Cisco TelePresence Video Communication Server with Jabber Guest

Deployment Guide

First Published: December 2016

Cisco VCS X8.9
Cisco Jabber Guest Server 10.6.9 (or later)
## Contents

Preface ......................................................................................................................... 4
  Change History ........................................................................................................... 4
Jabber Guest Services Overview ................................................................................. 5
  Information Scope ...................................................................................................... 5
  Deployment Options .................................................................................................... 5
Jabber Guest Licensing and Call Capacity ................................................................. 6
Configure Jabber Guest Services on VCS ................................................................. 7
  Jabber Guest Configuration Summary ........................................................................ 7
Configuring a Secure Traversal Zone Connection for Unified Communications .......... 9
  Installing VCS Security Certificates ......................................................................... 9
  Configuring Encrypted VCS Traversal Zones ............................................................... 9
Overview of VCS Expressway Deployment ............................................................... 12
Configure the VCS Expressway for Jabber Guest ....................................................... 13
  Task 1: Enable Jabber Guest Services ....................................................................... 13
  Task 2: Enable TURN Services ................................................................................ 13
  Task 3: Reduce the Default MTU to 1400 Bytes ......................................................... 13
  Task 4: [Dual NIC Deployment Only] Create Corresponding Neighbor Zones for Each of the Jabber Guest Servers ........................................................................ 13
  Task 5: [Dual NIC Deployment Only] Create a Search Rule for the Traversal Zone Between the VCS Expressway and VCS Control Servers ...................................................... 14
Configure the VCS Control for Jabber Guest ............................................................ 15
  Task 1: Enable Jabber Guest Services ....................................................................... 15
  Task 2: Enable Jabber Guest on the Required Domain .............................................. 15
  Task 3: Configure Jabber Guest Servers and Associate Their Addresses with the Jabber Guest Domain ................................................................................................................. 15
  Task 4: Verify that the SSH Tunnel is Active ............................................................. 15
  Task 5: [Single NIC Deployment Only] Create Corresponding Neighbor Zones for Each of the Jabber Guest Servers .................................................................................. 16
  Task 6: Set up a Connection Between VCS Control and Cisco Unified Communications Manager ......................................................................................................................... 17
Task 7: [Single NIC Deployment Only] Create a Search Rule on VCS Control to Route Calls to Cisco Unified Communications Manager .................................................................17

Task 8: Force the Protocol Between the Cisco Jabber Guest Server and the VCS Control to be HTTP: .................................................................17

Configure Call Routing for Jabber Guest .................................................................18
  Single NIC Deployment ................................................................................18
  Dual NIC Deployment ..................................................................................18
  Onward Routing Options (Both Deployment Types) ..................................18

Single NIC Deployment Signaling and Media Paths .........................................19
  Call Flow Summary in Single NIC Deployment ........................................19
  Call Signaling Flow ..............................................................................19
  Media Flow ........................................................................................20

Jabber Guest Signaling and Media Flows in Dual NIC Deployment ................22
  Call Flow Summary in Dual NIC Deployment ........................................22
  Call Signaling Flow ..............................................................................22
  RTP Media Flow ..................................................................................23

Configure your Firewall for Jabber Guest Traffic ..........................................24
  Single NIC Deployment ..........................................................................24
  Dual NIC Deployment ...........................................................................27

Troubleshooting Jabber Guest Services on VCS ........................................29

Cisco Legal Information ...........................................................................30
Cisco Trademark ......................................................................................30
Preface

Change History

Table 1  Deployment Guide Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2016</td>
<td>First published with X8.9 release.</td>
<td></td>
</tr>
</tbody>
</table>
Jabber Guest Services Overview

Cisco Jabber Guest is a consumer to business (C2B) solution that extends the reach of Cisco’s enterprise telephony to people outside of a corporate firewall who do not have phones registered with Cisco Unified Communications Manager.

It allows an external user to click on a hyperlink (in an email or a web page) that will download and install (on first use) an H.264 plugin into the user’s browser. It then uses http-based call control to "dial" a URL to place a call to a predefined destination inside the enterprise. The user is not required to open an account, create a password, or otherwise authenticate.

To enable the call to be placed, it uses the Expressway solution (a secure traversal zone between the VCS Control and VCS Expressway) as a Unified Communications gateway to traverse the firewall between the Jabber Guest client in the internet and the Jabber Guest servers inside the enterprise to reach the destination user agent (endpoint).

Information Scope

The topics here focus on the VCS configuration required to deploy the Jabber Guest solution. You can read more detailed information about Jabber Guest in the following documents:


Deployment Options

You can deploy the VCS Expressway using either one network interface or two, which affects the call signaling and media paths of the Jabber Guest calls. This document covers both the "single NIC" and "dual NIC" deployment options.

VCS Expressway and VCS Control provide the following functionality:

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

**Note:** Configure a dual NIC deployment if you require static NAT on the VCS Expressway.
Jabber Guest Licensing and Call Capacity

The VCS licensing requirements for Jabber Guest sessions are as follows:

- Each session typically uses four TURN server relays on the VCS Expressway.
- One traversal call license is required per Cisco Jabber Guest session on the VCS Expressway.

Note:

- Prior to X8.8, a traversal call license was required on the VCS Control for each Jabber Guest session.
- Changes to the licensing model in X8.8 release have revealed an issue with licensing of the Jabber Guest service on the VCS Expressway server. When the VCS pair is part of a "single NIC" deployment, the VCS Expressway should count one traversal call license for each Jabber Guest call, but it does not. This issue could cause confusion about the server's load because the usage appears low, even when the server is processing multiple calls. We recommend the dual NIC Jabber Guest deployment. If you are using the single NIC deployment, make sure your VCS Expressway is correctly licensed to ensure continuity of service when upgrading in future.
- An Advanced Networking license (required for the dual NIC deployment) is included when you order VCS.

The maximum number of Jabber Guest sessions supported depends on the VCS platform size, and whether the systems are deployed as a single VCS Control and VCS Expressway pair, or as a pair of clusters.

<table>
<thead>
<tr>
<th>Table 2 Jabber Guest Session Limits</th>
<th>Small / Medium systems</th>
<th>Large systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>One VCS Control and one VCS Expressway</td>
<td>100</td>
<td>500</td>
</tr>
<tr>
<td>A cluster of VCS Controls and a cluster of VCS Expressways (4 or more peers per cluster for maximum capacity)</td>
<td>400</td>
<td>2000</td>
</tr>
</tbody>
</table>
Configure Jabber Guest Services on VCS

Important Notes:

- You cannot use Jabber Guest services in conjunction with Mobile and Remote Access.
- The domain part of the VCS Expressway’s FQDN must be the same as the domain you create for Jabber Guest services.
- Your external firewall must allow media coming out from the DMZ that is destined for the public-facing IP address of the VCS Expressway:
  - In the single NIC deployment, media is sent from the VCS Control to the public-facing (static NAT) address of the VCS Expressway. See Configure your Firewall for Jabber Guest Traffic, page 24.
  - In the dual NIC deployment, media is sent from the inward-facing NIC of the VCS Expressway to the public-facing (static NAT) address of the VCS Expressway. See Configure your Firewall for Jabber Guest Traffic, page 24.

Where examples are required, we’re using the example of a Jabber Guest client calling the URL https://expressway.example.com/call/8111@example.com.

Jabber Guest Configuration Summary

Table 3 Taskflow for Configuring VCS for Jabber Guest

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Configuring a Secure Traversal Zone Connection for Unified Communications, page 9 | To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be a Unified Communications traversal zone connection between the VCS Control and the VCS Expressway. This involves:
  - Installing suitable security certificates on the VCS Control and the VCS Expressway.
  - Configuring a Unified Communications traversal zone between the VCS Control and the VCS Expressway. See Configuring a Secure Traversal Zone Connection for Unified Communications, page 9 for instructions about how to do this if your system does not already have a secure traversal zone in place. |
| Configure the VCS Expressway for Jabber Guest, page 13 | To turn on Jabber Guest services and enable media routing between Jabber Guest client and VCS Control. For the dual NIC deployment only, you also enable Jabber Guest on the appropriate domain, create Jabber Guest servers to link to that domain, and create neighbor zones to route calls from those servers. |
| Configure the VCS Control for Jabber Guest, page 15 | To turn on Jabber Guest services. For the single NIC deployment only, you also enable Jabber Guest on the appropriate domain, create Jabber Guest servers to link to that domain, and create neighbor zones to route calls from those servers. |
| Configure Call Routing for Jabber Guest, page 18 | To route the SIP calls coming from Jabber Guest toward the on-premises endpoints or bridges, create search rules that target the appropriate neighbor zones. |
Configure your Firewall for Jabber Guest Traffic, page 24 | To translate destination addresses and ports for inbound calls, and to enable the various call legs to traverse the external and internal firewalls as necessary. Much of the firewall configuration for the single NIC and dual NIC options is the same, but there are some differences.
Configuring a Secure Traversal Zone Connection for Unified Communications

To support Unified Communications features (such as mobile and remote access or Jabber Guest), there must be a Unified Communications traversal zone connection between the VCS Control and the VCS Expressway. This involves:

- Installing suitable security certificates on the VCS Control and the VCS Expressway.
- Configuring a Unified Communications traversal zone between the VCS Control and the VCS Expressway.

**Note:** You should configure only one *Unified Communications traversal zone* per VCS.

Installing VCS Security Certificates

You must set up trust between the VCS Control and the VCS Expressway:

1. Install a suitable server certificate on both the VCS Control and the VCS Expressway.
   - The certificate must include the **Client Authentication** extension. The system will not allow you to upload a server certificate without this extension when Unified Communications features have been enabled.
   - The VCS includes a built-in mechanism to generate a certificate signing request (CSR) and is the recommended method for generating a CSR:
     - Ensure that the CA that signs the request does not strip out the client authentication extension.
     - The generated CSR includes the client authentication request and any relevant subject alternate names for the Unified Communications features that have been enabled.
   - To generate a CSR and/or to upload a server certificate to the VCS, go to **Maintenance > Security certificates > Server certificate**. You must restart the VCS for the new server certificate to take effect.

2. Install on both VCSs the trusted Certificate Authority (CA) certificates of the authority that signed the VCS’s server certificates.

There are additional trust requirements, depending on the Unified Communications features being deployed. For mobile and remote access deployments:

- The VCS Control must trust the Unified CM and IM&P tomcat certificate.
- If appropriate, both the VCS Control and the VCS Expressway must trust the authority that signed the endpoints’ certificates.

For Jabber Guest deployments:

- When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the VCS Control either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server’s certificate.

To upload trusted Certificate Authority (CA) certificates to the VCS, go to **Maintenance > Security certificates > Trusted CA certificate**. You must restart the VCS for the new trusted CA certificate to take effect.

See *Cisco VCS Certificate Creation and Use Deployment Guide* on the VCS configuration guides page.

Configuring Encrypted VCS Traversal Zones

To support Unified Communications features via a secure traversal zone connection between the VCS Control and the VCS Expressway:

- The VCS Control and VCS Expressway must be configured with a zone of type *Unified Communications traversal*. This automatically configures an appropriate traversal zone (a traversal client zone when selected on VCS Control or a traversal server zone when selected on VCS Expressway) that uses SIP TLS with **TLS**.
verify mode set to On, and Media encryption mode set to Force encrypted.

- Both VCSs must trust each other's server certificate. As each VCS acts both as a client and as a server you must ensure that each VCS's certificate is valid both as a client and as a server.
- If an H.323 or a non-encrypted connection is also required, a separate pair of traversal zones must be configured.

To set up a secure traversal zone, configure your VCS Control and VCS Expressway as follows:

1. Go to Configuration > Zones > Zones.
2. Click New.
3. Configure the fields as follows (leave all other fields with default values):

<table>
<thead>
<tr>
<th></th>
<th>VCS Control</th>
<th>VCS Expressway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>&quot;Traversal zone&quot; for example</td>
<td>&quot;Traversal zone&quot; for example</td>
</tr>
<tr>
<td>Type</td>
<td>Unified Communications traversal</td>
<td>Unified Communications traversal</td>
</tr>
</tbody>
</table>

**Connection credentials section**

<table>
<thead>
<tr>
<th></th>
<th>&quot;exampleauth&quot; for example</th>
<th>&quot;exampleauth&quot; for example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>&quot;exmpl3.c0m&quot; for example</td>
<td>Click <a href="#">Add/Edit local authentication database</a>, then in the popup dialog click <a href="#">New</a> and enter the Name (&quot;exampleauth&quot;) and Password (&quot;exmpl3.c0m&quot;) and click <a href="#">Create credential</a>.</td>
</tr>
<tr>
<td>Password</td>
<td>&quot;exmpl3.c0m&quot; for example</td>
<td></td>
</tr>
</tbody>
</table>

**SIP section**

<table>
<thead>
<tr>
<th></th>
<th>VCS Control</th>
<th>VCS Expressway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>7001</td>
<td>7001</td>
</tr>
<tr>
<td>TLS verify subject name</td>
<td>Not applicable</td>
<td>Enter the name to look for in the traversal client's certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes). If there is a cluster of traversal clients, specify the cluster name here and ensure that it is included in each client's certificate.</td>
</tr>
</tbody>
</table>

**Authentication section**

<table>
<thead>
<tr>
<th>Authentication policy</th>
<th>VCS Control</th>
<th>VCS Expressway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not check credentials</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Location section**

<table>
<thead>
<tr>
<th>Peer 1 address</th>
<th>VCS Control</th>
<th>VCS Expressway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the FQDN of the VCS Expressway. Note that if you use an IP address (not recommended), that address must be present in the VCS Expressway server certificate.</td>
<td>Not applicable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peer 2...6 address</th>
<th>VCS Control</th>
<th>VCS Expressway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the FQDNs of additional peers if it is a cluster of VCS Expressways.</td>
<td>Not applicable</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **Create zone**.
Overview of VCS Expressway Deployment

Single NIC Deployment Summary

- The VCS Expressway is in the DMZ with a single NIC enabled.
- VCS Expressway in static NAT mode is optional and requires extra configuration on the Jabber Guest server.
- The VCS Expressway is used for TURN services and reverse proxy, not call control.
- SIP traffic goes from the Jabber Guest server to the VCS Control.
- Media flows between the VCS Expressway and VCS Control using TURN relay and not a traversal zone.

**Note:** You can optionally configure the VCS Expressway LAN interface to use static NAT mode. If you do, you must configure the Jabber Guest server with the public IP address (static NAT address), and the private IP address of the VCS Expressway. These details are on System > Network interfaces > IP.

Dual NIC Deployment Summary

- The VCS Expressway is in the DMZ with both NICs enabled.
- VCS Expressway in static NAT mode is optional and requires extra configuration on the Cisco Jabber Guest server.
- The VCS Expressway is used for TURN services, reverse proxy, and call control.
- SIP traffic goes from the Jabber Guest server to the VCS Expressway.
- Media flows between the VCS Expressway and VCS Control using a traversal zone.

**Note:**

- If the outward-facing LAN interface of the VCS Expressway has static NAT mode on, you need to configure the Jabber Guest server with the VCS Expressway’s public IP address, and both of its private IP addresses. These details are on System > Network interfaces > IP.
- If VCS Expressway is used for reverse proxy functionality, the Cisco Jabber Guest URL looks like http://expressway-e.example.com/call where expressway-e.example.com is the FQDN of the VCS Expressway.
Configure the VCS Expressway for Jabber Guest

Note: Before you begin ensure that you have set up VCS security certificates and a Unified CM traversal zone. See Configuring a Secure Traversal Zone Connection for Unified Communications, page 9

Task 1: Enable Jabber Guest Services

1. On the VCS Expressway, go to Configuration > Unified Communications > Configuration.
2. Set Unified Communications mode to Jabber Guest services.
3. Click Save.

Jabber Guest services are enabled. You need to enable Jabber Guest on a domain, then you can configure Jabber Guest servers. You do this on the VCS Expressway for the dual NIC deployment, or on the VCS Control for the single NIC deployment.

Task 2: Enable TURN Services

You must enable the VCS Expressway’s TURN server to allow media routing from the Jabber Guest clients to the VCS Control to be established through ICE:

1. Go to Configuration > Traversal > TURN.
2. Set TURN services to On.
3. Set the Authentication realm to its default of TANDBERG.
4. Click Save.

You do not have to set up any TURN client credentials in the local authentication database.

Note: To configure TURN credential provisioning and set up TURN server information on Jabber Guest, see the Cisco Jabber Guest Server Installation and Configuration Guide, for your version, at the Jabber Guest Installation and Upgrade Guides page.

Task 3: Reduce the Default MTU to 1400 Bytes

In some call scenarios, such as when using VPN / SSL tunnels, the available Maximum Transmission Unit (MTU) can be reduced. The default MTU on VCS Expressway of 1500 bytes can be too high and can cause packet loss. We recommended that you lower the MTU size on the relevant network interfaces to 1400 bytes.

1. Go to System > Network interfaces > IP.
2. In the Maximum transmission unit (MTU) field, enter 1400.
   
   If you have multiple transmission unit (MTU) field, enter 1400.
   
   If you have multiple interfaces, you will typically want to do this on the externally facing interface.
3. Click Save.

Task 4: [Dual NIC Deployment Only] Create Corresponding Neighbor Zones for Each of the Jabber Guest Servers

Note: These neighbor zones are used to receive traffic from the Jabber Guest servers. Do not configure any search rules to route traffic to these zones.

1. On the VCS Expressway, go to Configuration > Zones > Zones.
2. Click New.
3. Configure the fields as follows (leave all other fields with default values):

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name you want to give this zone, for example “Jabber Guest server [name]”.</td>
</tr>
<tr>
<td>Type</td>
<td>Neighbor</td>
</tr>
<tr>
<td>H.323 mode</td>
<td>Off</td>
</tr>
<tr>
<td>SIP mode</td>
<td>On</td>
</tr>
<tr>
<td>Transport</td>
<td>TLS</td>
</tr>
<tr>
<td>TLS verify mode</td>
<td>On</td>
</tr>
<tr>
<td>Media encryption mode</td>
<td>Force encrypted</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the same FQDN of the Jabber Guest server as configured on the Jabber Guest servers page.</td>
</tr>
<tr>
<td>Zone profile</td>
<td>Default</td>
</tr>
</tbody>
</table>

As these zones use a TLS verified connection you must ensure certificate trust between the VCS and the Jabber Guest servers.

- When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the VCS Control either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server’s certificate. To upload trusted Certificate Authority (CA) certificates to the VCS, go to Maintenance > Security certificates > Trusted CA certificate. You must restart the VCS for the new trusted CA certificate to take effect.
- You must install on the Jabber Guest server the trusted CA certificates of the authority that signed the VCS Control’s server certificate. To manage certificates on the Jabber Guest server, go to Settings > Local SSL Certificate.

4. Click Create zone.

5. Repeat this process for every Jabber Guest server.

Task 5: [Dual NIC Deployment Only] Create a Search Rule for the Traversal Zone Between the VCS Expressway and VCS Control Servers

For proper call routing, the SIP domain that you specify on the Jabber Guest server (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 VCS Expressway search rule to point to the traversal zone. See Configure Call Routing for Jabber Guest, page 18 for more information.
Configure the VCS Control for Jabber Guest

Task 1: Enable Jabber Guest Services

1. On the VCS Control, go to Configuration > Unified Communications > Configuration.
2. Set Unified Communications mode to Jabber Guest services.
3. Click Save.
   Jabber Guest services are enabled. You need to enable Jabber Guest on a domain, then you can configure Jabber Guest servers.

Task 2: Enable Jabber Guest on the Required Domain

**Important!** The domain that you create on the VCS Control, for associating Jabber Guest servers, is not related to any SIP domain(s) or internal DNS domains. The only requirement is that the domain must match the domain of the VCS Expressway's public-facing FQDN.

1. Go to Configuration > Domains.
2. Select the domain that supports Jabber Guest services.
   (If the domain does not yet exist, click New and enter the Domain name, in this case, example.com).
3. Set Jabber Guest to On.
4. Click Save.
   (The button reads Create domain if you are setting up the domain for the first time).

**Note:**
- Only one Jabber Guest domain is supported per VCS (cluster) deployment.
- Make sure that the domain has an associated DNS record that resolves to the VCS Expressway. The domain information is propagated from the VCS Control to the VCS Expressway through the SSH tunnel (port 2222). The information is used by the VCS Expressway to validate incoming HTTP requests for the Jabber Guest service.

Task 3: Configure Jabber Guest Servers and Associate Their Addresses with the Jabber Guest Domain

1. Go to Configuration > Unified Communications > Jabber Guest servers.
   This takes you to the Jabber Guest servers page.
2. Click New.
3. Enter the details of the Jabber Guest server:
   a. **Domain**: select the Jabber Guest domain that is to be mapped to a server hostname.
   b. **Server hostname**: enter the FQDN of a Jabber Guest server to use for the selected domain.
      This must be an FQDN, not an unqualified hostname or an IP address. The domain part of the FQDN does not need to match what you enter in Domain field.
   c. **Priority**: this controls the order in which connections to this hostname are attempted for this domain.
      All priority 1 hostnames are attempted first, followed by priority 2 hostnames, and so on.
      Give each Jabber Guest server a different priority so that calls are only sent to one Cisco Jabber Guest server in the deployment at a time.
4. Click Create entry.
5. If necessary, add further Jabber Guest server addresses for the domain. You can give each server the same priority for even load balancing.

Task 4: Verify that the SSH Tunnel is Active

1. On either the VCS Control or the VCS Expressway, go to Status > Unified Communications.
2. Click View ssh tunnel status.
3. Make sure that the Cisco Jabber Guest domain is listed and that the SSH tunnel is active.

Task 5: [Single NIC Deployment Only] Create Corresponding Neighbor Zones for Each of the Jabber Guest Servers

Note: These neighbor zones are used to receive traffic from the Jabber Guest servers. Do not configure any search rules to route traffic to these zones.

1. On the VCS Control, go to Configuration > Zones > Zones.
2. Click New.
3. Configure the fields as follows (leave all other fields with default values):

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name you want to give this zone, for example “Jabber Guest server [name].”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Neighbor</td>
</tr>
<tr>
<td>H.323 mode</td>
<td>Off</td>
</tr>
<tr>
<td>SIP mode</td>
<td>On</td>
</tr>
<tr>
<td>Transport</td>
<td>TLS</td>
</tr>
<tr>
<td>TLS verify mode</td>
<td>On</td>
</tr>
<tr>
<td>Media encryption mode</td>
<td>Force encrypted</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the same FQDN of the Jabber Guest server as configured on the Jabber Guest servers page.</td>
</tr>
<tr>
<td>Zone profile</td>
<td>Default</td>
</tr>
</tbody>
</table>

As these zones use a TLS verified connection you must ensure certificate trust between the VCS and the Jabber Guest servers.

- When the Jabber Guest server is installed, it uses a self-signed certificate by default. However, you can install a certificate that is signed by a trusted certificate authority. You must install on the VCS Control either the self-signed certificate of the Jabber Guest server, or the trusted CA certificates of the authority that signed the Jabber Guest server’s certificate. To upload trusted Certificate Authority (CA) certificates to the VCS, go to Maintenance > Security certificates > Trusted CA certificate. You must restart the VCS for the new trusted CA certificate to take effect.

- You must install on the Jabber Guest server the trusted CA certificates of the authority that signed the VCS Control’s server certificate. To manage certificates on the Jabber Guest server, go to Settings > Local SSL Certificate.
4. Click **Create zone**.
5. Repeat this process for every Jabber Guest server. Do not configure any search rules for these neighbor zones. These zones are used to receive traffic only.

**Task 6: Set up a Connection Between VCS Control and Cisco Unified Communications Manager**

1. On Cisco Unified Communications Manager, set up a nonsecure or secure SIP trunk to the VCS Control.
2. On VCS Control, set up a neighbor zone to Cisco Unified Communications Manager.
   
   See *Cisco Unified Communications Manager with VCS (SIP Trunk) Deployment Guide* on the **VCS configuration guides** page.

**Task 7: [Single NIC Deployment Only] Create a Search Rule on VCS Control to Route Calls to Cisco Unified Communications Manager**

You must create a search rule on VCS Control to route calls to Cisco Unified Communications Manager. See *Configure Call Routing for Jabber Guest, page 18* for more information.

**Task 8: Force the Protocol Between the Cisco Jabber Guest Server and the VCS Control to be HTTP:**

1. Sign in to the VCS Control command line interface as an administrator. In a clustered VCS Control deployment, sign in to the primary peer VCS Control.
2. Enter the following command: `xconf CollaborationEdge JabbercProxyProtocol: http`

**Note:** HTTP requests go from the VCS Expressway to the VCS Control to the Jabber Guest server.
Configure Call Routing for Jabber Guest

You configure call routing on the VCS Control or on the VCS Expressway, depending on whether you're deploying the VCS Expressway with a single NIC or with both NICs. In each case, the objective is to listen for SIP calls from Jabber Guest servers and route them toward the on-premises destinations.

You already created neighbor zones to the Jabber Guest servers. Now you need to create search rules for calls originating from these zones.

Single NIC Deployment

For each Jabber Guest server neighbor zone on the VCS Control, create a search rule that:

- Matches the pattern of the destinations set by Jabber Guest on calls to that zone.
  - The destinations are either DN numbers or SIP URIs in the Jabber Guest database, where they are associated with call URIs. Jabber Guest server forms them as SIP URIs by appending the domain as required. Hopefully the incoming SIP URIs match endpoints or bridges that are routable by call control agents neighbored to this VCS Control.
- Targets the neighbor zone of the call control agent that knows how to route to the matched destination (see Onward Routing Options (Both Deployment Types), page 18).

Dual NIC Deployment

For each Jabber Guest server neighbor zone on the VCS Expressway, create a search rule that:

- Matches the pattern of the destinations set by Jabber Guest on calls to that zone.
  - The destinations are either DN numbers or SIP URIs in the Jabber Guest database, where they are associated with call URIs. Jabber Guest server forms them as SIP URIs by appending the domain as required.
- Targets the secure traversal zone to the VCS Control.

Onward Routing Options (Both Deployment Types)

When the Jabber Guest SIP call arrives at the VCS Control, either in the VCS Expressway traversal client zone (dual NIC), or the Jabber Guest neighbor zone (single NIC), the search rule must target the neighbor zone that can route to the supplied destination.

For example, if the destination address is 8111@example.com, the alias pattern would be something like \(8(\text{d}3)@example\.com\), and the target zone options could include:

- **Endpoints / bridges registered to Unified CM**: the search rule targets the SIP trunk / neighbor zone between Unified CM and VCS Control. See Cisco Unified Communications Manager with VCS (SIP Trunk) Deployment Guide on the VCS configuration guides page.
- **Endpoints registered to the local VCS Control**: in this case you need suitable search rules to route calls for the Jabber Guest domain to the relevant endpoints.

**Note**: For endpoints that are registered with VCS, the call path must include Cisco Unified Communications Manager.
Single NIC Deployment Signaling and Media Paths

This topic summarizes the Jabber Guest traffic flow through the VCS Expressway and VCS Control deployment when the VCS Expressway has one network interface card (NIC) active.

For more information on configuring signaling and media, see the *Cisco Jabber Guest Server Installation and Configuration Guide*, for your version, at the Jabber Guest Installation and Upgrade Guides page.

**Call Flow Summary in Single NIC Deployment**

1. The Jabber Guest client sends an HTTP(S) request which is routed using HTTPS tunnels through the Expressway solution and on to the Jabber Guest server inside the enterprise.
2. The Jabber Guest server converts the HTTP(S) request into SIP and sends it to the VCS Control.
3. The VCS Control routes the call to the appropriate destination endpoint or bridge, typically through a SIP trunk to Unified CM.
4. VCS Control back-to-back user agent (B2BUA) connects the call (media) to the originating Jabber Guest client through the VCS Expressway’s TURN server.

   Media path: Collaboration endpoint or bridge \(\rightarrow\) VCS Control (B2BUA) \(\rightarrow\) VCS Expressway (TURN server) \(\rightarrow\) Jabber Guest client

**Call Signaling Flow**

When the Jabber Guest client initiates the call, the following diagram shows how the signaling is typically routed through the VCS Control, Jabber Guest server, to Unified CM. Cisco Unified Communications Manager routes the call onward to the endpoint or bridge.

The return signaling, from the user agent to the Jabber Guest client, follows the same path in reverse.

*Figure 2  Call Signaling Path*
Media Flow

Media channels negotiation results in the allocation of TURN relays between the Jabber Guest client and the VCS Expressway.

Note: Jabber Guest media does not go through the traversal link between VCS Expressway and VCS Control. Media is sent from the VCS Control to the outward-facing/NAT interface of the VCS Expressway. You may need to configure your external firewall to allow the media back in.

Figure 3  Media Path Negotiation

Figure 4  Media Path and Typical Ports

The following diagram shows the media flows and typical port usage on the VCS Expressway and VCS Control. The TURN server on the VCS Expressway relays the media between the Jabber Guest client and the B2BUA on the VCS Control, and the media also flows between the B2BUA and the internal endpoint.

See Configure your Firewall for Jabber Guest Traffic, page 24 for full information about port requirements.
Note: If the VCS Expressway is behind a NAT, extra 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 VCS Expressway on the Cisco Jabber Guest server. This allows media to be sent to the DMZ external address of the VCS Expressway, avoiding NAT reflection on the outside firewall.
Jabber Guest Signaling and Media Flows in Dual NIC Deployment

This topic summarizes the Jabber Guest traffic flow through the VCS Expressway and VCS Control deployment when the VCS Expressway has both NICs active.

For more information on configuring signaling and media, see the Cisco Jabber Guest Server Installation and Configuration Guide, for your version, at the Jabber Guest Installation and Upgrade Guides page.

Call Flow Summary in Dual NIC Deployment

The typical call flow for Jabber Guest can be summarized as follows:

1. The Jabber Guest client sends an HTTP(S) request which is routed using HTTPS tunnels through the Expressway solution and on to the Jabber Guest server inside the enterprise.
2. The Jabber Guest server converts the HTTP(S) request into SIP and sends it to the inward-facing NIC of the VCS Expressway.
3. The SIP traffic traverses the internal firewall from the VCS Expressway to the VCS Control.
4. The VCS Control routes the call to the appropriate destination (typically to Unified CM which routes it on to an endpoint or conferencing bridge).
5. The media path is established from the bridge or endpoint as follows:
   Internal party <-> VCS Control <-> VCS Expressway (inward-facing NIC) <-> TURN server (VCS Expressway outward-facing NIC) <-> Jabber Guest client.

Call Signaling Flow

**Figure 5  Signaling Flow of Jabber Guest Call on Dual NIC VCS Expressway Deployment**

1. Jabber Guest client initiates call by HTTP(S) ROAP to external IP address of VCS Expressway.
   The external firewall translates addresses and ports as necessary to reach correct listening socket on VCS Expressway’s outward-facing NIC.
2. VCS Expressway tunnels HTTPS through internal firewall to VCS Control.
3. VCS Control routes HTTPS to Jabber Guest server through a neighbor zone.
4. Jabber Guest server wraps the HTTPS ROAP as SIP and connects out (through internal firewall) to the inward-facing NIC of VCS Expressway.
5. SIP traverses the internal firewall through the Unified Communications traversal zone between VCS Expressway and VCS Control.
6. VCS Control routes the call on the SIP trunk to Unified CM.
7. Unified CM routes the call to the destination endpoint or bridge.

RTP Media Flow

Figure 6  Media Path

1. The internal endpoint call connects to the VCS Control.
2. The B2BUA sends media to the TURN server (on the public address of the outward-facing NIC of the VCS Expressway).
   To get there, the media traffic goes through the Unified Communications traversal zone to the inward-facing NIC on VCS Expressway, where it hairpins and goes out to the public IP address of the outward-facing NIC.
3. VCS Expressway’s TURN server negotiates TURN with the Jabber Guest client, and allocates TURN relays between the Jabber Guest client and the VCS Control.
   The TURN server on the VCS Expressway relays the media from the Jabber Guest client, across the traversal zone, to the B2BUA on the VCS Control.
4. The media then flows between the B2BUA and the internal endpoint / bridge.

Note:

- Because the media hairpins between the two VCS Expressway NICs, the TURN traffic and SIP traffic must reside on the same VCS Expressway server. You must configure the static NAT address, DMZ external address, and DMZ internal address of the VCS Expressway on the Cisco Jabber Guest server.
- If the VCS Expressway is behind a NAT, extra 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 VCS Expressway on the Jabber Guest server. This allows media to be sent to the DMZ external address of the VCS Expressway, avoiding NAT reflection on the outside firewall.

See also:

- Jabber Guest Licensing and Call Capacity, page 6 for licensing requirements.
- Configure your Firewall for Jabber Guest Traffic, page 24 for full information about port requirements.
Configure your Firewall for Jabber Guest Traffic

This section summarizes the ports that need to be opened for Jabber Guest traffic on the firewalls between your internal network (where the VCS Control is located) and the DMZ (where the VCS Expressway is located) and between the DMZ and the public internet.

Note:

- HTTP and HTTPS traffic from Jabber Guest clients in the internet is sent to ports 80 and 443 TCP respectively. Therefore the firewall between the VCS Expressway and the public internet must translate destination port 80 to 9980 and destination port 443 to 9443 for all TCP traffic that targets the VCS Expressway address.
- The VCS Expressway redirects HTTP requests on port 9980 to HTTPS on 9443.
- 80/443 TCP are the standard HTTP/S administration interfaces on the VCS. If the VCS Expressway 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 Jabber Guest client can reach the VCS Expressway. The FQDN of the VCS Expressway in DNS must include the Jabber Guest domain, so in this case it could be expressway.example.com. Use round-robin DNS if it is a cluster of VCS Expressways.

Note that this is public DNS configuration and it does not impose any configuration requirements on the VCS Expressway itself (host name / domain name on the DNS page, or the cluster name etc.)

Single NIC Deployment

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Src. IP</th>
<th>Src. ports</th>
<th>Protocol</th>
<th>Dest. IP</th>
<th>Dst. Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jabber Guest Client Media (TURN)</td>
<td>Any</td>
<td>1024-65535</td>
<td>UDP</td>
<td>VCS Expressway Public IP</td>
<td>3478 or 3478-3483*</td>
</tr>
<tr>
<td>Jabber Guest Client Signaling (HTTP)</td>
<td>Any</td>
<td>1024-65535</td>
<td>TCP</td>
<td>VCS Expressway Public IP</td>
<td>80</td>
</tr>
<tr>
<td>Jabber Guest Client Secure Signaling (HTTPS)</td>
<td>Any</td>
<td>1024-65535</td>
<td>TLS</td>
<td>VCS Expressway Public IP</td>
<td>443</td>
</tr>
<tr>
<td>Avoid port conflicts on VCS Expressway</td>
<td>External firewall's inward facing IP</td>
<td>80</td>
<td>TLS</td>
<td>VCS ExpresswayPrivate IP</td>
<td>9980+</td>
</tr>
<tr>
<td>Avoid port conflicts on VCS Expressway</td>
<td>External firewall's inward facing IP</td>
<td>443</td>
<td>TLS</td>
<td>VCS ExpresswayPrivate IP</td>
<td>9443+</td>
</tr>
<tr>
<td>Redirect inward traffic on VCS Expressway</td>
<td>VCS Expressway Private IP</td>
<td>9980</td>
<td>TCP</td>
<td>VCS Expressway Private IP</td>
<td>9443</td>
</tr>
<tr>
<td>SSH Tunnels from VCS Control VCS Expressway</td>
<td>VCS Control</td>
<td>35000-35999</td>
<td>TLS</td>
<td>VCS Expressway Public IP</td>
<td>2222</td>
</tr>
<tr>
<td>SIP Signaling</td>
<td>VCS Control</td>
<td>25000-25999</td>
<td>TLS</td>
<td>VCS Expressway Public IP</td>
<td>7001</td>
</tr>
<tr>
<td>TURN media relays</td>
<td>VCS Control</td>
<td>36000-59999</td>
<td>UDP</td>
<td>VCS Expressway Public IP</td>
<td>24000-29999</td>
</tr>
</tbody>
</table>

* On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.
Configure your Firewall for Jabber Guest Traffic

- Port translation in external firewall

**Note:**

- Inbound firewall rules are required to allow media to flow from the VCS Expressway to VCS Control.

- You may find that two-way media can still be established even if the inbound from VCS Expressway (DMZ) to VCS Control (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 it, only from outside to inside).
Configure your Firewall for Jabber Guest Traffic

**Jabber Guest client**

**Jabber Guest Server**

**Unified Communications Manager**

**Collaboration Endpoint or Bridge**

**Expressway-C**

**Expressway-E**

**NAT & PAT**

**Private IP**

**External firewall**

**Internal firewall**

KEY:
- **TLS**
- **UDP**
- **TCP**

Configure your Firewall for Jabber Guest Traffic.
## Dual NIC Deployment

Table 5  Port Reference for Jabber Guest Dual NIC Deployment

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Src. IP</th>
<th>Src. ports</th>
<th>Protocol</th>
<th>Dest. IP</th>
<th>Dst. Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROAP signaling</td>
<td>Any (web browser)</td>
<td>1024-65535</td>
<td>TCP</td>
<td>VCS Expressway Public IP</td>
<td>80</td>
</tr>
<tr>
<td>ROAP signaling</td>
<td>Any (web browser)</td>
<td>1024-65535</td>
<td>TLS</td>
<td>VCS Expressway Public IP</td>
<td>443</td>
</tr>
<tr>
<td>ROAP signaling</td>
<td>External firewall private IP</td>
<td>80</td>
<td>TCP</td>
<td>VCS Expressway Private IP (NIC 2)</td>
<td>9980</td>
</tr>
<tr>
<td>ROAP signaling</td>
<td>External firewall private IP</td>
<td>443</td>
<td>TLS</td>
<td>VCS Expressway Private IP (NIC 2)</td>
<td>9443</td>
</tr>
<tr>
<td>TURN requests</td>
<td>Any (web browser)</td>
<td>1024-65535</td>
<td>UDP</td>
<td>VCS Expressway Public IP</td>
<td>3478 (S/M systems)</td>
</tr>
<tr>
<td>TURN requests</td>
<td>External firewall private IP</td>
<td>1024-65535</td>
<td>UDP</td>
<td>VCS Expressway Private IP (NIC 2)</td>
<td>3478-3483 (L systems)</td>
</tr>
<tr>
<td>TURN media*</td>
<td>External Firewall public IP</td>
<td>24000-29999</td>
<td>UDP</td>
<td>VCS Expressway Public IP (external firewall address)</td>
<td>24000-29999</td>
</tr>
<tr>
<td>TURN media</td>
<td>External Firewall public IP</td>
<td>24000-29999</td>
<td>UDP</td>
<td>VCS Expressway Public IP (external firewall address)</td>
<td>24000-29999</td>
</tr>
</tbody>
</table>

* NAT reflection
† Port translation required
Configure your Firewall for Jabber Guest Traffic
Troubleshooting Jabber Guest Services on VCS

Packet loss on calls

Check if the Maximum Transmission Unit (MTU) on VCS Expressway is too high. We recommended that you lower the MTU size on the relevant network interfaces from 1500 to 1400 bytes.

Jabber Guest client fails to connect and gets "Not Found on Accelerator" message

This error can occur if:

- The VCS Expressway domain is different from the Jabber Guest domain.
- The SIP trunk between the Jabber Guest server and the VCS Control is not active.

Jabber Guest client fails to connect and gets "Link Not Found" message

This error can occur if:

- The URL being called is wrong.
- The correct URL is being called but it has not been enabled in the Jabber Guest server or it has expired.
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 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)