

## Table of Contents

### **1) Best Way To Use This Guide - page 2**

### **2) System Requirements - page 3**

- Security Options and CA-Signed Certificates - page 3
- Firewall and Network Access - page 4
- Network Bandwidth - page 5
- Video Devices - page 5
- Endpoint Configuration for CUCM - page 6
- Endpoint Configuration for VCS-C - page 9

### **3) Topology - page 10**

- Video devices registered to Cisco Video Conference Server (VCS-C) as controller with Cisco Video Conference Server (VCS-E) as 'Edge' node for firewall transversal - page 10
- Video devices registered to Cisco Unified Call Manager (CUCM) as controller with Cisco Video Conference Server (VCS-E) as 'Edge' node for firewall transversal - page 11
- Video devices registered to Cisco Unified Call Manager (CUCM) to Cisco Video Conference Server (VCS-C) to Cisco Video Conference Server (VCS-E) as 'Edge' node for firewall transversal - page 12

### **4) Deployment and Configuration - page 13**

- Step 1 - Configure Port Range - page 13
- Step 2 - Configure DNS Zone - page 13
- Step 3 - Configure a Transversal Server/Client (optional) - page 19
- Step 4 - Reduce SIP Timeout on VCS-Expressway (optional) - page 20
- Step 5 - Configure SIP Profile and Trunk - page 21
- Step 6 - Enable BFCP - page 23
- Step 7 - Add Route Pattern - page 24
- Cisco VCS-C as the Controller - page 29
- Configuring Cisco VCS-E - page 34
- Step 8 - Bandwidth Controls - page 37
- Step 9 - Simplify the Video Dial String / Dial Transforms - page 38
- Step 10 - Verify the Service and Test with BlueJeans - page 39

### **5) Configure SIP For Early Offer - page 41**

### **6) Troubleshooting - page 42**

- Calls Dropping in Exactly 15 Minutes - page 42
- 30 Second Delay for the BlueJeans Welcome Screen - page 43
- No Content Receive - Unknown Protocol - page 44
- Cannot Dial IP Addresses When Registered to CUCM - page 45

### **7) Contacting BlueJeans Support - page 45**

## Best Way To Use This Guide

This guide was created to show best practices for integrating video devices registered to Cisco Unified Call Manager (CUCM) and/or utilizing Cisco Video Conference Server (VCS) to connect successfully to BlueJeans meetings.

Participants can join BlueJeans via web browser (WebRTC), BlueJeans Desktop application, BlueJeans Mobile application, from a telephone, or from a video device. Video devices negotiate all media (main video, content, and audio) to and from BlueJeans. This media flows over IP address negotiated by using SIP or H.323. Cisco VCS may be used for call control and firewall traversal, but is not required.

Video endpoints (video devices) supporting SIP can register to Cisco CUCM, in order to make or receive voice/video calls. Alternatively, endpoints can register to Cisco VCS-C configured acting as SIP registrar. The purpose of Cisco VCS Expressway is to provide network 'edge' functionality, by converting voice/video traffic from private corporate network to the public Internet. The purpose of the CUCM and VCS-C working in registrar mode is somewhat similar (for these example configurations) providing 'control' of TelePresence endpoints.

This guide shows recommended configuration for Cisco Unified Call Manager (CUCM), Cisco Video Conference Server (VCS-C) Controller and Cisco Video Conference Server (VCS-E) Expressway.

The best way to use this guide is to match the Cisco infrastructure you are using and follow the suggested configuration in the deployment section:

- 1) Video devices registered to Cisco Video Conference Server (VCS-C) as controller with Cisco Video Conference Server (VCS-E) as 'Edge' node for firewall transversal.
- 2) Video devices registered to Cisco Unified Call Manager (CUCM) as controller with Cisco Video Conference Server (VCS-E) as 'Edge' node for firewall transversal.
- 3) Video devices registered to Cisco Unified Call Manager (CUCM) to Cisco Video Conference Server (VCS-C) to Cisco Video Conference Server (VCS-E) as 'Edge' node for firewall transversal.

Other deployments are also possible including:

- Utilizing Cisco Unified Border Element (CUBE) - See CUBE guide in BlueJeans Knowledge Base.
- Some customers may have multiple CUCM and/or Cisco VCS devices or use a combination of these basic topologies.
- Some customers may have their endpoints registered to CUCM and do not have a SBC (Session Border Controller) like a VCS or CUBE. They just have a SIP trunk to the Internet.

This guide is not designed to be the definitive document on Cisco Infrastructure. Just recommendations to help make successful calls to BlueJeans. This guide is assuming that your

Cisco Infrastructure is up and running and that you have a working knowledge of how CUCM/VCS works. Further questions or issues may require contacting Cisco Support. For more details please consult Cisco Administration Guides for the specific devices that are deployed.

## System Requirements

1) Customer has a working Cisco deployment inside their Enterprise with the below software versions for the mandatory components:

- Properly configured and working video device or room system
- Cisco Unified Communications Manager (CUCM) version 8.6.1 or later
- Cisco TelePresence Video Communications Server (VCS-Expressway) version 6.x or later with encryption and traversal licenses

2) Customer firewall has been setup to allow the entire IP/ port range from their VCS-Expressway to BlueJeans. Make sure to open firewall ports against BJN's entire IP/Port range:

- 199.48.152.0/22
- 31.171.208.0/21
- 103.20.59.0/24
- 103.255.54.0/24
- 8.10.12.0/24
- 165.254.117.0/24
- 13.210.3.128/26

Note: BlueJeans has several POPs distributed globally. The call will be automatically redirected to the closest POP to the end point or media egress point. Audio/video traffic will likely be routed to any of above IP range based on geolocation. Hence it's important that firewall ports are opened against entire IP/Port range.

H.323 based systems:

Outbound TCP Port 1720 - H.225 Signaling for H.323

Outbound TCP Ports 5000-5999 - H.245 Call Control for H.323

Outbound UDP Ports 5000-5999 - RTP Media

SIP based systems:

Outbound TCP Port 5060 - SIP Signaling

Outbound TCP Port 5061 - SIPS (TLS) Signaling

Outbound UDP Ports 5000-5999 - RTP Media

## Security Options - Encryption (TLS and sRTP)

By default, the Cisco VCS Expressway uses self-signed certificates. For each SIP call, it attempts TLS signaling with fallback to TCP, and sRTP with fallback to RTP. For H.323 calls BlueJeans

supports non-secure H.225/H.245 signaling and H.235 media encryption methods. If you want your calls to be encrypted (recommended) when connecting to BlueJeans you must configure at least the VCS Expressway-E to use TLS/sRTP.

Best practice is that any communications that egress your enterprise should use TLS and sRTP. The VCS Expressway can provide that security interworking, allowing your communications internally within UC Manager to remain TCP/RTP but as soon as it hits VCS Expressway and is destined to go out over the Traversal Zone it should get encrypted. Therefore, the ideal best practice is to use TLS/sRTP end-to-end, but if you want to use TCP/RTP internally then at the very least you should mandate TLS/sRTP on the Traversal Zone on VCS-C so that the traffic is encrypted before sending through your firewall to the VCS-E that is sitting outside your firewall in the DMZ. We recommend enabling TLS Verify on the DNS Zone for BlueJeans so your VCS-E will verify the Bluejeans certificate when using TLS to communicate with the BlueJeans. See configuration details in the VCS Expressway section in this guide.

### **CA-Signed Certificates (Optional)**

You do not need a CA-signed certificates to encrypt calls to BlueJeans. However, only CA-signed certificates can provide authentication. These CA-signed certificates must be issued by a Root Certificate Authority (or one of their Intermediate Certificate Authorities).

For SIP calls, any combination of certificate type, TCP/RTP or TLS/sRTP are supported calling BlueJeans.

### **Deploy with CA-Signed Certificates**

If you want to use CA-signed certificates to enable secure calling to BlueJeans. These tasks require the Cisco Expressway Series (Cisco Expressway-C and Cisco Expressway-E) or Cisco VCS (Cisco VCS Control and Cisco VCS Expressway).

Replacing the default VCS server certificate:

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

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

**Note: We recommend that Early Offer is always used on CUCM and/or VCS SIP trunks to BlueJeans SIP servers. Early Offer (versus Delayed Offer sometimes selected by default on CUCM and/or VCS) helps to avoid various compatibility issues such as failure to join a meeting, calls being dropped after 15 minutes, asymmetric codecs being negotiated, etc.**

### **3) Firewall and Network access**

Make sure that the port range for Cisco Expressway-E, Cisco VCS Expressway, or other edge traversal devices and firewalls allows the following:



- inbound media traffic from BlueJeans for the RTP port range 5000 - 5999 TCP/UDP
- inbound SIP signaling traffic from BlueJeans over TCP for ports 5060 and 5061 TCP
- inbound H.323 signaling traffic from BlueJeans over TCP port 1720 and port range 5000 - 5999 (if H.323 is being used)
- outbound media traffic to BlueJeans over UDP for the RTP port range 5000 - 5999
- outbound SIP signaling traffic to BlueJeans over TCP for the ports 5060 – 5061
- outbound H.323 signaling traffic to BlueJeans over TCP port 1720 and port range 5000 - 5999 (if H.323 is being used)

#### 4) Network bandwidth

The amount of network bandwidth required depends on the requirements of each video device to provide the desired video quality plus presentation data. We recommend at least 1.5 Mbps per call for an optimal experience. Some video devices can take advantage of higher rates, and the service can accommodate lower rates, depending on the device.

#### 5) Video Devices

SIP: In order for the participant to present or view shared content, the device must be able to negotiate Binary Floor Control Protocol (BFCP) with BlueJeans. Without BFCP, content cannot be shared and will be seen embedded in the main video channel.

H.323: In order for the participant to present or view shared content, the device must be able to negotiate H.239 with BlueJeans. Without H.239, content cannot be shared and will be seen embedded in the video.

BlueJeans supports H.323 or SIP protocol, but most enterprises using Cisco Infrastructure with CUCM/VCS will likely want to use SIP. This guide mainly shows configurations for SIP.

Both CUCM and VCS Expressway can support H.323 endpoints. For CUCM, Inter-cluster Trunk (Non-Gatekeeper Controlled) needs to be configured to allow calls from H.323 endpoints.

Cisco VCS Expressway can function as H.323 gatekeeper (optionally) and can provide interworking of calls from H.323 to SIP. Dial plan / Search rules are used to find the right zone for outgoing part of the call. This zone can be configured as SIP or H.323, so if incoming call is H.323 and outgoing is SIP, then Expressway performs interworking between protocols. Note, that in this scenario SIP call leg uses delayed offer (DO) by default. There are different combinations possible and can be configured for specific scenarios.

For assistance in registering your video devices to CUCM or VCS (if not already registered) see below.

## Endpoint Configuration for CUCM

The screenshot displays the Cisco Endpoint Configuration web interface. At the top, there is a blue header with the Cisco logo on the left and the user 'Stephen-BlueJeans' with 'Cisco EX60' on the right. Below the header is a navigation bar with tabs: Home, Call Control, Configuration (selected), Diagnostics, and Maintenance. The main content area is titled 'System Configuration' and features a left-hand sidebar with a search bar and a list of configuration categories: Audio, Cameras, Conference, FacilityService, H323, Logging, Network, NetworkServices, Peripherals, Phonebook Server, Provisioning (highlighted in blue), RTP Ports Range, Security, SerialPort, SIP, Standby, SystemUnit, Time, UserInterface, and Video. The main panel shows the 'Provisioning' section, which includes a 'Refresh' button, 'Collapse all' and 'Expand all' buttons, and a list of settings: Connectivity (Auto), HttpMethod (POST), LoginName (empty field, 0 to 80 characters), Mode (CUCM), and Password (empty field, 0 to 64 characters, with a 'Clear' button). Below this is the 'ExternalManager' section, which includes: Address (10.4.7.xx, 0 to 64 characters), AlternateAddress (empty field, 0 to 64 characters), Domain (empty field, 0 to 64 characters), Path (empty field, 0 to 255 characters), and Protocol (HTTP).

Figure 1

**To configure Cisco Endpoint to work with CUCM using web UI (see screenshot above Figure 1):**

- 1) Go to Configuration > System Configuration > Provisioning section and set Mode to CUCM. Click ok to save the changes.
- 2) Go to the ExternalManager section and enter the IP address or DNS name of the CUCM in the External Manager input field. Click ok to save the changes.

Note: this assumes endpoints are already configured on CUCM side.

**To configure Cisco Endpoint to go back to non-CUCM (autonomous) mode (see screenshots below Figure 2 and 3):**

- 1) Go to Configuration > System Configuration > Provisioning section and set Mode to Off. Click ok to save the changes.
- 2) Go to Configuration > System Configuration > Network Services. Make sure H323 Mode and SIP Mode are set to On.
- 3) Go to Configuration > System Configuration > SIP. Clear Proxy 1 Address.

The screenshot displays the Cisco EX60 configuration web interface. The top navigation bar includes the Cisco logo, a user profile for 'Stephen-BlueJeans', and tabs for 'Home', 'Call Control', 'Configuration', 'Diagnostics', and 'Maintenance'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, with 'NetworkServices' highlighted. The main content area is titled 'NetworkServices' and contains a table of service modes. Two red arrows point to the 'H323 Mode' and 'SIP Mode' rows, both of which are set to 'On'. The interface also includes a search bar, a 'Refresh' button, and 'Collapse all'/'Expand all' controls.

Service	Mode
CDP Mode	On
H323 Mode	On
HTTP Mode	On
Medianet Metadata	Off
SIP Mode	On
Telnet Mode	Off
WelcomeText	On
XMLAPI Mode	On

Figure 2

SerialPort

SIP

Standby

SystemUnit

Time

UserInterface

Video

Profile 1

DefaultTransport

Auto

DisplayName

Stephen-BlueJeans

(0 to 255 characters)

Line

Private

Mailbox

(0 to 255 characters)

Outbound

Off

TlsVerify

Off

Type

Standard

URI

(0 to 255 characters)

Authentication 1

LoginName

(0 to 128 characters)

Password

Clear

(0 to 128 characters)

Ice

DefaultCandidate

Host

Mode

Auto

Proxy 1

Address

(0 to 255 characters)

Discovery

Manual




Figure 3

The screenshot shows the Cisco VCS-C web interface. The top navigation bar includes 'Home', 'Call Control', 'Configuration', 'Diagnostics', and 'Maintenance'. The user is logged in as 'admin'. The left sidebar lists various configuration categories, with 'Provisioning' selected. The main content area is titled 'System Configuration' and contains two sections: 'Provisioning' and 'ExternalManager'. The 'Provisioning' section has fields for 'Connectivity' (set to 'Auto'), 'HttpMethod' (set to 'POST'), 'LoginName' (empty, with a note '(0 to 80 characters)'), 'Mode' (set to 'VCS'), and 'Password' (empty, with a 'Clear' button and a note '(0 to 64 characters)'). The 'ExternalManager' section has fields for 'Address' (set to '10.4.7.xx', with a note '(0 to 64 characters)'), 'AlternateAddress' (empty, with a note '(0 to 64 characters)'), 'Domain' (empty, with a note '(0 to 64 characters)'), 'Path' (empty, with a note '(0 to 255 characters)'), and 'Protocol' (set to 'HTTP').

System Configuration

Search...

Audio

Cameras

Conference

FacilityService

H323

Logging

Network

NetworkServices

Peripherals

Phonebook Server

Provisioning

RTP Ports Range

Security

SerialPort

SIP

Standby

SystemUnit

Time

UserInterface

Video

Provisioning

Refresh

Collapse all

Expand all

Connectivity

Auto

HttpMethod

POST

LoginName

(0 to 80 characters)

Mode

VCS

Password

Clear

(0 to 64 characters)

ExternalManager

Address

10.4.7.xx

(0 to 64 characters)

AlternateAddress

(0 to 64 characters)

Domain

(0 to 64 characters)

Path

(0 to 255 characters)

Protocol

HTTP

Figure 4

**To configure Cisco Endpoint to work with Cisco VCS-C using web UI (see screenshot above Figure 4):**

- 1) Go to Configuration > System Configuration > Provisioning section and set Mode to VCS. Click ok to save the changes.
- 2) Go to the ExternalManager section and enter the IP address or DNS name of the VCS-C in the External Manager input field. Click ok to save the changes.

## Example: Cisco VCS-Expressway Connecting to BlueJeans

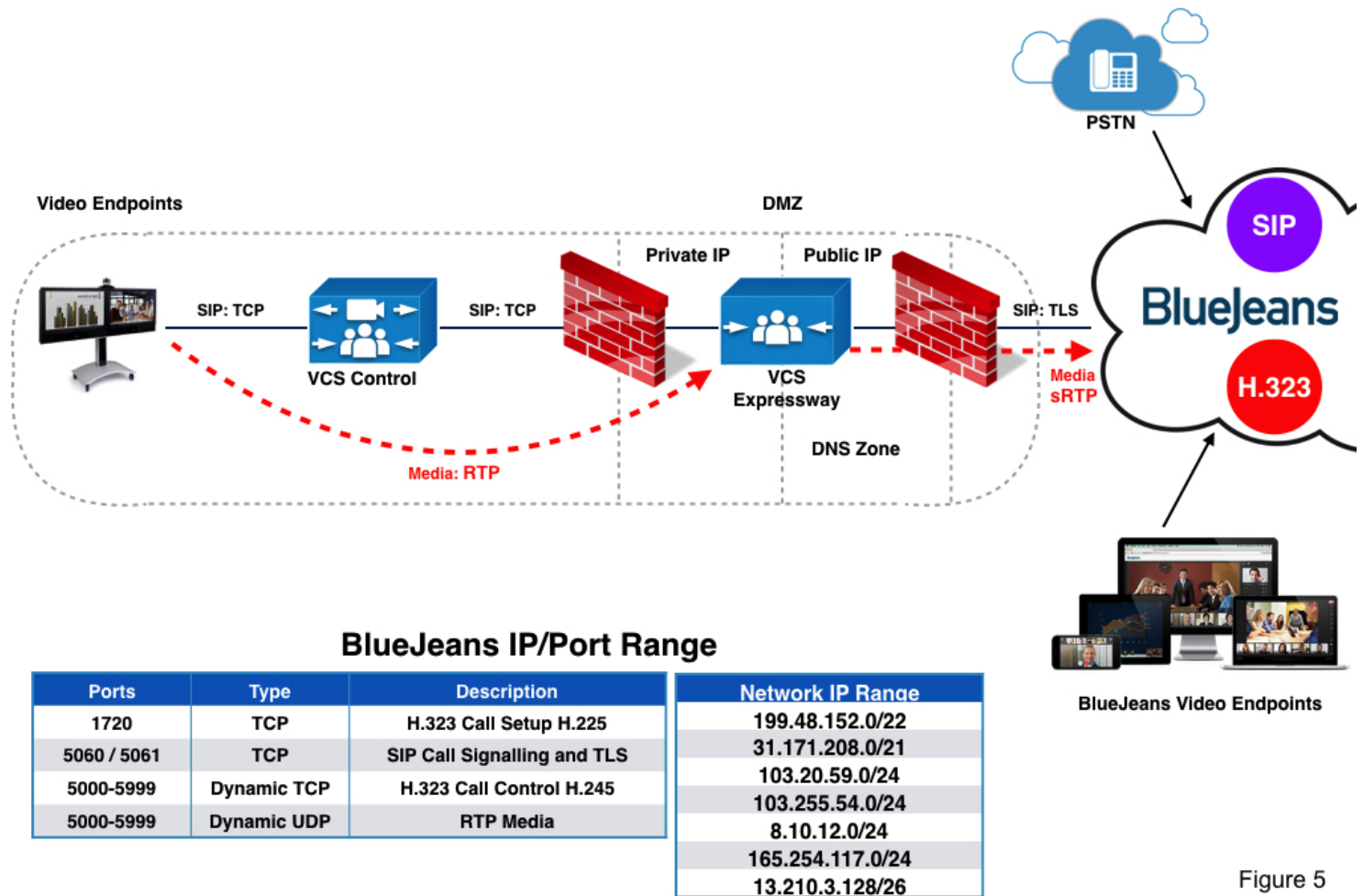


Figure 5

### Video devices registered to Cisco Video Conference Server (VCS-C) as controller with Cisco Video Conference Server (VCS-E) as 'Edge' node

In this configuration your video devices (room systems) register to Cisco VCS-C acting as the controller with Cisco VCS-Expressway as 'Edge' node for firewall transversal. In the above topology, Room system registers (in non-secure mode) to Cisco VCS-C > SIP Trunk provisioned > Cisco VCS-E > BlueJeans cloud. The call is made to @bjn.vc. The VCS-C routes call to VCS-E based on 'bjn.vc' host portion of SIP URL.

The VCS-E has two IP addresses: private and public. It performs conversion of SIP signaling from TCP to TLS and media from RTP to SRTP for encrypted calls.

## Example: Cisco CUCM/VCS-E Connecting to BlueJeans

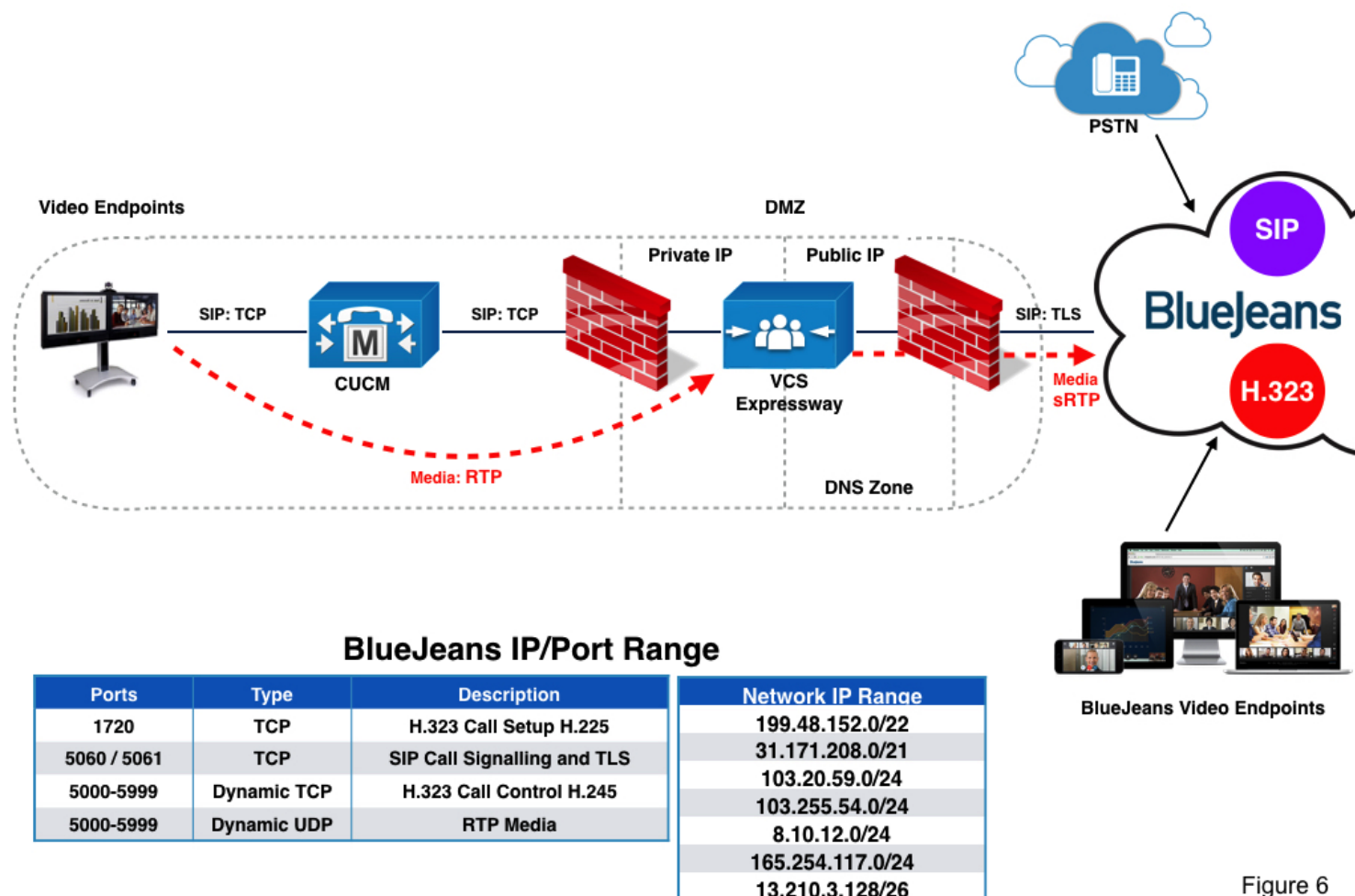


Figure 6

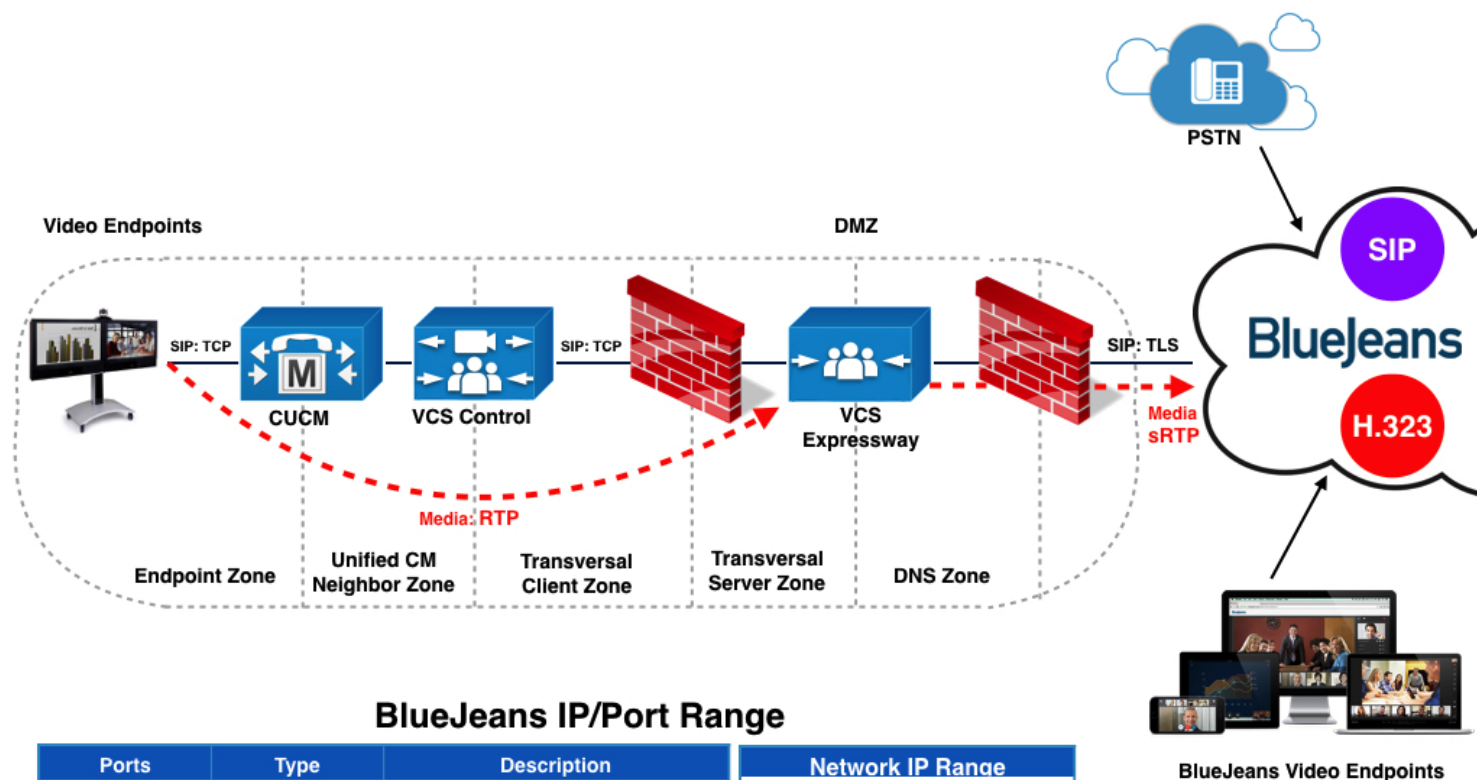
### Video devices registered to Cisco Unified Call Manager (CUCM) as controller with Cisco Video Conference Server (VCS-E) as 'Edge' node

In this configuration video devices (room systems) are registered to Cisco Unified Call Manager (CUCM) acting as the controller with Cisco VCS-Expressway as 'Edge' node for firewall transversal. In the above topology, Room system registers to CUCM > SIP trunk is provisioned > Cisco VCS-E > BlueJeans cloud. The call is made to @bjn.vc. The CUCM routes call to VCS-E based on 'bjn.vc' host portion of SIP URL.

VCS-E has two IP addresses: private and public. It performs conversion of SIP signaling from TCP to TLS and media from RTP to SRTP for encrypted calls.



## Example: Cisco Infrastructure Connecting to BlueJeans



BlueJeans IP/Port Range

Ports	Type	Description	Network IP Range
1720	TCP	H.323 Call Setup H.225	199.48.152.0/22
5060 / 5061	TCP	SIP Call Signalling and TLS	31.171.208.0/21
5000-5999	Dynamic TCP	H.323 Call Control H.245	103.20.59.0/24
5000-5999	Dynamic UDP	RTP Media	103.255.54.0/24
			8.10.12.0/24
			165.254.117.0/24
			13.210.3.128/26

Figure 7

### Cisco Unified Communications Manager (CUCM), with Cisco Expressway-C and Cisco Expressway-E

In this example above, the enterprise video devices are registered to Cisco Unified Communications Manager (CUCM), with Cisco Expressway-C and Cisco Expressway-E being used for secure calling and firewall traversal.

The diagram above displays the overall setup and call flow. The enterprise architecture consists of the appropriate components based on the Cisco Video deployment guides. The video device or room system (Endpoint Zone) would register to the Cisco Unified Communications Manager (CUCM) and the CUCM would have a SIP trunk for external video calls to the Cisco VCS-Expressway. The VCS-Expressway is usually deployed in the DMZ as the video edge device for calls in or out of the enterprise.



NOTE: It is recommended that a brand new Traversal Zone pair and DNS Zone be created as many customers use VCS/Expressway for all sorts of different use cases. Doing this way will avoid any potential disruption.

## Deployment and Configuration

The following steps cover the required one time setup for connecting to BlueJeans. We are assuming here that your Cisco Infrastructure is up and running.

Specifics for the configuration will depend on what topology you are using and if your video endpoints are registered to a Cisco Unified Call Manager or a Cisco VCS Expressway-C.

### Step 1 - Configure Port Range

Set the port range for Cisco VCS Expressway, or other edge traversal devices and firewalls for BlueJeans (see range above).

### Step 2 - Configure DNS Zone

Configure the DNS zone and search rule if you want to ensure that TLS and sRTP (recommended) are used in fallback scenarios.

You can use the default DNS zone configuration on the Cisco VCS-E to route calls to BlueJeans. The default configuration will result in Cisco Expressway attempting best-effort TLS (with fallback to TCP) and sRTP media encryption (with fallback to RTP). But if you want to ensure that TLS and sRTP are used it is recommended you create a new DNS Zone to use for encryption.

<b>Zone Configuration Setting</b>	<b>Value if Using 3rd-Party CA Signed Certificate</b>	<b>Value if Using Self-Signed Certificate</b>
<b>H.323 Mode</b>	<b>On</b> (default) or <b>Off</b> (recommended)	<b>On</b> (default) or <b>Off</b> (recommended)
<b>SIP Media encryption mode</b>	<b>Auto</b> (default)	<b>Auto</b> (default)
<b>TLS Verify mode</b>	<b>On</b>	<b>Off</b>
<b>Advanced zone profile</b>	<b>Default</b> or <b>Custom</b> (required if <b>H.323 Mode</b> is set to <b>Off</b> )	<b>Default</b> or <b>Custom</b> (required if <b>H.323 Mode</b> is set to <b>Off</b> )
<b>Automatically respond to SIP searches</b>	<b>Off</b> (default) or <b>On</b> (required if <b>H.323 Mode</b> is set to <b>Off</b> )	<b>Off</b> (default) or <b>On</b> (required if <b>H.323 Mode</b> is set to <b>Off</b> )
<b>SIP SDP attribute line limit mode</b>	<b>Off</b> (required if <b>Advanced zone profile</b> is set to <b>Custom</b> )	<b>Off</b> (required if <b>Advanced zone profile</b> is set to <b>Custom</b> )

Figure 8

Use the above table (Figure 8) to configure the DNS zone on Cisco Expressway-E. The configuration varies depending on the type of certificate in use, and whether you turn on H.323 mode.










Status	System	Configuration	Applications	Users	Maintenance
<b>DNS</b>					
<b>DNS settings</b>					
System host name	<input type="text"/>  				
Domain name	<input type="text"/> 				
DNS requests port range	<input type="text" value="Use the ephemeral port range"/> 				
<b>Default DNS servers</b>					
Address 1	<input type="text" value="10.4.4.11"/> 				
Address 2	<input type="text" value="10.4.4.12"/> 				
Address 3	<input type="text"/> 				
Address 4	<input type="text"/> 				
Address 5	<input type="text"/> 				

Figure 9

Configure the Cisco Expressway-E to route calls to BlueJeans. Make sure Cisco Expressway-E has the appropriate DNS server configured System > DNS

Make sure Cisco Expressway-E is setup for dual network interfaces and the firewall rules (previous step) are setup to allow traffic from video device to CUCM or (VCS-Expressway-C) to VCS-Expressway-E.

## Recommend DNS Zone for Encryption

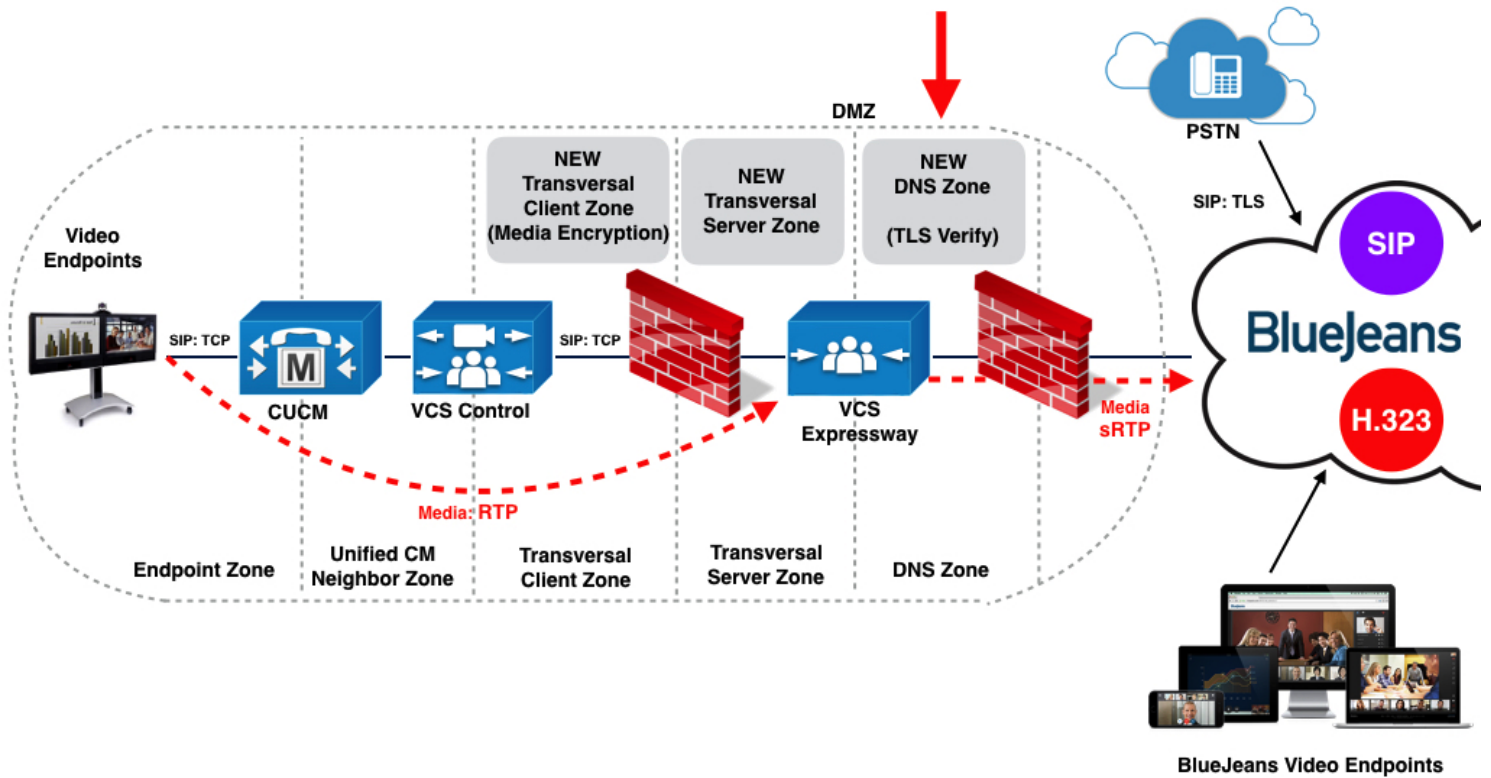


Figure 10

Creating a New DNS Zone for BlueJeans calls is recommended so to have no risk of any disruption to a production environment, but is optional as you can use existing DNS Zone if desired.





































Status	System	Configuration	Applications	Users	Maintenance
<b>Edit zone</b>					
<b>SIP</b>					
Mode	On  				
TLS verify mode	Off  				
Fallback transport protocol	TLS  				
Media encryption mode	Force encrypted  				
ICE support	Off  				
Preloaded SIP routes support	Off  				
Modify DNS request	Off  				
AES GCM support	Off  				
<b>Authentication</b>					
SIP authentication trust mode	Off  				
<b>Advanced</b>					
Include address record	Off  				
Zone profile	Custom  				
Automatically respond to SIP searches	Off  				
Send empty INVITE for interworked calls	Off  				
SIP parameter preservation	Off  				
SIP poison mode	Off  				
SIP UDP/BFCP filter mode	Off  				
SIP UDP/IX filter mode	Off  				
SIP record route address type	IP  				
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Delete"/>					

Figure 11

Create a New DNS zone (or use existing one) to route outbound calls by going to VCS-Expressway-E Configuration > Zones > New DNS Zone and adding a zone per below configuration. The above configuration (Figure 11) is using encryption which is recommended.

NOTE: If you already have one, make sure the configuration matches this below:

Go to Configuration > Zones > Zones -> Create New

- Name: ZONE-BJN-PROD (or whatever you want to name it)
- Type: DNS

- H.323 Mode: Off
- SIP Mode: On
- Fallback transport protocol: TLS
- Media encryption mode: Force encrypted
- Zone profile: custom
- Send empty INVITE for interworked calls: off

**Note: We recommend that Early Offer is always used on CUCM and/or VCS SIP trunks to BlueJeans SIP servers. Early Offer (versus Delayed Offer sometimes selected by default on CUCM and/or VCS) helps to avoid various compatibility issues such as failure to join a meeting, calls being dropped after 15 minutes, asymmetric codecs being negotiated, etc. Recommended setup for Early Offer is presented later in this guide.**

## Recommend Transversal Zone Pair for Encryption

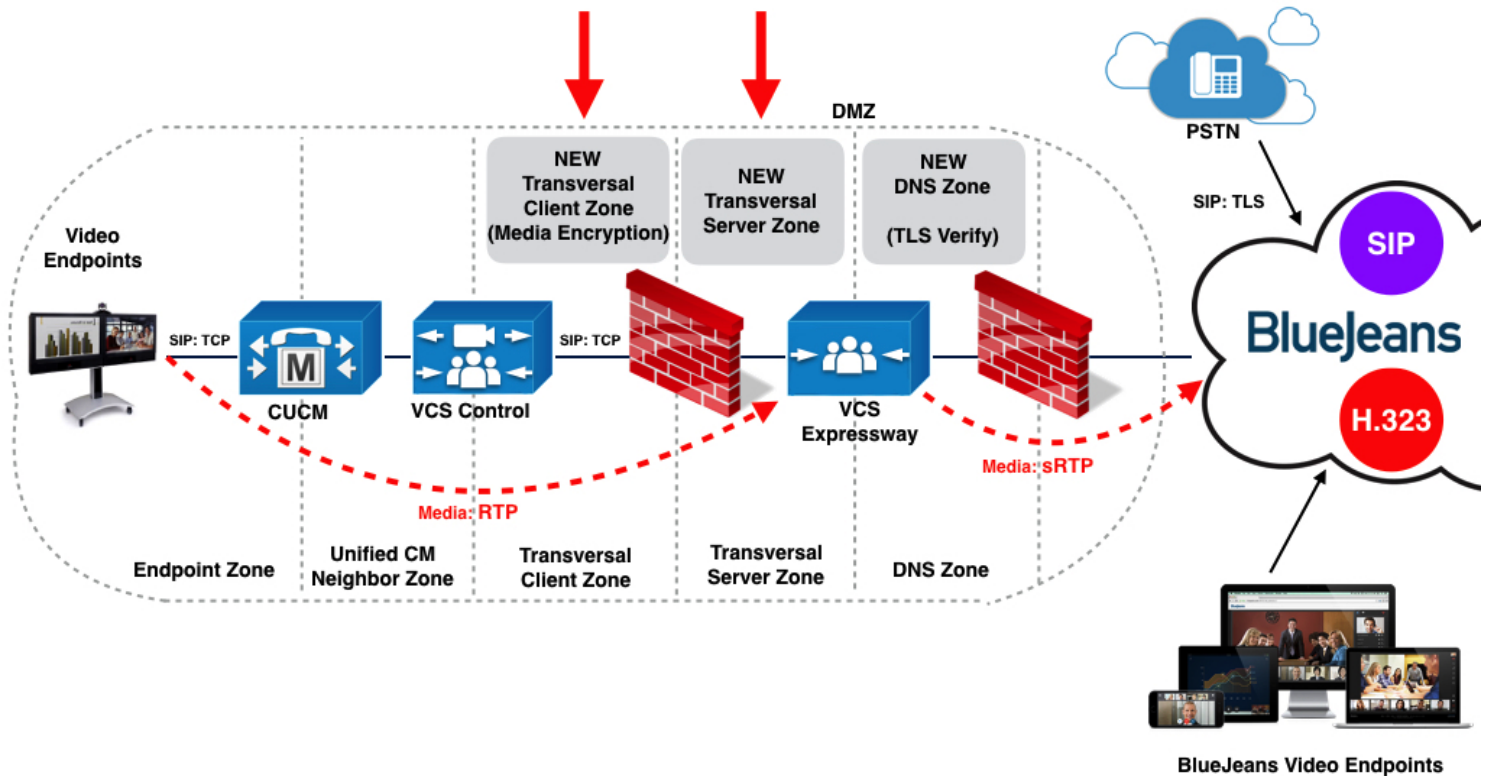


Figure 12

### Step 3 - Configure a Transversal Server/Client Pair (Optional)

For secure calling, configure a Traversal Client zone and search rule on Cisco Expressway-C (or Cisco VCS Control) and a Traversal Server zone on Cisco Expressway-E (or Cisco VCS-E).

You can skip this task if you are happy with Cisco Expressway attempting best-effort TLS (with fallback to TCP) and sRTP media encryption (with fallback to RTP). In that case, the DNS zone configuration from the previous task is sufficient.

The recommended zone configuration for secure calling uses a Traversal Client zone on Cisco VCS-C and a Traversal Server zone and DNS zone on Cisco VCS-E. If you already have one or more Traversal Client/Traversal Server zone pairs in your configuration, you can use these zones, but we recommend adding a new pair specifically for BlueJeans.

In this procedure:

- On the Cisco Expressway-C, you apply the media encryption policy on the Traversal Client zone, and create a search rule that routes outbound BlueJeans calls towards that zone.
- On the Cisco Expressway-E, you configure the TLS Verify mode on the DNS zone. (The search

rule that routes outbound BlueJeans calls towards that zone was configured in the previous task.)

We recommend this configuration for two reasons:

- To avoid unnecessarily engaging the B2BUA (back-to-back user agent) on the Cisco Expressway-E.
- To encrypt all traffic that egresses the firewall so that someone who may have access to your DMZ cannot sniff your traffic.

Use the following table (Figure 13) to configure the Traversal Client and Traversal Server zones:

<b>Zone Configuration Setting</b>	<b>Value On Traversal Client Zone (Cisco Expressway-C)</b>	<b>Value on Traversal Server Zone (Cisco Expressway-E)</b>
<b>H.323 Mode</b>	<b>Off</b> (recommended) or <b>On</b> (default)	<b>Off</b> (recommended) or <b>On</b> (default)
<b>SIP Media encryption mode</b>	<b>Force Encrypted</b> or <b>Best Effort</b> (required if <b>H.323 Mode</b> is set to <b>On</b> )	<b>Auto</b>

Figure 13

#### **Step 4 - Reduce SIP Timeout on VCS-Expressway (Optional)**

Configure the SIP TCP timeout value on Cisco Expressway / Cisco VCS (X8.6). From Cisco Expressway / Cisco VCS Version X8.6 the SIP TCP timeout value is configurable. The default value is 10 seconds. It is recommended that you set the timeout to the lowest value that is appropriate for your deployment. A value of 1 second is likely to be suitable in most cases, unless your network has extreme amounts of latency (such as video over satellite communications).

To set the SIP TCP timeout value:

- Access the command line interface (this setting cannot be configured through the web interface).

- Type the following command, replacing "n" with the required timeout value: xConfiguration SIP Advanced SipTcpConnectTimeout: *n*

Example: xConfiguration SIP Advanced SipTcpConnectTimeout: 1

Note: Reducing the timeout is optional, but may improve performance.



**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

**SIP Profile Configuration** Related Links: Back To Find/List

Save Delete Copy Reset Apply Config Add New

**Status**

- Status: Ready
- All SIP devices using this profile must be restarted before any changes will take affect.

**SIP Profile Information**

Name\* Standard SIP Profile - Trunk EO

Description Standard SIP Profile - Trunk EO

Default MTP Telephony Event Payload Type\* 101

Early Offer for G.Clear Calls\* Disabled

User-Agent and Server header information\* Pass Through Received Information as User-Ag

Version in User Agent and Server Header\* Major And Minor

Dial String Interpretation\* Phone number consists of characters 0-9, \*, #

Confidential Access Level Headers\* Disabled

☐ Redirect by Application

☐ Disable Early Media on 180

☐ Outgoing T.38 INVITE include audio mline

☐ Offer valid IP and Send/Receive mode only for T.38 Fax Relay

☒ Use Fully Qualified Domain Name in SIP Requests

☐ Assured Services SIP conformance

☐ Enable External QoS\*\*

**SDP Information**

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites\* TIAS and AS

SDP Transparency Profile Pass all unknown SDP attributes

Accept Audio Codec Preferences in Received Offer\* Default

☐ Require SDP Inactive Exchange for Mid-Call Media Change

☐ Allow RR/RS bandwidth modifier (RFC 3556)

Figure 14

## Step 5 - Configure SIP Profile and SIP Trunk

Configure the SIP profile and trunk to Cisco Expressway-E on the Cisco Unified Communications Manage (CUCM) in order for endpoints registered to CUCM to participate in a video meeting.

- In Unified Communications Manager, configure a SIP trunk between Unified Communications Manager and Cisco Expressway-C (or Cisco VCS Control).
- Configure the SIP profile. Configure a new SIP Trunk Profile by going to Device > Device Settings > SIP Profiles and add new profile with values (shown in above screenshot Figure 14).

Modify the following parameters:

- Name: Standard SIP Profile - Trunk (can name it whatever you like)
- User-Agent and Server header information: Pass-Through Received Information as User-Agent and Server Header
- Use Fully Qualified Domain Name in SIP Requests: check box

SDP Information:

- SDP Session-level Bandwidth for Early Offer and Re-invites: TIAS and AS

- SDP Transparency Profile: Pass all unknown SDP attributes

All other parameters should be OK as default.

Note: If there is already a SIP Trunk setup please ensure the configuration matches. All other parameters can be set to the default values.

The screenshot shows a configuration page with three main sections:

- Trunk Specific Configuration:**
  - Reroute Incoming Request to new Trunk based on\*: Never
  - Resource Priority Namespace List: < None >
  - SIP Rel1XX Options\*: Disabled
  - Video Call Traffic Class\*: Immersive
  - Calling Line Identification Presentation\*: Default
  - Session Refresh Method\*: Invite
  - Early Offer support for voice and video calls\*: Best Effort (no MTP inserted)
  - ☐ Enable ANAT
  - ☐ Deliver Conference Bridge Identifier
  - ☐ Allow Passthrough of Configured Line Device Caller Information
  - ☐ Reject Anonymous Incoming Calls
  - ☐ Reject Anonymous Outgoing Calls
  - ☐ Send ILS Learned Destination Route String
  - ☐ Connect Inbound Call before Playing Queuing Announcement
- SIP OPTIONS Ping:**
  - ☐ Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"
  - Ping Interval for In-service and Partially In-service Trunks (seconds)\*: 60
  - Ping Interval for Out-of-service Trunks (seconds)\*: 120
  - Ping Retry Timer (milliseconds)\*: 500
  - Ping Retry Count\*: 6
- SDP Information:**
  - ☐ Send send-receive SDP in mid-call INVITE
  - ☒ Allow Presentation Sharing using BFCP
  - ☒ Allow iX Application Media
  - ☒ Allow multiple codecs in answer SDP

Figure 15

Trunk Specific Configuration (above screenshot Figure 15)

- Video Call Traffic Class: Immersive
- Early Offer support for voice and video calls: Best Effort (no MTP inserted)

SDP Information:

Select (check boxes):

- Allow Presentation Sharing using BFCP
- Allow iX Application Media
- Allow multiple codecs in answer SDP

Keep all other parameters unchanged. Save configuration.

Note: Note that if no encryption will be used with CUCM should use Early Offer.

Parameter	Value
Name	SIP Profile with BFCP (or any name you choose)
SDP Session Level Bandwidth modifier	TIAS and AS
User-Agent and Server Header information	Pass through received information as User-Agent
Early Offer support for voice and video calls (insert MTP if needed)	Check the box
Allow presentation sharing using BFCP	Check the box

Figure 16

Parameter	Value
Device Name	A name for the trunk
Device Pool	Appropriate device pool for video calls
Destination	Add IP address of internal VCS interface and port 5060
SIP Trunk Security Profile	Non Secure SIP Trunk Profile (NOTE if secure SIP Trunk is needed, need to modify this accordingly)
SIP Profile	SIP Profile with BFCP (configured in previous step)

Figure 17

## Step 6 - Enable BFCP

Enable BFCP for Presentation Sharing

Depending on which topology you are using you will want to make sure to enable BFCP (Binary Floor Control Protocol)

Verify that BFCP is enabled on the Unified Communications Manager neighbor zone in Cisco Expressway-C or Cisco VCS Control:

- If you are using X8.1 or later, BFCP is automatically enabled when you choose the Cisco Unified Communications Manager (8.6.1 or later) zone profile on the Unified Communications Manager neighbor zone.
- If you are using a release prior to X8.1, set **SIP UDP/BFCP filter mode** to **Off** on the zone profile in Cisco VCS Control.

Verify that BFCP is enabled on the SIP profile in Unified Communications Manager:

- If you are using X8.1 or later, BFCP is automatically enabled if you choose the **Standard SIP Profile for Cisco VCS** when defining the SIP trunk to the Cisco Expressway-C or Cisco VCS Control.
- If you are using a release prior to X8.1, check the **Allow Presentation Sharing using BFCP** box on the SIP profile.

- To enable presentation sharing, check the **Allow Presentation Sharing using BFCP** check box in the **Trunk Specific Configuration** section of the **SIP Profile Configuration** window.

The screenshot shows the Cisco Unified CM Administration web interface. The top navigation bar includes links for System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main title is "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The user is logged in as "admin".

The page is titled "SIP Route Pattern Configuration". It includes a "Related Links" section with "Back To Find/List" and "Go". Below the title bar, there are buttons for "Save", "Delete", "Copy", and "Add New".

The configuration is organized into several sections:

- Status:** Shows "Status: Ready".
- Pattern Definition:**
  - Pattern Usage: Domain Routing
  - IPv4 Pattern\*: bjn.vc
  - IPv6 Pattern: (empty)
  - Description: (empty)
  - Route Partition: < None >
  - SIP Trunk/Route List\*: TRUNK-SIP-EXP-E (with an "Edit" link)
  - ☐ Block Pattern
- Calling Party Transformations:**
  - ☐ Use Calling Party's External Phone Mask
  - Calling Party Transformation Mask: (empty)
  - Prefix Digits (Outgoing Calls): (empty)
  - Calling Line ID Presentation\*: Default
  - Calling Line Name Presentation\*: Default
- Connected Party Transformations:**
  - Connected Line ID Presentation\*: Default
  - Connected Line Name Presentation\*: Default

At the bottom, there are buttons for "Save", "Delete", "Copy", and "Add New".

Figure 18

## Step 7 - Add Route Pattern CUCM

On the Unified Communications Manager, add a route pattern to route to BlueJeans domain from video device to the VCS-Expressway via the SIP trunk from CUCM. You need to add a route pattern for \*.bjn.vc and point it at the SIP trunk to Cisco Expressway-E (or Cisco Cisco Expressway-C if in use) by choosing the SIP trunk you created in previous step.

To configure SIP Route Pattern:

Call Routing > SIP Route Pattern and click to Add New (or select Find to edit existing one)

Pattern Usage: select Domain or IP address routing, depending on situation

IPv4 Pattern: enter domain name (such as bjn.vc) or IP address

SIP Trunk/Route List: select corresponding SIP trunk from the list (needs to be configured already)

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

**Phone Configuration** Related Links: Back To Find/List

Save Delete Copy Reset Apply Config Add New

**Status**  
Status: Ready

**Association**  
Modify Button Items  
1 Line [1] - 2101 (no partition)  
----- Unassigned Associated Items -----  
2 Line [2] - Add a new DN

**Phone Type**  
Product Type: Cisco TelePresence Codec C60  
Device Protocol: SIP

**Real-time Device Status**  
Registration: Registered with Cisco Unified Communications Manager mveng-cucm  
IPv4 Address: 10.4.4.58  
Active Load ID: TC7.3.9.b938c8e  
Inactive Load ID: None  
Download Status: None

**Device Information**  
☒ Device is Active  
☒ Device is trusted  
 MAC Address\* 00506083300B  
 Description SEP00506083300B  
 Device Pool\* Default View Details  
 Common Device Configuration < None > View Details  
 Phone Button Template\* Standard Cisco TelePresence C60 Codec  
 Common Phone Profile\* Standard Common Phone Profile View Details  
 Calling Search Space < None >  
 AAR Calling Search Space < None >  
 Media Resource Group List < None >  
 User Hold MOH Audio Source < None >  
 Network Hold MOH Audio Source < None >  
 Location\* Hub\_None  
 AAR Group < None >  
 User Locale < None >  
 Network Locale < None >  
 Privacy\* Default  
 Device Mobility Mode\* Default View Current Device Mobility Settings  
 Owner ☐ User ☒ Anonymous (Public/Shared Space)  
 Owner User ID  
 Mobility User ID < None >  
 Phone Load Name  
 Use Trusted Relay Point\* Default  
 Always Use Prime Line\* Default  
 Always Use Prime Line for Voice Message\* Default  
 Geolocation < None >  
☒ Retry Video Call as Audio  
☐ Ignore Presentation Indicators (internal calls only)  
☒ Allow Control of Device from CTI  
☒ Logged Into Hunt Group  
☐ Remote Device

**Number Presentation Transformation**  
**Caller ID For Calls From This Phone**  
 Calling Party Transformation CSS < None >  
☒ Use Device Pool Calling Party Transformation CSS (Caller ID For Calls From This Phone)

Figure 19

To configure new device (TelePresence Endpoint):  
Device > Phone and click to Add New (or select Find to edit existing one)

Phone Type: select 'Cisco Telepresence SX10' or another, depending on your device type

- MAC Address: enter MAC address
- Device Pool: Default
- Phone Button Template: Standard ...
- Device Security Profile: ... Standard ...
- SIP Profile: Standard SIP Profile - TelePresence Endpoint
- Owner: Anonymous



- Web Access: HTTP+HTTPS

## Now Save Configuration

Now configure the Blue Jeans number as a favorite on all room systems. On the CUCM administration page, go to Device > Phone and search for all video room systems. Go to one of the video devices and on the right top choose “Add/Update Speed Dials” in the related links dropdown.

The screenshot shows the 'Phone Configuration' page in Cisco Unified CM Administration. The 'Protocol Specific Information' section is expanded, showing various configuration options. The 'Web Access' dropdown is set to 'HTTP+HTTPS'. The 'SIP Profile' dropdown is set to 'Standard SIP Profile - TelePresence Endpoint'. The 'Digest User' dropdown is set to '< None >'. The 'Media Termination Point Required' checkbox is unchecked. The 'Unattended Port' checkbox is unchecked. The 'Require DTMF Reception' checkbox is unchecked.

Parameter	Value
Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco TelePresence Codec C60 - Standard SIP I
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile - TelePresence Endpoint
Digest User	< None >
Media Termination Point Required	<input type="checkbox"/>
Unattended Port	<input type="checkbox"/>
Require DTMF Reception	<input type="checkbox"/>

Figure 20

The screenshot shows the 'Phone Configuration' page in Cisco Unified CM Administration. The 'Product Specific Configuration Layout' section is expanded, showing various configuration options. The 'Web Access' dropdown is set to 'HTTP+HTTPS'. The 'SSH Access' dropdown is set to 'Disabled'. The 'Default Call Protocol\*' dropdown is set to 'SIP'. The 'Quality Improvement Server' dropdown is set to 'Use Endpoint'. The 'Telnet Access\*' dropdown is set to 'Off'. The 'Microphone Unmute On Disconnect\*' dropdown is set to 'On'. The 'Call Logging Mode\*' dropdown is set to 'On'. The 'OSD Encryption Indicator\*' dropdown is set to 'Auto'. The 'Alternate phone book server type\*' dropdown is set to 'UDS'. The 'Alternate phone book server address' field is empty. The 'Default Volume' field is set to 70. The 'Max Total Downstream Rate' field is set to 10000. The 'Max Total Upstream Rate' field is set to 10000. The 'System Name' field is empty.

Parameter	Value
Room Name (from Exchange(R))	
Web Access*	HTTP+HTTPS
SSH Access*	Disabled
Default Call Protocol*	SIP
Quality Improvement Server	Use Endpoint
Multipoint Mode*	Use Endpoint
Telnet Access*	Off
Microphone Unmute On Disconnect*	On
Call Logging Mode*	On
OSD Encryption Indicator*	Auto
Alternate phone book server type*	UDS
Alternate phone book server address	
Default Volume	70
Max Total Downstream Rate	10000
Max Total Upstream Rate	10000
System Name	

Figure 21

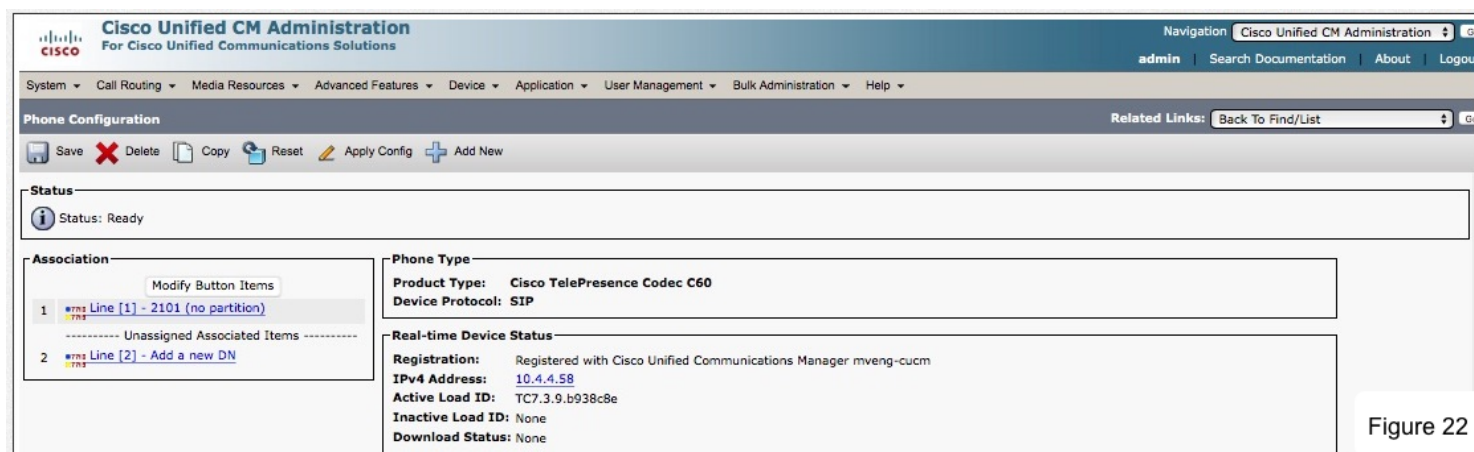


Figure 22

Add a number to the directory. Makes sense to make the number with a meaningful label such as “BlueJeans”.

Go to the Line 1 on each video device by going to Device > Phone and searching for each device. Click on the Line configuration on the Left panel as see above screenshot (Figure 22).

Select Line [1] - Add a new DN (see below screenshot)

Directory Number: enter new number to correspond to numbering scheme (21..)

Click Save

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

admin | Search Documentation | About | Log out

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

**Directory Number Configuration** Related Links: [Configure Device \(SEP00506083300B\)](#)

Save Delete Reset Apply Config Add New

**-Status-**  
Status: Ready

**-Directory Number Information-**

Directory Number\* 2101 ☐ Urgent Priority

Route Partition < None >

Description

Alerting Name

ASCII Alerting Name

External Call Control Profile < None >

☒ Allow Control of Device from CTI

Associated Devices SEP00506083300B

[Edit Device](#)  
[Edit Line Appearance](#)

Dissociate Devices

**-Directory Number Settings-**

Voice Mail Profile < None > (Choose <None> to use system default)

Calling Search Space < None >

BLF Presence Group\* Standard Presence group

User Hold MOH Audio Source < None >

Network Hold MOH Audio Source < None >

Auto Answer\* Auto Answer Off

☐ Reject Anonymous Calls

Figure 23

Note: you can also add 3rd party SIP device, for that select Phone Type as 'Third-Party SIP Device (Advanced)'

Repeat this for every video room system you want to connect to BlueJeans.



The screenshot displays the Cisco Expressway-C configuration web interface. At the top, the Cisco logo and 'Cisco Expressway-C' are visible. Below the logo is a navigation bar with tabs: Status, System (selected), Configuration, Applications, Users, and Maintenance. The main content area is titled 'DNS' and contains two sections: 'DNS settings' and 'Default DNS servers'. In the 'DNS settings' section, the 'System host name' field is set to 'mveng-expwy-c', the 'Domain name' is 'corp.bluejeans.com', and the 'DNS requests port range' is set to 'Use the ephemeral port range'. The 'Default DNS servers' section lists five addresses: Address 1 (10.4.4.11), Address 2 (10.4.4.12), and three empty fields for Address 3, Address 4, and Address 5. Each field has an information icon (i) to its right.

**System host name**: mveng-expwy-c

**Domain name**: corp.bluejeans.com

**DNS requests port range**: Use the ephemeral port range

































**Default DNS servers**

Address	Value
Address 1	10.4.4.11
Address 2	10.4.4.12
Address 3	
Address 4	
Address 5	

Figure 24

If your topology is using the Cisco VCS-Expressway-C as the controller here are some guidelines for the configuration. If you are registering your video endpoints to the CUCM or are not using Cisco VCS-Expressway-C skip this.

Configure the VCS-Expressway-C to route calls to BlueJeans. Make sure VCS has the appropriate DNS server configured System > DNS (see screenshot above Figure 24)

Status	System	Configuration	Applications	Users	Maintenance
<b>Edit zone</b>					
<b>Configuration</b>					
Name	* ZONE-VCS-E 				
Type	Neighbor				
Hop count	* 15 				
<b>H.323</b>					
Mode	Off  				
<b>SIP</b>					
Mode	On  				
Port	* 5060 				
Transport	TCP  				
Accept proxied registrations	Allow  				
Media encryption mode	Auto  				
ICE support	Off  				
Multistream mode	On  				
Preloaded SIP routes support	Off  				
AES GCM support	Off  				
<b>Authentication</b>					
Authentication policy	Treat as authenticated  				
SIP authentication trust mode	Off  				
<b>Location</b>					
Look up peers by	Address  				
Peer 1 address	10.4.7.208 				
Peer 2 address	<input type="text"/> 				
Peer 3 address	<input type="text"/> 				
Peer 4 address	<input type="text"/> 				
Peer 5 address	<input type="text"/> 				

To configure Cisco Expressway-C as Controller (see screenshot above Figure 25)

Configuration > Zones > Zones > Add New

- Name: ZONE-VCS-E
- Type: Neighbor
- H.323 Mode: Off
- SIP Mode: On
- Port: 5060
- Transport: TCP
- Location:
- Look up peers by: Address
- Peer 1 address: 10.4.xxx.xxx (Expressway E private address)

See screenshot below:

- Zone profile: custom
- Send empty INVITE for interworked calls: off

Advanced

Zone profile

Custom

Monitor peer status

No

Call signaling routed mode

Auto

Automatically respond to H.323 searches

Off

Automatically respond to SIP searches

Off

Send empty INVITE for interworked calls

Off

SIP parameter preservation

Off

SIP poison mode

Off

SIP encryption mode

Auto

SIP REFER mode

Forward

SIP multipart MIME strip mode

Off

SIP UPDATE strip mode

Off

Interworking SIP search strategy

Options

SIP UDP/BFCP filter mode

Off

SIP UDP/IX filter mode

Off

SIP record route address type

IP

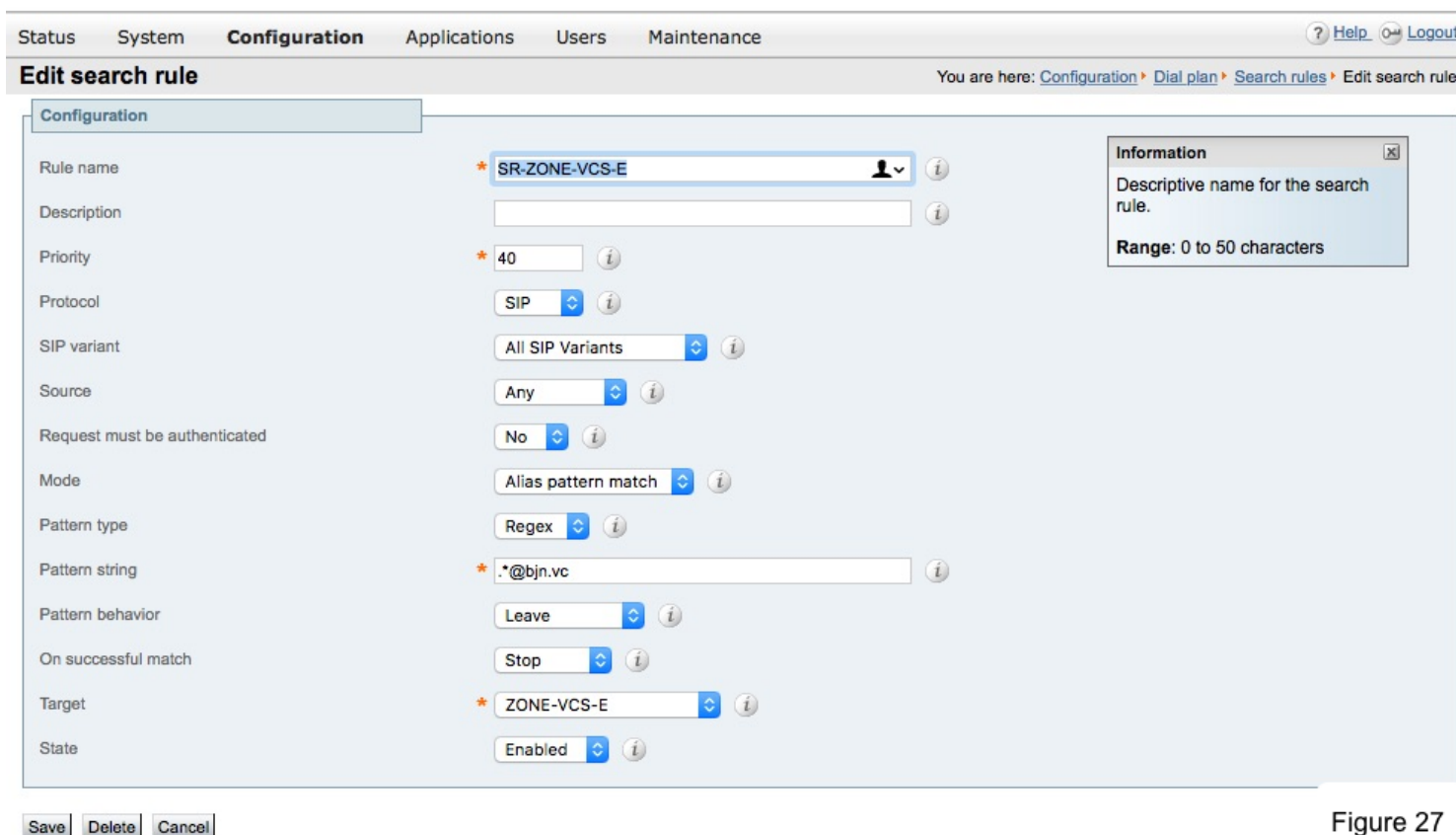
SIP Proxy-Require header strip list

Save

Cancel

Delete

Figure 26



Status System **Configuration** Applications Users Maintenance

**Edit search rule** You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > [Edit search rule](#)

**Configuration**

Rule name \* SR-ZONE-VCS-E ⓘ

Description ⓘ

Priority \* 40 ⓘ

Protocol SIP ⓘ

SIP variant All SIP Variants ⓘ

Source Any ⓘ

Request must be authenticated No ⓘ

Mode Alias pattern match ⓘ

Pattern type Regex ⓘ

Pattern string \* \*. \*@bjn.vc ⓘ

Pattern behavior Leave ⓘ

On successful match Stop ⓘ

Target \* ZONE-VCS-E ⓘ

State Enabled ⓘ

**Information** ⓘ

Descriptive name for the search rule.  
Range: 0 to 50 characters

Save Delete Cancel

Figure 27

If you are registering your video endpoints to the CUCM or are not using Cisco VCS-Expressway-C skip this.

Search rules define how the VCS routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule.

Create a search rule on Cisco Expressway-C with the following properties:

Go to Configuration > Dial Plan > Search Rules > Add New

- Rule name: SR-ZONE-VCS-E
- Priority: 40 or ANY
- Protocol: SIP
- Source: ANY
- Mode: Alias pattern match
- Pattern type: Regex
- Pattern string: \*. \*@bjn.vc
- Pattern behavior: Leave
- On successful match: Stop

- Target: ZONE-VCS-E (to point to previously created zone)
- State: Enabled

## Configuring VCS Expressway-E

The screenshot displays the Cisco Expressway-E configuration web interface. At the top, the Cisco logo and 'Cisco Expressway-E' title are visible. Below this is a navigation bar with tabs: Status, **System**, Configuration, Applications, Users, and Maintenance. The 'System' tab is active, and the 'DNS' section is selected. The 'DNS settings' panel includes fields for 'System host name' (with a dropdown arrow), 'Domain name', and 'DNS requests port range' (set to 'Use the ephemeral port range'). Each field has an information icon. Below this is the 'Default DNS servers' panel, which lists five addresses: Address 1 (10.4.4.11), Address 2 (10.4.4.12), Address 3, Address 4, and Address 5, each with an information icon.

Figure 28

Configure the VCS-Expressway-E to route calls to BlueJeans. Make sure VCS has the appropriate DNS server configured System > DNS

Status
System
**Configuration**
Applications
Users
Maintenance

Edit zone

Configuration

Name
\* ZONE-BJN-PROD ⓘ

Type
DNS

Hop count
\* 15 ⓘ

H.323

Mode
Off ⓘ

SIP

Mode
On ⓘ

TLS verify mode
Off ⓘ

Fallback transport protocol
TLS ⓘ

Media encryption mode
Force encrypted ⓘ

ICE support
Off ⓘ

Preloaded SIP routes support
Off ⓘ

Modify DNS request
Off ⓘ

AES GCM support
Off ⓘ

Authentication

SIP authentication trust mode
Off ⓘ

Advanced

Include address record
Off ⓘ

Zone profile
Custom ⓘ

Automatically respond to SIP searches
Off ⓘ

Send empty INVITE for interworked calls
Off ⓘ

SIP parameter preservation
Off ⓘ

SIP poison mode
Off ⓘ

SIP UDP/BFCP filter mode
Off ⓘ

SIP UDP/IX filter mode
Off ⓘ

SIP record route address type
IP ⓘ

Save
Cancel
Delete

Figure 29

For VCS-Expressway-E

Go to Configuration > Zones > Zones > Add New

Name: ZONE-BJN-PROD

• Type: DNS

• H.323 Mode: Off

- SIP Mode: On
- Fallback transport protocol: TLS
- Media encryption mode: Force encrypted

#### Advanced Section:

- Zone profile: custom
- Send empty INVITE for interworked calls: off
- SIP UDP/BFCP filter mode: OFF

**Cisco Expressway-E**

Status System **Configuration** Applications Users Maintenance

**Edit search rule**

Configuration

Rule name: SR-ZONE-BJN-PROD

Description:

Priority: 40

Protocol: SIP

SIP variant: All SIP Variants

Source: Any

Request must be authenticated: No

Mode: Alias pattern match

Pattern type: Regex

Pattern string: .\*@bjn.vc

Pattern behavior: Leave

On successful match: Stop

Target: ZONE-BJN-PROD

State: Enabled

Save Delete Cancel

Figure 30

Search rules define how the VCS routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule.

Go to Configuration > Dial Plan > Search Rules > Add New

Rule name: SR-ZONE-BJN-PROD

- Priority: 40



- Protocol: SIP
- Source: ANY
- Request Must Be Authenticated: No
- Mode: Alias pattern match
- Pattern type: Regex
- Pattern string: .\*@bjn.vc
- Pattern behavior: Leave
- On successful match: Stop
- Target: ZONE-BJN-PROD (points to previously created zone)
- \* State: Enabled

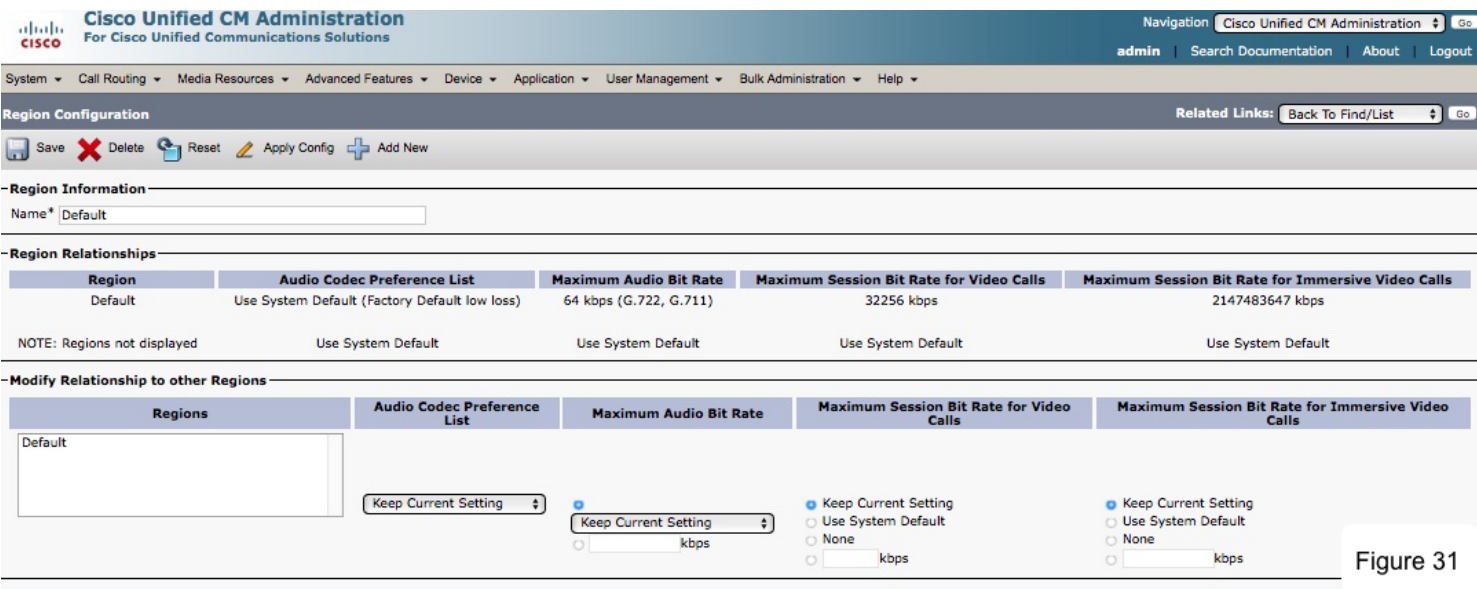


Figure 31

**Step 8 - Bandwidth Controls**

Configure your minimum desired bandwidth in Cisco Unified Communications Manager (CUCM), and in Cisco VCS Expressway.

To increase default bandwidth available for video calls on CUCM (see screenshot above):  
System > Region Information > Region

Select 'Default'

Increase 'Maximum Session Bit Rate for Video Calls' to at least 1.5 Mbps.

- In Unified Communications Manager, set the region to permit the minimum desired bandwidth, to ensure optimum SIP audio and video connectivity between and BlueJeans.
- In Cisco VCS Expressway set zones and pipes appropriately (according to your network’s requirements) to allow the minimum desired bandwidth.

We recommend at least 1.5 Mbps per call for an optimal experience. Some video devices can take advantage of higher rates, and the service can accommodate lower rates, depending on the device.

Status System **Configuration** Applications Users Maintenance

**Edit transform** You are here: [Configuration](#)

**Configuration**

Priority  ⓘ

Description  ⓘ

Pattern type  ⓘ

Pattern string  ⓘ

Pattern behavior  ⓘ

Replace string  ⓘ

State  ⓘ

Figure 32

### Step 9 - Simplify the Video Dial String - Transforms

Transforms modify the destination alias of all call attempts made to destination aliases which do not contain an '@'. This has the effect of standardizing all called destination aliases into a SIP URI format.

To join a scheduled BlueJeans meeting, users must dial the meeting id followed by the @ symbol and the BlueJeans domain -- for example, 123456789@bjn.vc.

You can simplify this string for SIP and H.323 video devices within your enterprise by using pattern replacement. In this example, you add a short prefix that replaces the need for users to include the domain when dialing. In the example deployment, where enterprise video devices are registered to Cisco Unified Communications Manager and the Cisco VCS Expressway Series is used for remote devices and firewall traversal, the simplified dial string is routed and converted into the full video dial string by a Unified Communications Manager route pattern and a Cisco Expressway transform.

Add a transform to convert the phone number into a Blue Jeans URI by going to VCS

Configuration > Dial Plan > Transforms & click on Add New.

Priority: 1 (can be a lower number depending on your configuration)

Description: Convert to BlueJeans URI

Pattern Type: Regex

Pattern String: `([^\@]*)` Example: `(4087407256)*` - this example shows BlueJeans dial-in number or can use any desired number

Pattern Behavior:

Replace String: `\1@bjn.vc`

State: Enabled

In this example, when a user dials 4087407256, the call is ultimately routed as `*@bjn.vc` where they will connect to BlueJeans IVR and then input the Meeting ID. However you can configure your system to dial a specific Meeting ID that would join the BlueJeans meeting directly bypassing the IVR using transform. Example is user dials 4087407256 and the call is routed as `<meeting ID>@bjn.vc` (basically the meeting of your choice).

This completes the one time configuration of having a video endpoint dial 4087407256 (example BlueJeans dial in number) and to join a meeting.

### Verify the Service and Test with BlueJeans

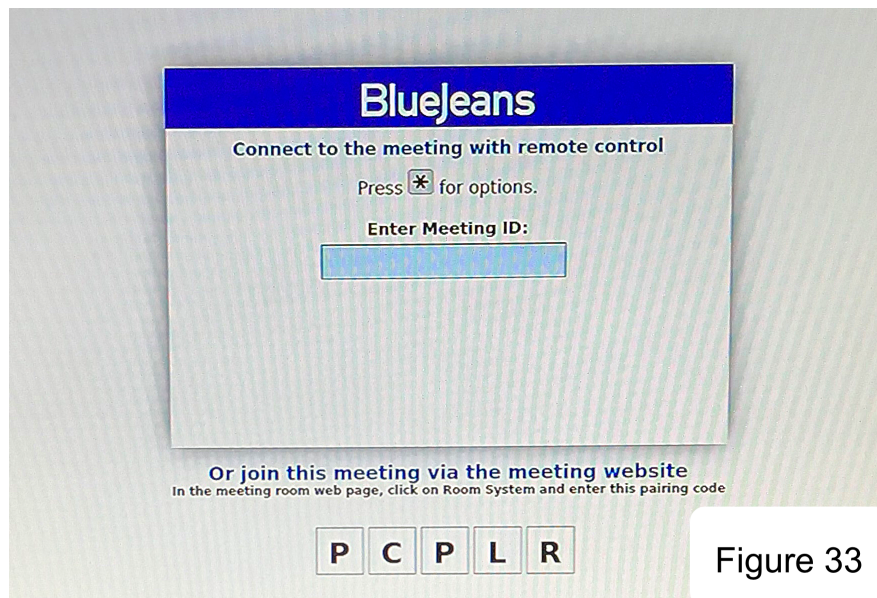


Figure 33

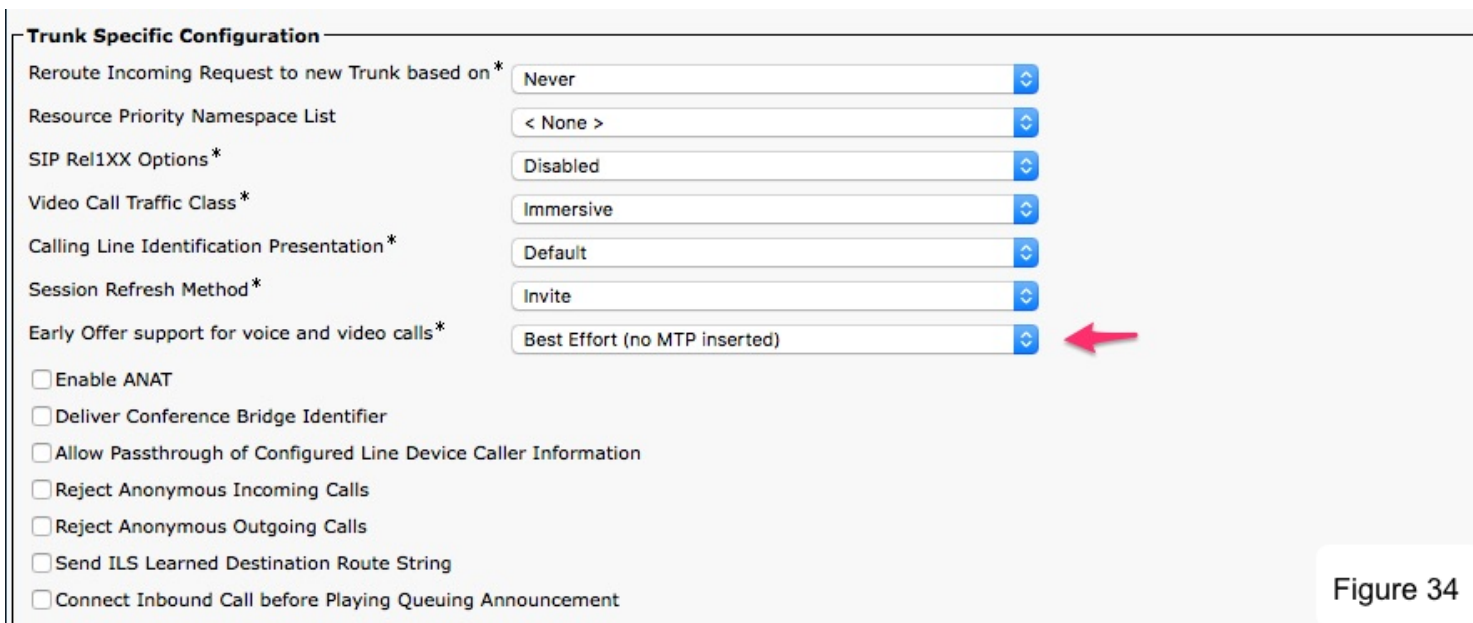
### Step 10 - Verify the Service and Test with BlueJeans

Login to BlueJeans and schedule / start a meeting – refer to “Scheduling a Meeting” for assistance OR if you received an invitation via email, click on the meeting link in the email.

To join the meeting dial the configured number. You should see the BlueJeans IVR Welcome Screen come up and can enter meeting ID and passcode (if there is one) at IVR Screen. You should then be connected to the meeting.

Important to test content sharing and other functions. Also make sure that calls stay connected after 15 minutes.

## Configure SIP For Early Offer



**Trunk Specific Configuration**

Reroute Incoming Request to new Trunk based on\* Never

Resource Priority Namespace List < None >

SIP Rel1XX Options\* Disabled

Video Call Traffic Class\* Immersive

Calling Line Identification Presentation\* Default

Session Refresh Method\* Invite

Early Offer support for voice and video calls\* Best Effort (no MTP inserted)

☐ Enable ANAT

☐ Deliver Conference Bridge Identifier

☐ Allow Passthrough of Configured Line Device Caller Information

☐ Reject Anonymous Incoming Calls

☐ Reject Anonymous Outgoing Calls

☐ Send ILS Learned Destination Route String

☐ Connect Inbound Call before Playing Queuing Announcement

Figure 34

When using Early Offer the SDP is sent along with the initial SIP invite (can easily be seen in logs). Delayed Offer sends SDP later. This is important for video conferencing, when SDP in the message body of an INVITE request. The headers of the INVITE describe the kind of session you want to establish and the SDP describes the media you are willing to send and receive. This is Early Offer and it allows for choosing the type of media and other attributes for the session. With Delayed Offer the SIP INVITE has no message body. Receiving endpoint is not aware of what codec or other parameters will be involved in the session. When the call is answered, a 200 Ok with SDP is sent and the caller responds back with an ACK. However, the ACK will now contain the SDP that would have been sent in the INVITE. With this change in SDP placement, the caller gets to decide which codec will be used for this session.

- Early Offer = SDP in INVITE
- Delayed Offer = SDP in ACK

It is recommended that Early Offer be used when dialing BlueJeans. Especially for unencrypted calls.

To configure SIP Trunks with Early Offer (EO):

By default, CUCM prefers to use Delayed Offer (DO) for outgoing SIP calls. It is possible, however, to force EO. Here is how:

Device > Device Settings > SIP Profile

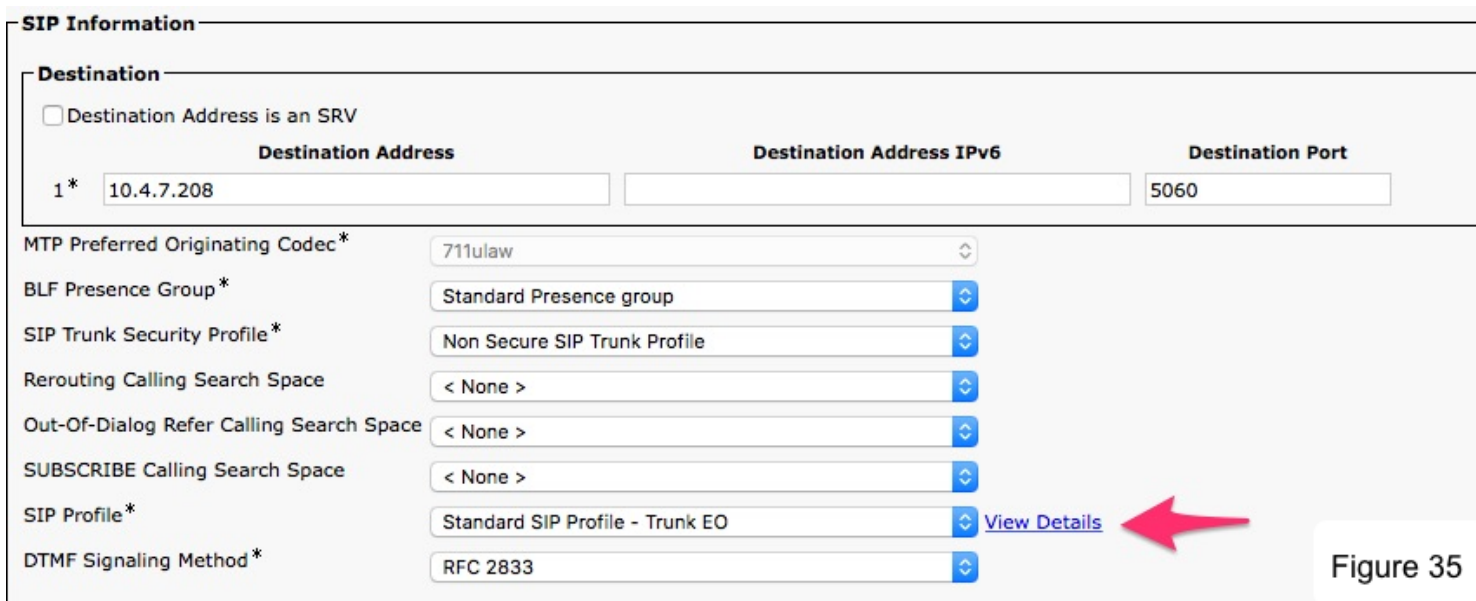
- Select Standard SIP Profile - press Copy (or create a new one).

Leave all parameters unchanged, except:

- Name: Standard SIP Profile - Trunk EO (or any name you like) - see above screenshot Figure 34

Make sure that the Trunk Specific Configuration is set:

- Early Offer support for voice and video calls: Best Effort (no MTP inserted) then Save



**SIP Information**

**Destination**

☐ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1 *	10.4.7.208		5060

MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* Non Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* Standard SIP Profile - Trunk EO [View Details](#)

DTMF Signaling Method\* RFC 2833

Figure 35

After Standard SIP Profile - Trunk EO' is created, go to the SIP trunks configuration Device > Trunk and modify:

- SIP Profile: Standard SIP Profile - Trunk EO (or whatever you named it) - see above screenshot Figure 35

Also on the VCS-E DNS Zone > Advance (see Figure 29)

- Send empty INVITE for interworked calls: Off

**Note: We recommend that Early Offer is always used on CUCM and/or VCS SIP trunks to BlueJeans SIP servers. Early Offer (versus Delayed Offer sometimes selected by default on CUCM and/or VCS) helps to avoid various compatibility issues such as failure to join a meeting, calls being dropped after 15 minutes, asymmetric codecs being negotiated, etc.**



## Troubleshooting



To help with troubleshooting, VCS-Expressway provides a Call History which allows you to view details when a call cannot get setup by going to Status > Calls > History and searching for the call in question. You can then click on View under Actions to get more details on the call itself.

Check Call signaling:

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

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

### Calls Dropping in Exactly 15 Minutes

Issue: Call to BlueJeans connects fine, but drops at 15 minutes each time.

If you see that calls are dropping at exactly 15 minutes this could be caused by the Cisco Unified Call Manager (CUCM) when it does a session refresh (every 15 minutes) and sends an new invite that has capability mismatch. We have seen this when:

- 1) CUCM sends INVITE without SDP (Delayed Offer being used).
- 2) ConnectSIP responds with 200 OK - RTP/SAVP (Strict SRTP)
- 3) CUCM responds with ACK - RTP/AVP (no crypto lines - RTP only)

There are two fixes to resolve this issue:

- 1) Enable Early Offer on the CUCM SIP Trunk configuration

- Endpoint's SIP profile set to EO (Early Offer), if needed
- Trunk set to EO and reset.
- If VCS is utilized, the neighbor zones set "Allow empty invite" to NO under the custom zone profile options.

\* Important to make sure that Early Offer is used for video calls. Early Offer means that the Cisco endpoint sends the SDP (Session Description Protocol) with the initial invite. The SDP is a set of rules that defines how the endpoints will participate in the session.

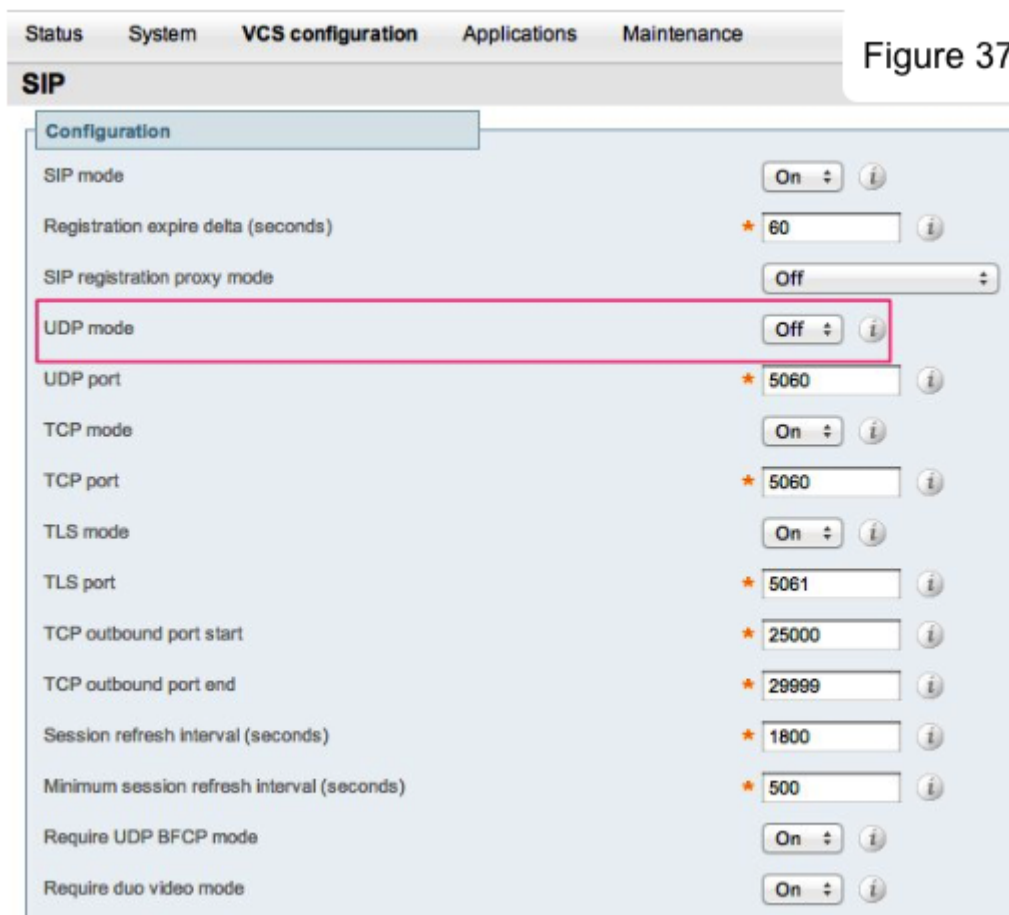
- 2) Enable secure calling (SRTP media encryption).

Early Offer configuration is minimal compared to CUCM security configuration. In this guide we show examples for setting up for encrypted calls which is recommended.

To configure SIP Trunks with Early Offer (EO) please see configuration above.

**Note: We recommend that Early Offer is always used on CUCM and/or VCS SIP trunks to BlueJeans SIP servers. Early Offer (versus Delayed Offer sometimes selected by default on CUCM and/or VCS) helps to avoid various compatibility issues such as failure to join a meeting, calls being dropped after 15 minutes, asymmetric codecs being negotiated, etc.**

### 30 Second Delay for the BlueJeans Welcome Screen



Issue: There is a delay in reaching the BlueJeans IVR Welcome Screen

If there is a 30 second delay in the BlueJeans Welcome Screen showing up, it may be because the VCS-Expressway has SIP UDP enabled. Most times SIP UDP is not required for SIP video endpoints and can be turned off by going to VCS Configuration > Protocols > SIP > Configuration and setting the SIP UDP Mode to OFF. If SIP UDP cannot be turned off for a reason, then at this time the delay will be present.



## No Content Receive - 'Unknown' Protocol Shown

The screenshot displays the configuration interface for SIP settings, organized into four main sections: H.323, SIP, Authentication, and Advanced. Each section contains a list of configuration items on the left and their corresponding settings on the right. The 'SIP UDP/BFCP filter mode' setting in the Advanced section is highlighted with a red arrow.

Section	Configuration Item	Value
H.323	Mode	Off
SIP	Mode	On
	TLS verify mode	Off
	Fallback transport protocol	TLS
	Media encryption mode	Force encrypted
	ICE support	Off
	Preloaded SIP routes support	Off
	Modify DNS request	Off
	AES GCM support	Off
Authentication	SIP authentication trust mode	Off
Advanced	Include address record	Off
	Zone profile	Custom
	Automatically respond to SIP searches	Off
	Send empty INVITE for interworked calls	Off
	SIP parameter preservation	Off
	SIP poison mode	Off
	SIP UDP/BFCP filter mode	Off
	SIP UDP/IX filter mode	Off
	SIP record route address type	IP

At the bottom of the interface, there are three buttons: Save, Cancel, and Delete.

Issue: Content share cannot be seen or in some cases sent properly. Investigating the VCS can see RTP received, but protocol is shown as 'unknown.'

1) Make sure the configuration on the zone between the VCS Expressway-E (or VCS Expressway-C) and the CUCM called SIP UDP/BFCP filter mode which was set to OFF. Setting this to ON can cause the VCS Expressway to change the protocol used for presentation sharing which can change the negotiation between the endpoint and the external endpoint to be incorrect. When this setting is turned to OFF, the negotiation for Presentation Sharing can proceed unmodified and restored the ability to share in both directions. See above screenshot.

2) Make sure BFCP (or H.239 if using H.323) is properly configured. **See Step 6 - Enable BFCP above.**

## Cannot Dial IP Addresses When Registered to CUCM

Issue: Cannot dial an IP address to reach BlueJeans or another endpoint.

The information here is based on these software and hardware versions:

- Cisco VCS x8.1 and later
- CUCM Release 9 and later

Cisco Unified Call Manager (CUCM) does not support IP address dialing by default. Room Systems registered to CUCM cannot dial IP addresses to reach other endpoints. If you want to use IP address dialing, Cisco recommends one of the two options below. An example use case would be for endpoints registered to CUCM to dial an H.323 endpoint by IP address. In some cases, dialing IP addresses from some room systems registered to CUCM may end up dialing out H.323 direct and trying to transversing the firewall directly and the call may fail if not properly configured.

### Option 1

Add a suffix to the IP address, so that the string resembles a SIP Uniform Resource Identifier (URI). For example, in order to dial the IP address 198.51.100.2, users will dial 198.51.100.2@domain. Admin has to educate users to dial <IP address>@domain.

### Option 2

Replace the dots with a symbol in order to turn the IP address into a string. For example, in order to dial the IP address 198.51.100.2, users will dial 198\*51\*100\*2.

For complete configuration see Cisco Guide: Dial IP Addresses from Endpoints Registered to CUCM with VCS / Expressway Configuration Example or contact Cisco Support.

## Contacting BlueJeans Support

If you need additional assistance, please contact BlueJeans Support via [support@bluejeans.com](mailto:support@bluejeans.com) or via telephone:

US, Canada and accessible worldwide  
+1 (408) 791-2830

UK  
+44 (0) 800 014 8214

France  
+33 186265360

Australia  
+61 280363149 Option 2

Singapore

+65 31587560 Option 2

Please provide the Support Engineer with the following information regarding issues with your Cisco Infrastructure connecting to BlueJeans:

- 1) Description of issue (calls do not connect, calls drop after connecting, sharing not working, etc)
- 2) What topology are you using for your Cisco Infrastructure (call flow)
- 3) What video devices (Model and Firmware) are experiencing the issue