dual NIC Deployment

We recommend enabling Session Initiation Protocol (SIP) over Transport Layer Security (TLS) for call control signaling and enabling Secure Real-Time Transfer Protocol (SRTP) for secure media. Secure media requires secure signaling.

Before You Begin

On Cisco Expressway-C, make sure that you have created a neighbor zone for each Cisco Jabber Guest server. For more information, see Configure Cisco Expressway-E and Cisco Expressway-C: Cisco Expressway-E with Dual NIC Deployment, on page 22.

Procedure

Step 1 To enable SIP over TLS, obtain the Cisco Expressway-E server certificate or the Cisco Expressway-E certificate authority certificate:

- If you have a single Cisco Expressway-E, obtain the Cisco Expressway-E server certificate.
- If Cisco Expressway-E is a cluster of servers, obtain the Cisco Expressway-E certificate authority certificate. This certificate must be uploaded to the Cisco Jabber Guest server so that Cisco Jabber Guest can communicate with all nodes in the Cisco Expressway-E cluster.

Step 2 Upload the certificate to Cisco Jabber Guest Administration:

a) Sign in to Cisco Jabber Guest Administration as an administrator.
b) Click **Settings**, and then click **Secure SIP Trust Certificate**.
c) Under **Secure SIP Trust Certificate**, click **Choose File**.
d) Select the certificate that you obtained, and then click **Upload**.

Step 3 Configure the **Call Control and Media** settings in Cisco Jabber Guest Administration:

a) Click **Call Control and Media**.
b) Select **Route calls using Cisco Expressway**.
c) Check **Enable SIP over TLS**.
d) Check **Enable SRTP**.
e) For **SIP port**, enter 5061.
f) For **SIP domain**, enter the SIP domain. This setting is used if the Cisco Jabber Guest link does not contain a SIP domain. In most cases, this is the enterprise SIP domain as configured in Cisco Unified Communications Manager.

   Important For proper call routing, the SIP domain must be configured on the Cisco Expressway-E search rule to point to the traversal zone.

g) For a single Cisco Expressway-E server, for **SIP server**, enter the IP address or FQDN of the Cisco Expressway-E.
h) Select where to send SIP traffic:

   - For a single Cisco Expressway-E server, select **SIP server specified above**.
   - For cluster of Cisco Expressway-E servers:

     1. Select **Expressway-E server that provided TURN service**.

        Important The TURN relay and SIP signaling must reside on the same server.

2 Under **Cisco Expressway-E Network Address Map**, enter the external IP addresses and internal IP addresses of each of the Cisco Expressway-E servers in the cluster. Mapping allows the Cisco Jabber Guest server to send the SIP to the same Cisco Expressway-E servers as the TURN relay.

If static NAT mode is enabled on Cisco Expressway-E with either single NIC deployment or dual NIC deployment, the Cisco Jabber Guest server must be configured for static NAT mode as well.

Step 4 Click **Update**.
The message `Update successful` appears.

Step 5 Restart Tomcat:

```
service tomcat-as-standalone.sh restart
```

Step 6 On the Cisco Expressway-E, verify that the neighbor zones for each Cisco Jabber Guest server are active:

a) Choose **Configuration** > **Zones** > **Zones**.

b) View the **SIP status** column.

Configure Static NAT Mode on Cisco Expressway-E

If static NAT mode is enabled on Cisco Expressway-E with either single NIC deployment or dual NIC deployment, the Cisco Jabber Guest server must be configured for static NAT mode as well. This allows the media to flow within the DMZ, avoiding NAT reflection (sending media to the NATed address).

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration.

Step 2 Click **Settings**, and then click **Call Control and Media**.

Step 3 Under **Cisco Expressway-E Network Address Map**, check **Static NAT mode**.
This check box appears only when the option,**Route calls using Cisco Expressway**, is selected.

Step 4 Under **Public IP (Static NAT)**, enter the static NAT IP address of the Cisco Expressway-E server.

Step 5 Under **External IP (DMZ)**, enter the external IP address of the Cisco Expressway-E server.

Step 6 Repeat Steps 4 and 5 for each of the Cisco Expressway-E servers in the cluster.

Step 7 Click **Update**.

Configure TURN Credential Provisioning

The Cisco Jabber Guest client needs TURN credentials to allocate TURN relays on the Cisco Expressway-E. The Cisco Jabber Guest server provisions these credentials on the Cisco Expressway-C when the Cisco Jabber Guest client connects.

The Cisco Jabber Guest server uses an HTTP-based XML API to communicate with Cisco Expressway-C.

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Call Control and Media**.

Step 3 Under **Cisco Expressway-C**, for **Expressway-C (IP address or DNS name)**, enter the Cisco Expressway-C IP address or DNS name.

Step 4 Specify whether short-term TURN credentials are requested from the Cisco Expressway-C that proxied the HTTP request from the Cisco Jabber Guest client or from the server entered in Step 3.

Step 5 For **HTTPS port**, specify the port.

Step 6 For **Domain**, enter the domain on Cisco Expressway-C that has Jabber Guest services enabled.

Step 7 For **Username** and **Password**, enter the username and password of the administrator account on Cisco Expressway-C that has read, write, and API access.

Step 8 Click **Update**.

Set Up TURN Server Information

The Cisco Jabber Guest client needs to know which Cisco Expressway-E to use for TURN relays.

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Call Control and Media**.

Step 3 Under **Cisco Expressway-E**, for **Expressway-E TURN server (IP address or DNS name)**, enter the Cisco Expressway-E TURN server outside IP address or DNS name.

Step 4 For **TURN port**, enter the UDP port. The port is typically 3478 but you can enter a range of ports, such as 3478-3483. The range is necessary if the Cisco Expressway-E supports multiple TURN ports.

Important The port must match the port specified on the Cisco Expressway-E (under **Configuration** > **Traversal** > **TURN**).

Step 5 Click **Update**.

Set FQDN of Cisco Jabber Guest Server

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Call Control and Media (Local)**.

Step 3 Enter the FQDN of the Cisco Jabber Guest server.

Important The FQDN must match the value specified in the Cisco Jabber Guest **Server hostname** field on the Cisco Expressway-C. Cisco Expressway-C uses the FQDN to forward the per-session HTTP traffic to the appropriate Cisco Jabber Guest server in the cluster.

Step 4 Click **Update**.

What to Do Next

Make sure that you populate the **Cisco Jabber Guest local FQDN** field for each node in the Cisco Jabber Guest cluster.

Set Domain Used for Links

To create links on the Cisco Jabber Guest server, you must enter the domain that is configured on the Cisco Expressway.

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Links**.

Step 3 For **Domain used for links**, enter the the public DNS name of the Cisco Expressway-E. You can add a subdomain for Cisco Jabber Guest service.

Example:
If `yourcompany.com` is configured as the domain on the Cisco Expressway and `jg.yourcompany.com` is configured on the Cisco Jabber Guest server, the format of the link is `https://jg.yourcompany.com/call/`*`<directory number>`*.

Step 4 Click **Update**.

Change MTU Size

In some call scenarios, such as when using VPN, the default Maximum Transmission Unit (MTU) on Cisco Expressway-E is too high and can cause packet loss. The default MTU is 1500 bytes. We recommend that you lower the MTU to 1400 bytes. If you do not, callers may experience problems, such as one-way video.

Procedure

Step 1 On Cisco Expressway-E, do one of the following:

- If you have Cisco Expressway-E 8.2, choose **System** > **IP**.

- If you have Cisco Expressway-E 8.5 or later, choose **System** > **Network Interfaces** > **IP**.

Step 2 In the **LAN 1** section, for **Maximum transmission unit (MTU)**, enter 1400.

Step 3 Click **Save**.

Configure Load Balancing

You can balance the load on your Cisco Expressway-C, Cisco Expressway-E, and Cisco Jabber Guest server clusters.

The following table describes the methods of load balancing that are available to distribute different types of traffic across the network.

Table 12: Load Balancing Methods

Network Traffic		**Method of Load Balancing Available**
SIP for call control	Send SIP to the Cisco Expressway-C server cluster	• Round-robin DNS • Round-robin comma-separated values (CSV) • HTTP
	Send SIP to the Cisco Expressway-E server cluster	Send SIP to the Cisco Expressway-E server that provided TURN service **Important** For a clustered Cisco Expressway-E with dual NIC deployment. you must send SIP to the Cisco Expressway-E server that provided TURN service.
TURN credential provisioning requests to the Cisco Expressway-C server cluster		• Round-robin DNS • Round-robin CSV • HTTP
HTTPS from the Cisco Jabber Guest client to the Cisco Expressway-E server cluster		Round-robin DNS

Network Traffic	Method of Load Balancing Available
TURN for media between the Cisco Jabber Guest client and the Cisco Expressway-E server cluster	• Round-robin DNS for the Cisco Expressway-E server IP address and port range for round-robin TURN port range • Round-robin CSV for the Cisco Expressway-E server IP address and port range for round-robin TURN port range **Important** TURN port ranges are only supported when you use the large Cisco Expressway-E virtual machine.
HTTP between the Cisco Expressway-E and Cisco Jabber Guest server clusters	Configure Cisco Jabber Guest server priorities on the Cisco Expressway-C server.

Related Topics

Round-Robin DNS Load Balancing, on page 31
Configure Round-Robin CSV Loading Balancing, on page 33
Configure HTTP Load Balancing, on page 34
Configure Round-Robin TURN Port Range Load Balancing, on page 34

Round-Robin DNS Load Balancing

With round-robin DNS load balancing, a DNS server returns an ordered list of IP addresses associated with a single host name. With each new query on that host name, the DNS server rotates through the list. Multiple servers at different IP addresses take turns handling new requests to provide the same service.

For TURN traffic, an advantage of round-robin DNS load balancing is that it also provides redundancy. If a TURN server is down or unreachable, the client will try another server.

Note The order of the IP address list returned for a DNS lookup is difficult to predict if the DNS server is under any kind of load directed at the host name. The important thing to expect is that calls to the host name will go to different servers over time.

Procedure

Step 1 Make sure that the DNS server has round-robin enabled.

Step 2 Make sure that the FQDNs for the Cisco Expressway-C and Cisco Expressway-E clusters are configured on the DNS server to round-robin through the IP addresses of the server cluster.

Step 3 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 4 Click **Settings**, and then click **Call Control and Media**.

Step 5 To set up round-robin DNS for the SIP server:

a) In the **SIP server** field, enter the FQDN of the Cisco Expressway-C cluster.
b) Next to **Send SIP traffic to**, click **SIP server specified above**.

Step 6 To set up round-robin DNS to request short-term TURN credentials from Cisco Expressway-C:

a) In the **Expressway-C (IP address or DNS name)** field, enter the FQDN of the Cisco Expressway-C cluster.
b) Next to **Request short-term TURN credentials from**, click **Expressway-C server specified above**.

Step 7 To set up round-robin DNS for the TURN server: In the **Expressway-E TURN server (IP address or DNS name)** field, enter the FQDN of the Cisco Expressway-E cluster.
Successive clients making TURN requests to that cluster FQDN will be directed to different servers in the Cisco Expressway-E cluster; however, whether and how a particular client uses round-robin DNS for subsequent calls can be influenced by DNS caching.

Step 8 Click **Update**.

Round-robin DNS takes effect if the Cisco Jabber Guest call URL that is used by a client browser to make a Cisco Jabber Guest call uses the FQDN for the Cisco Expressway-E cluster.

What to Do Next

To ensure that the number of new call requests does not exceed the capacity of the Cisco Expressway-C, make sure that you change the throttle calls per second limit.

Change the Throttle Calls Per Second Limit

To ensure that the number of new call requests (SIP INVITES) does not exceed the capacity of the Cisco Expressway-C, the Cisco Jabber Guest server implements a call throttling mechanism.

For a clustered Cisco Expressway-C deployment in which load balancing is achieved by round-robin DNS, we recommend that you change the `throttleCallsPerSecLimit` setting to 10 multiplied by the number of servers in the Cisco Expressway-C cluster to which Cisco Jabber Guest sends SIP. For example, if there are two servers in the Cisco Expressway-C cluster, set `throttleCallsPerSecLimit` to 20.

Procedure

Step 1 Sign in to the server as root.

Step 2 For a clustered Cisco Jabber Guest server, credentials are required to access MongoDB from root. Sign in to the database:

```
cat/var/opt/cisco/webcommon/.security/.clusterkey |base64 --decode
mongo webcommon -u <user> -p <password>
```

Step 3 Change the `throttleCallsPerSecLimit` limit:

```
db.urlSettings.update( {}, { "$set": { "throttleCallsPerSecLimit": NumberInt(10) } } )
```

Step 4 Verify that the limit has changed:

```
> db.urlSettings.find().pretty()
```

Configure Round-Robin CSV Loading Balancing

With round-robin CSV load balancing, a Cisco Jabber Guest server can be configured to make requests, in round-robin order, across individually specified servers by using a CSV list. After a server is used, the next server on the list is used, until the choice rotates to the beginning of the list and then repeats.

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Call Control and Media**.

Step 3 To set up a CSV list for the SIP server:

a) For **SIP server**, enter a list of IP addresses or FQDNs for individual Cisco Expressway-C servers. The list of IP addresses or FQDNs must be separated by commas and must not contains spaces.

Example:
expressway-c-1.somedomain.com,*expressway-c-2.somedomain.com*,*expressway-c-3.somedomain.com*

b) Next to **Send SIP traffic to**, click **SIP server specified above**.

Step 4 To set up a CSV list to request short-term TURN credentials from Cisco Expressway-C:

a) For **Expressway-C (IP address or DNS name)**, enter a list of IP addresses or FQDNs for individual Cisco Expressway-C servers. The list of IP addresses or FQDNs must be separated by commas and must not contains spaces.

Example:
expressway-c-1.somedomain.com,*expressway-c-2.somedomain.com*,*expressway-c-3.somedomain.com*

b) Next to **Request short-term TURN credentials from**, click **Expressway-C server specified above**.

Step 5 To set up a CSV list for the TURN server: For **Expressway-E TURN server (IP address or DNS name)**, enter a list of FQDNs for individual Cisco Expressway-E servers. The list of FQDNs must be separated by commas and must not contains spaces.

Example:

expressway-e-1.somedomain.com,*expressway-e-2.somedomain.com*,*expressway-e-3.somedomain.com*

Step 6 Click **Update**.

Configure HTTP Load Balancing

Cisco Jabber Guest server can take advantage of HTTP load balancing from the Cisco Expressway-C by sending SIP and TURN credential requests to the Cisco Expressway-C that sent the HTTP.

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Call Control and Media**.

Step 3 To send SIP to the Cisco Expressway-C that sent the HTTP, next to **Send SIP traffic to**, click **Expressway-C server that proxied the HTTP request from Jabber Guest client**.

Step 4 To send TURN credential requests to the Cisco Expressway-C that sent the HTTP, next to **Request short-term TURN credentials from**, click **Expressway-C server that proxied the HTTP request from Jabber Guest client**.

Step 5 Click **Update**.

Configure Round-Robin TURN Port Range Load Balancing

You can configure Cisco Jabber Guest to take advantage of the load-balancing potential for TURN requests by using different TURN ports for each successive TURN request.

On a large Cisco Expressway-E deployment, up to six TURN request ports can be specified as a range. When used in combination with round-robin DNS or round-robin CSV for TURN servers, this multiplies the number of TURN request ports in use.

Procedure

Step 1 Sign in to Cisco Jabber Guest Administration as an administrator.

Step 2 Click **Settings**, and then click **Call Control and Media**.

Step 3 For **TURN port**, enter a hyphenated range of port numbers that matches the range of TURN request ports configured on Cisco Expressway-E (under **Configuration** > **Traversal** > **TURN**).

Example:
3478-3483

Step 4 Click **Update**.

Upgrade Cisco Jabber Guest Server

Cisco Jabber Guest Server is upgraded through vSphere on the Microsoft Windows platform. The upgrade is delivered as an ISO file, and requires a CD or DVD drive that can be connected to the image.

Procedure

Step 1 Download `JabberGuest-10.x.x.x.iso`.

Step 2 Open vSphere.

Step 3 Browse to the virtual machine to upgrade.

Step 4 Right-click the virtual machine and select **Open console**.

Step 5 Connect the CD/DVD drive to the ISO image:

a) From the console of the virtual machine, click on the CD/DVD button whose icon image is a disk with a wrench.

b) Click the **CD/DVD drive 1** menu item and then select the **Connect to ISO image on local disk...** menu item.

c) In the **Open** window, browse to the ISO image downloaded in Step 1 and double-click it.

Step 6 Click inside the virtual machine console and sign in as root.

Step 7 Under the `/mnt` directory, create a new directory named `cdrom` to use as the mount location for the CD/DVD drive.

```
mkdir /mnt/cdrom
```

Step 8 Mount the CD/DVD drive to `/mnt/cdrom`:

```
mount /dev/cdrom /mnt/cdrom
```

Step 9 Change directory to `/mnt/cdrom`:

```
cd /mnt/cdrom
```

Step 10 Execute the upgrade script:

```
bash upgrade
```