Cisco Integration Guide

Table of Contents

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 combonation 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 Infrastucture. 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 Admininstration 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

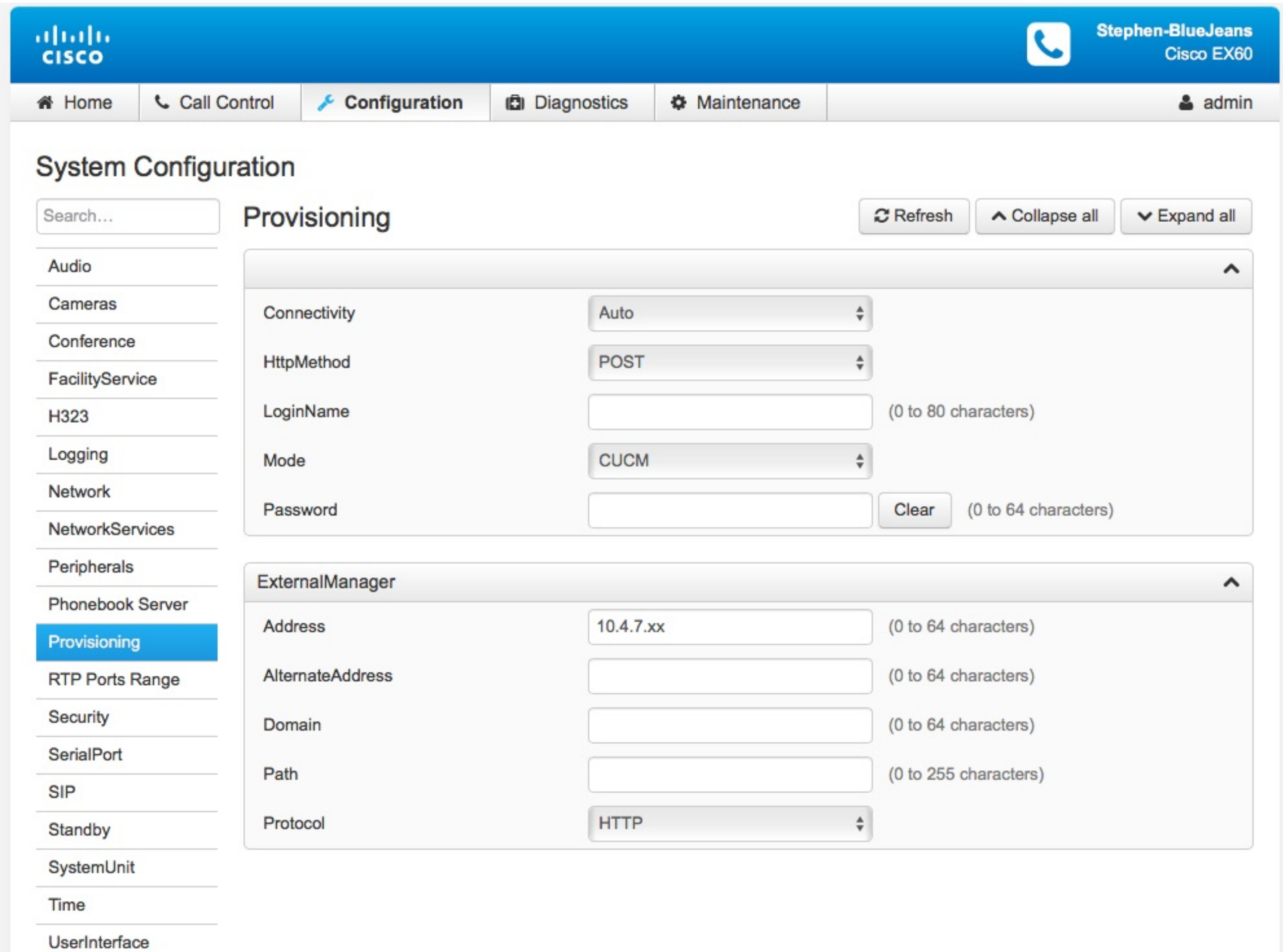


Figure 1

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 Extermal 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.

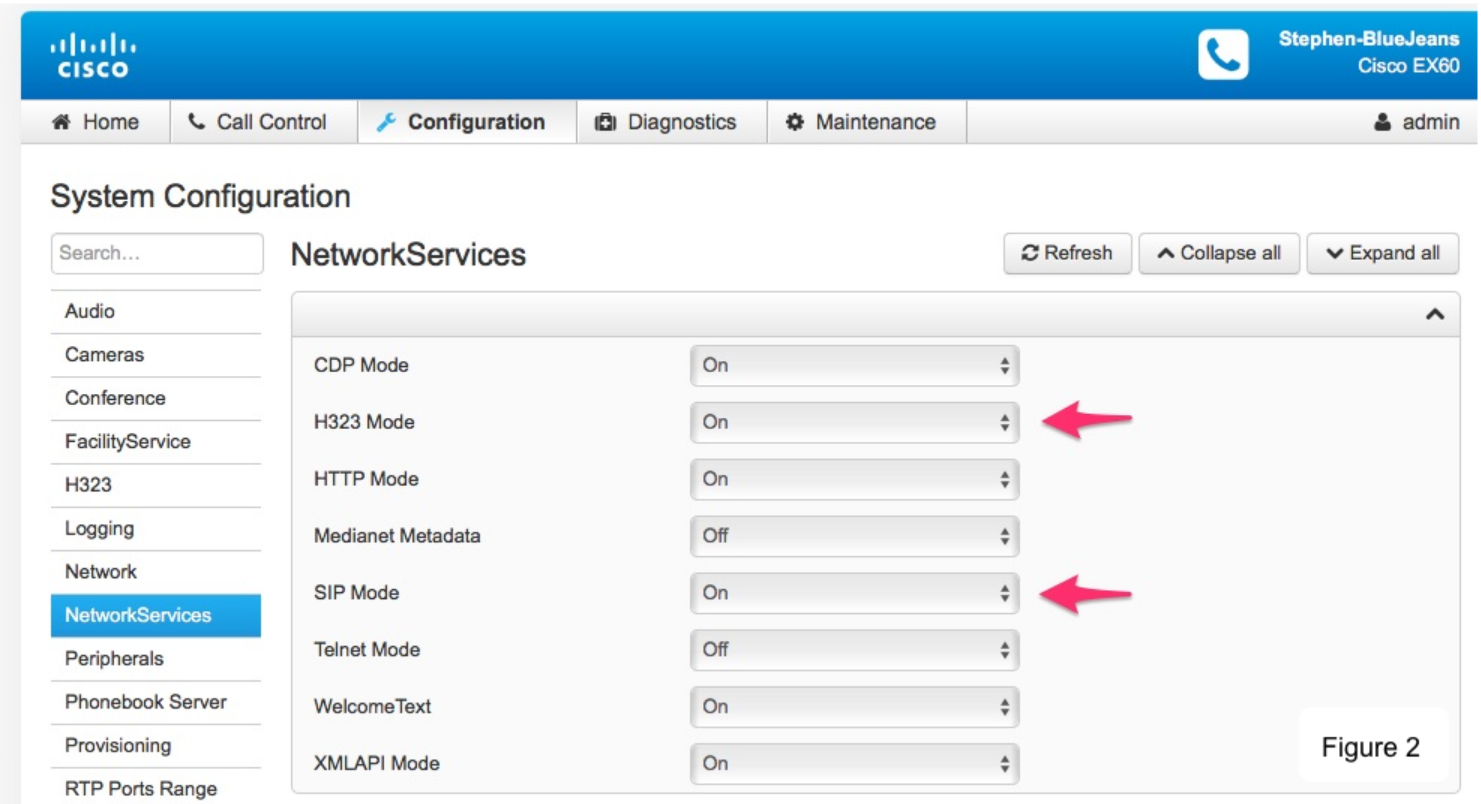


Figure 2

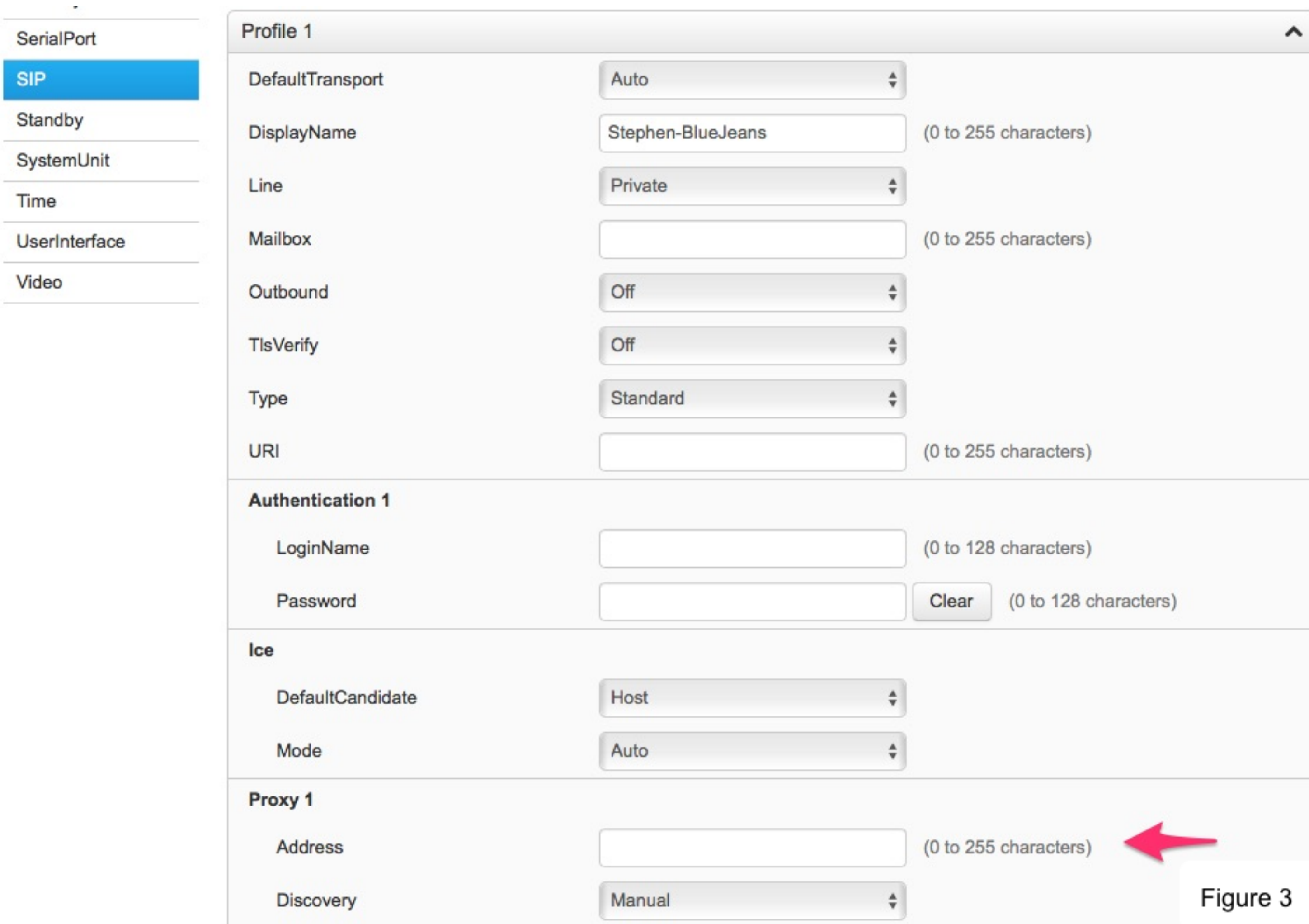

SerialPort
SIP
Standby
SystemUnit
Time
UserInterface
Video
Profile 1
DefaultTransport
Auto
DisplayName
Stephen-BlueJeans
(0 to 255 characters)
Line
Private
Mailbox
(0 to 255 characters)
Outbound
Off
TlsVerify
Off
Type
Standard
URI
(0 to 255 characters)
Authentication 1
LoginName
(0 to 128 characters)
Password
Clear
(0 to 128 characters)
Ice
DefaultCandidate
Host
Mode
Auto
Proxy 1
Address
(0 to 255 characters)
Discovery
Manual

Figure 3

Endpoint Configuration for Cisco VCS-C

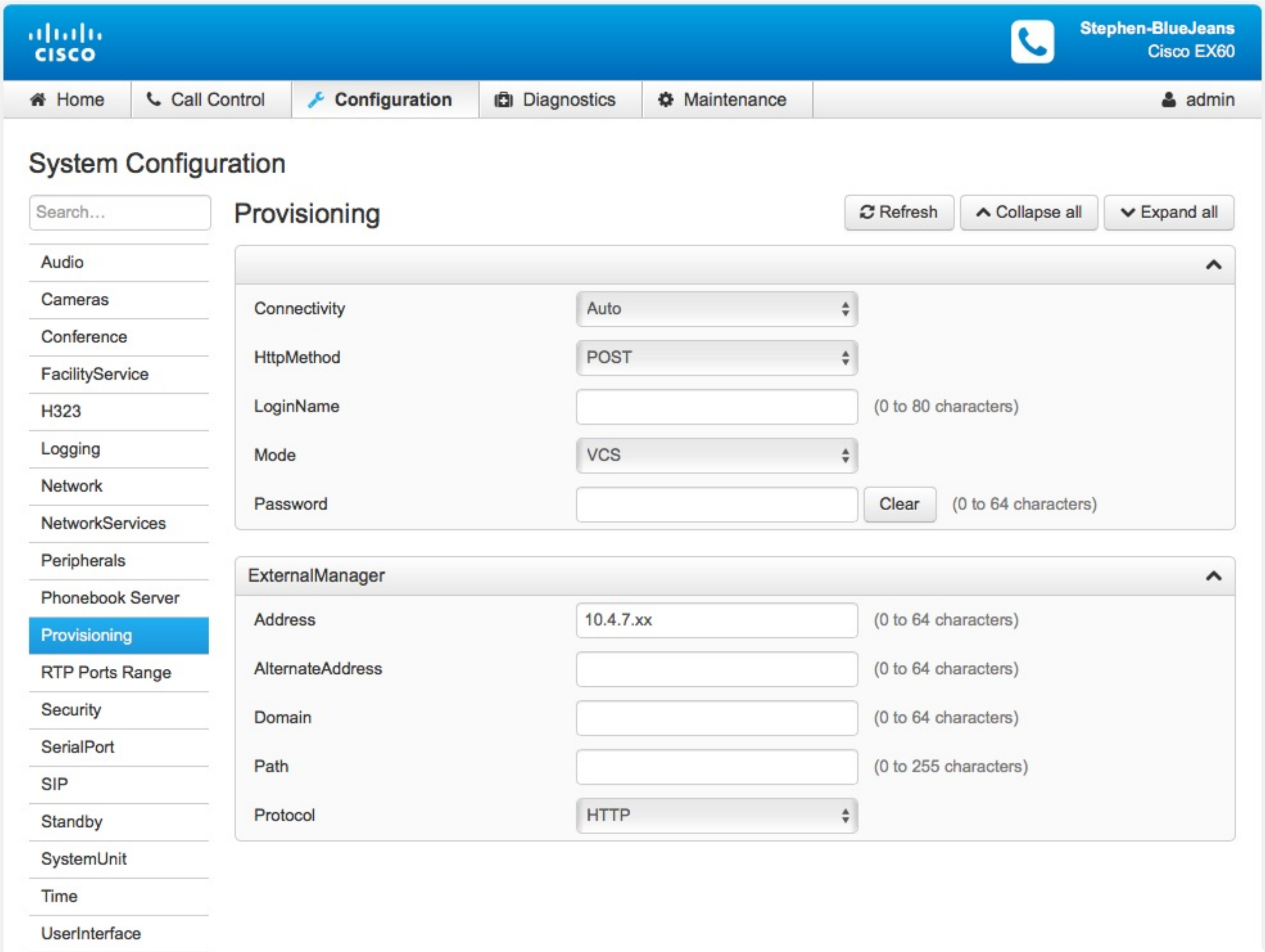


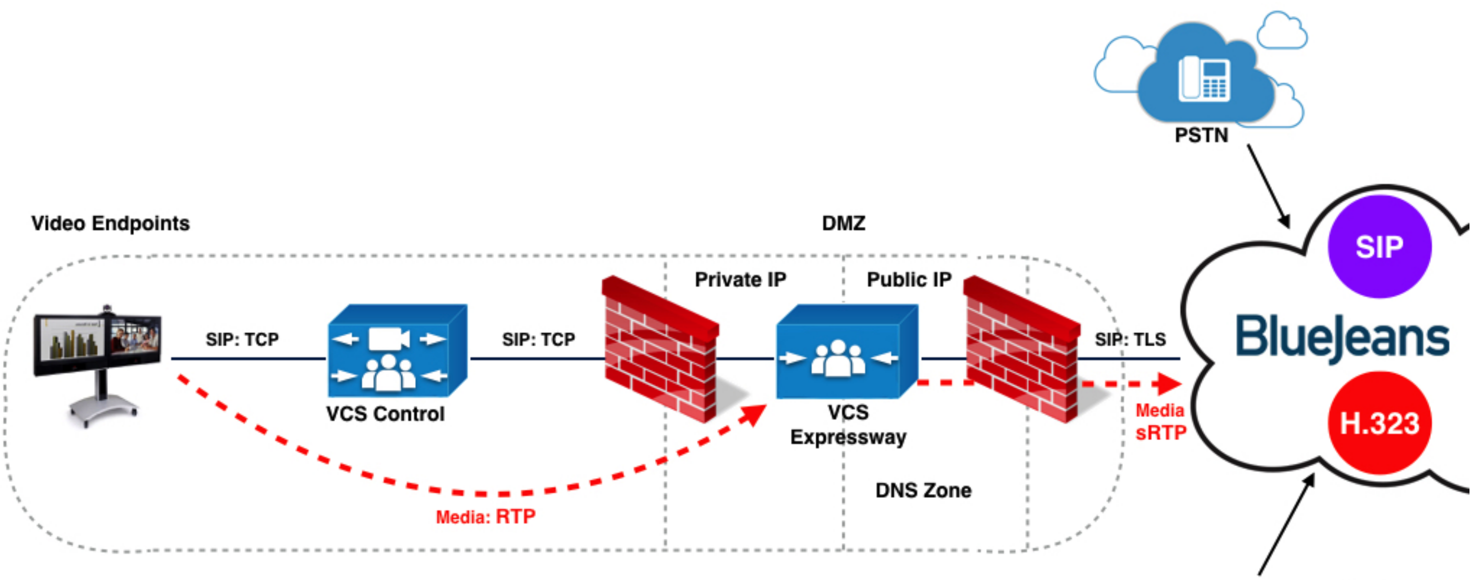
Figure 4

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 Extermal Manager input field. Click ok to save the changes.

Topology

Example: Cisco VCS-Expressway Connecting to BlueJeans



BlueJeans IP/Port Range

Ports	Type	Description
1720	TCP	H.323 Call Setup H.225
5060 / 5061	TCP	SIP Call Signalling and TLS
5000-5999	Dynamic TCP	H.323 Call Control H.245
5000-5999	Dynamic UDP	RTP Media

Network IP 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

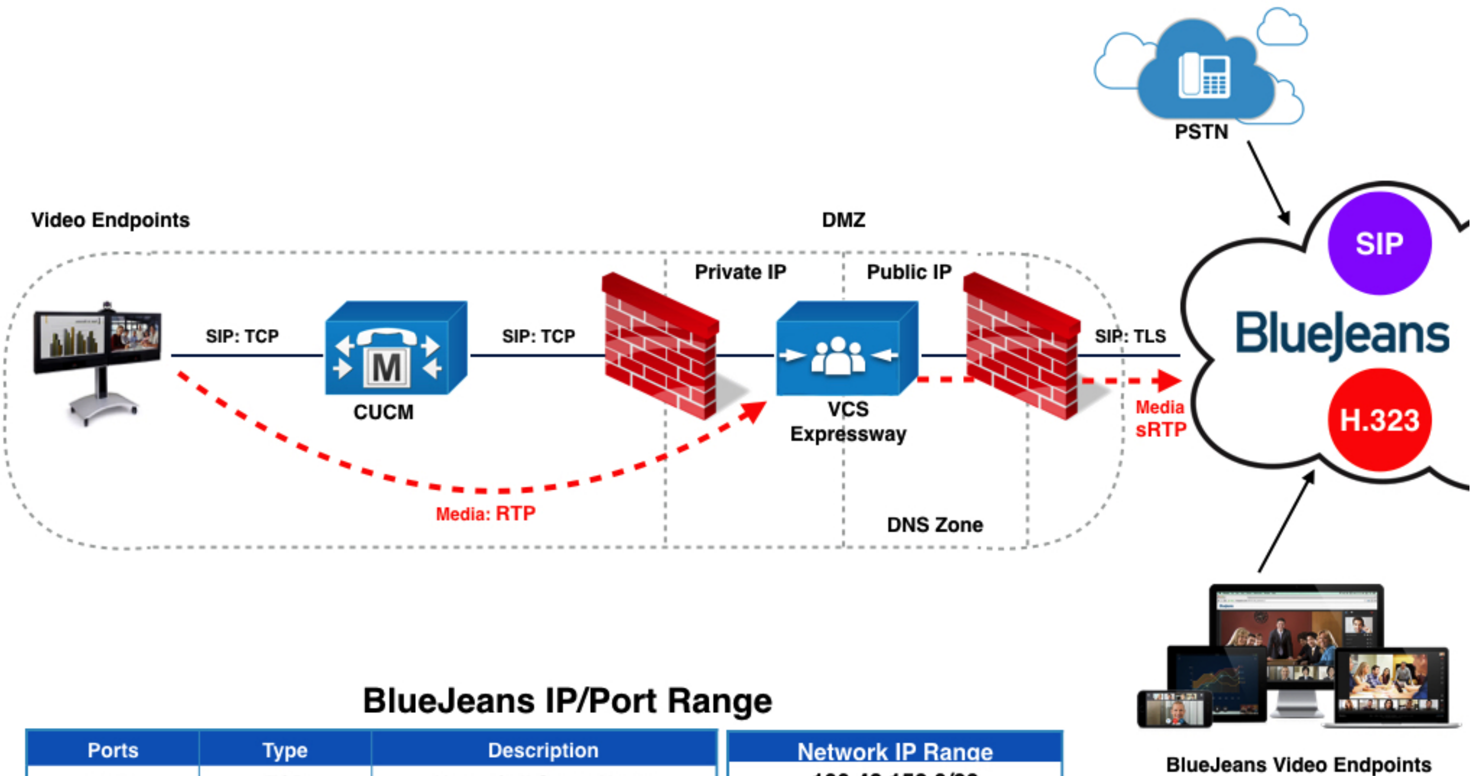
Figure 5

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



BlueJeans IP/Port Range

Ports	Type	Description
1720	TCP	H.323 Call Setup H.225
5060 / 5061	TCP	SIP Call Signalling and TLS
5000-5999	Dynamic TCP	H.323 Call Control H.245
5000-5999	Dynamic UDP	RTP Media

Network IP 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

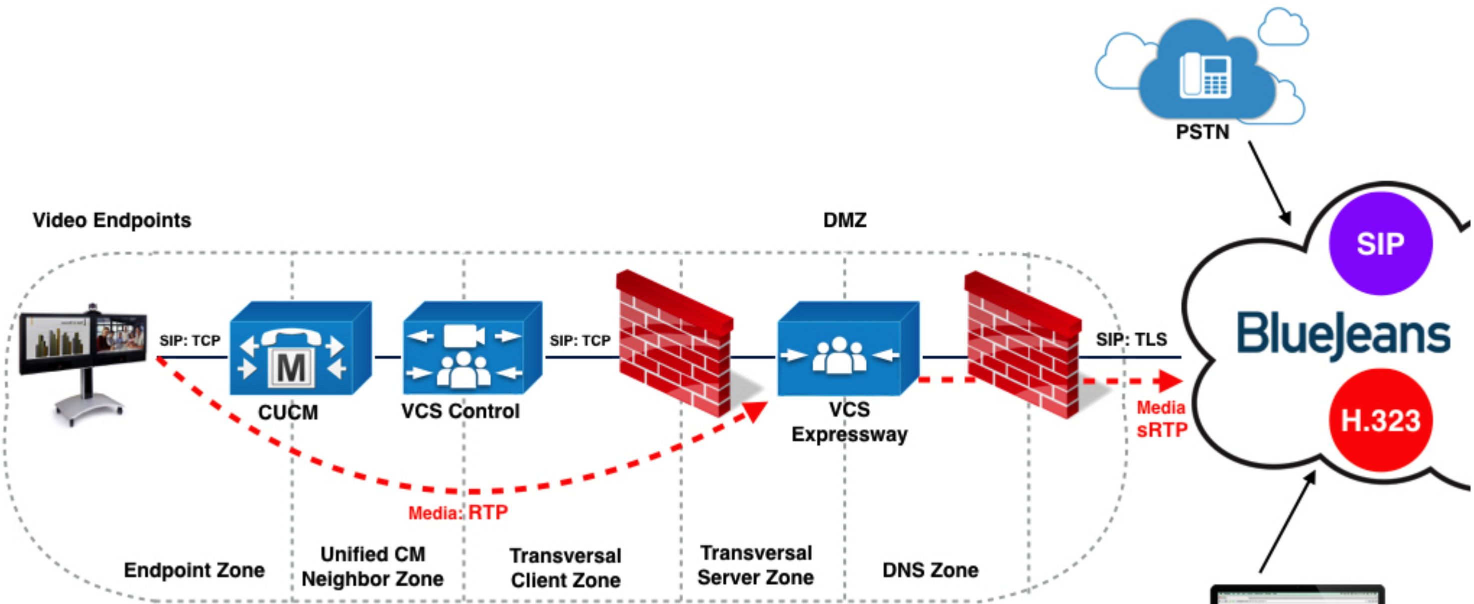
Figure 6

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
1720	TCP	H.323 Call Setup H.225
5060 / 5061	TCP	SIP Call Signalling and TLS
5000-5999	Dynamic TCP	H.323 Call Control H.245
5000-5999	Dynamic UDP	RTP Media

Network IP 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

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 is 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 encrytpion.

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

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.

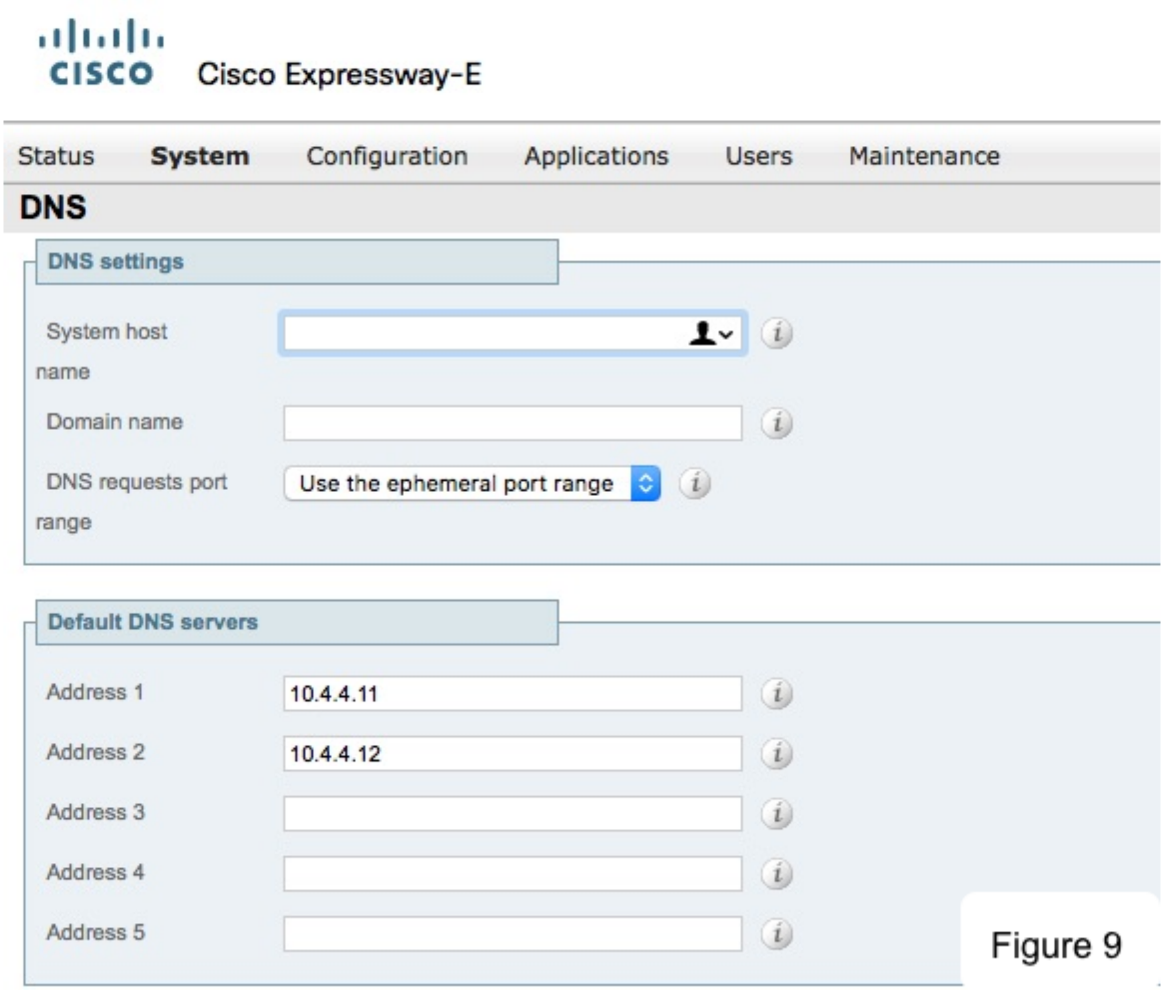


Figure 9

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

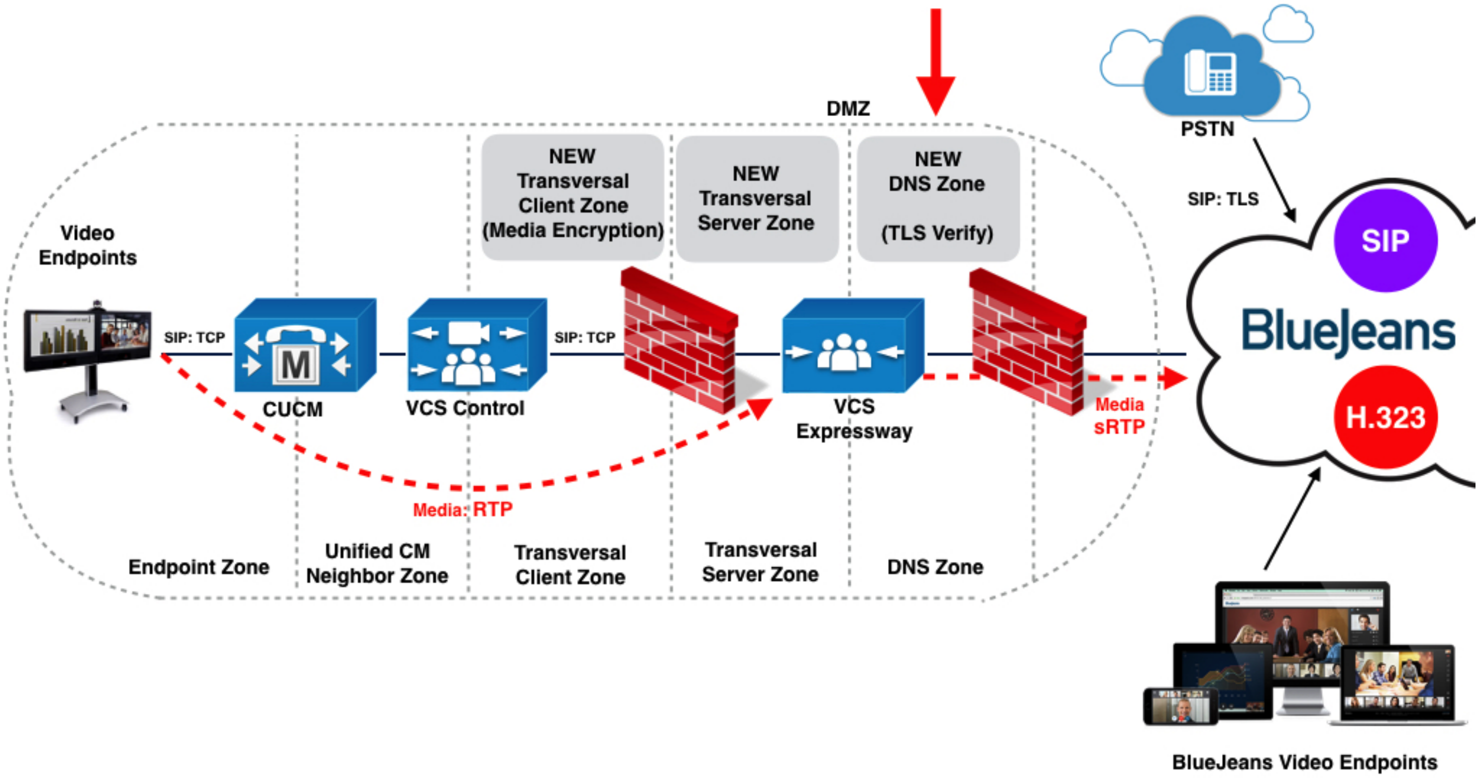


Figure 10

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

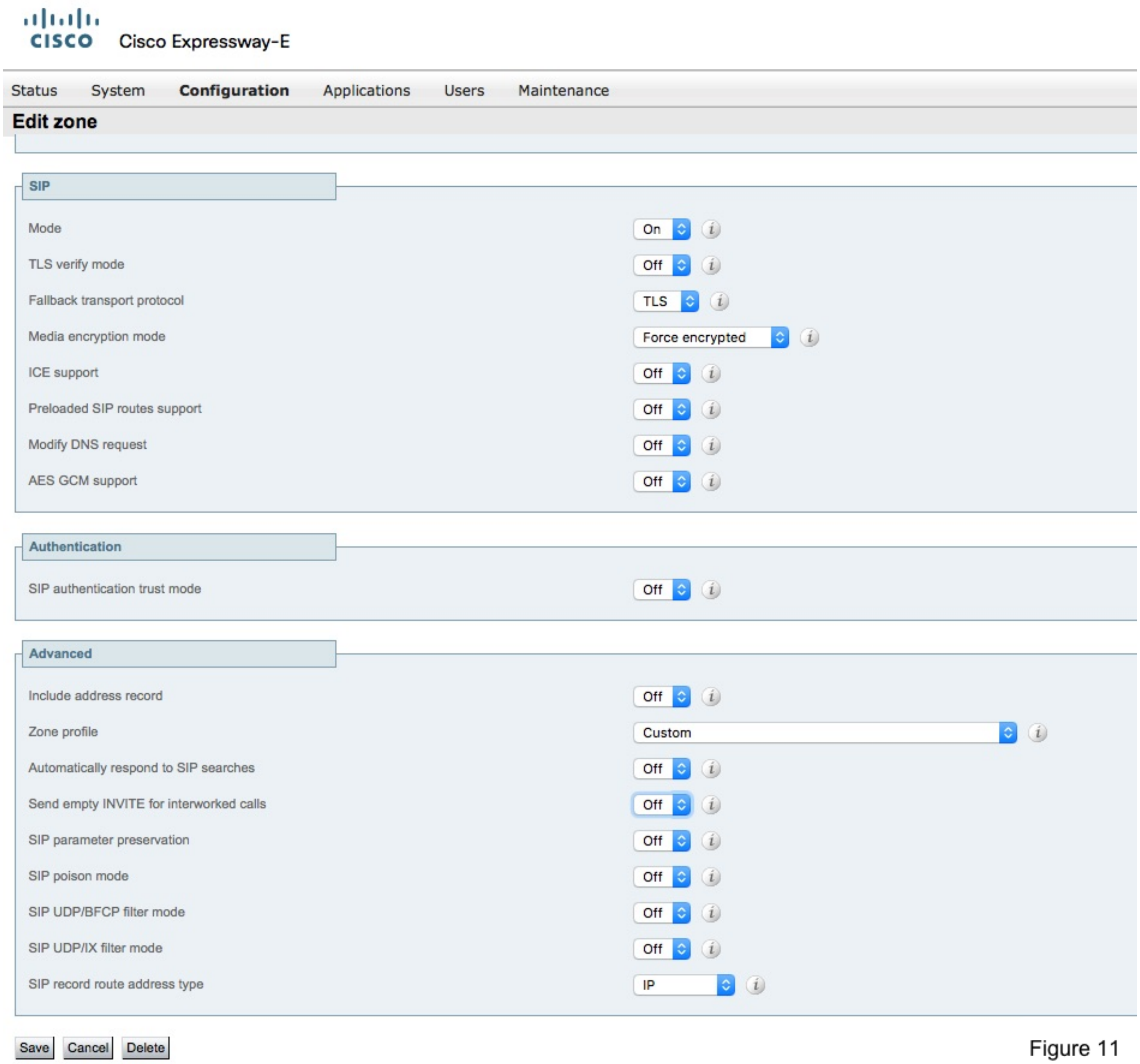


Figure 11

Create a New DNS zone (or use exosting 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 recommeded.

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. Recommeded setup for Early Offer is presented later in this guide.

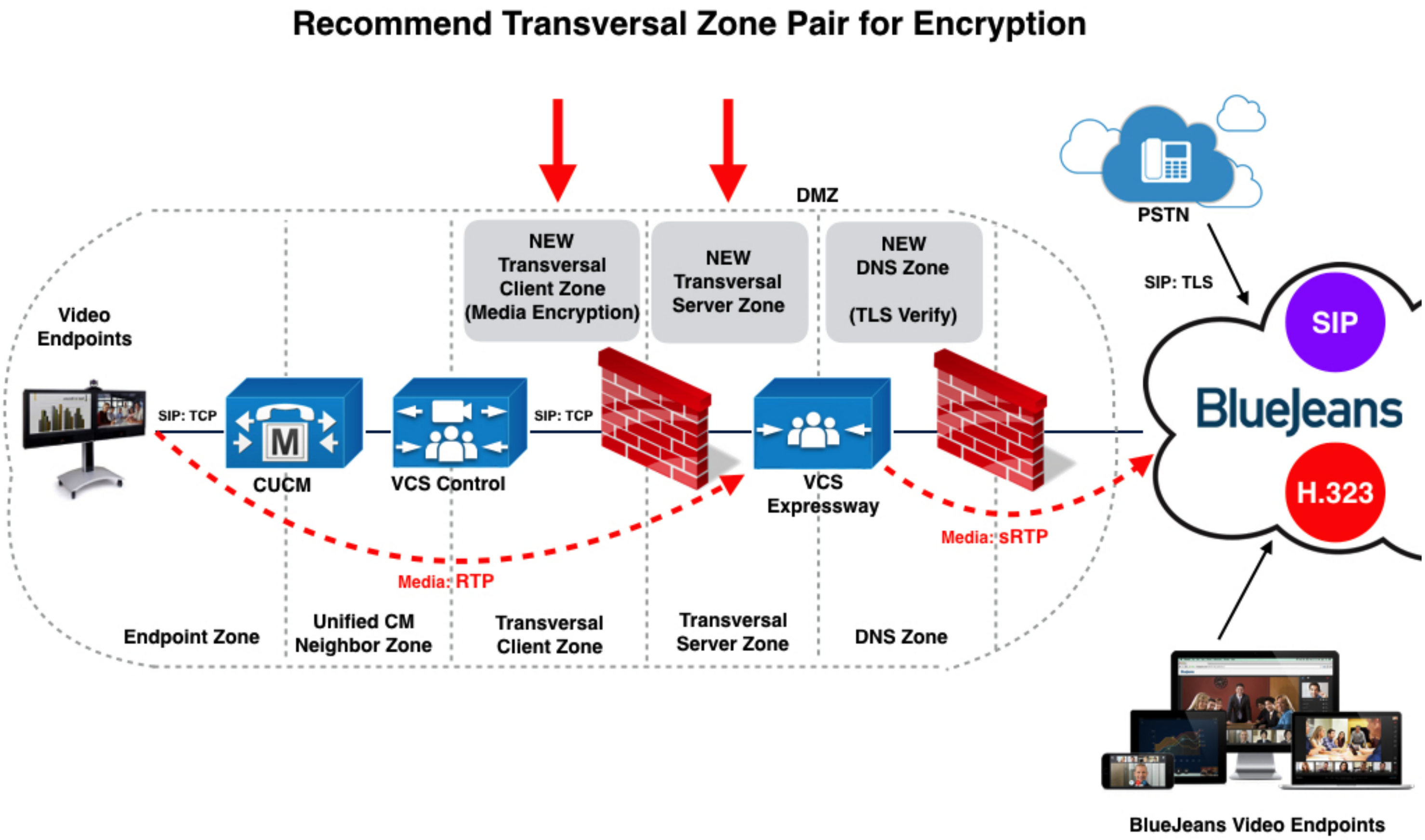


Figure 12

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:

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

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.

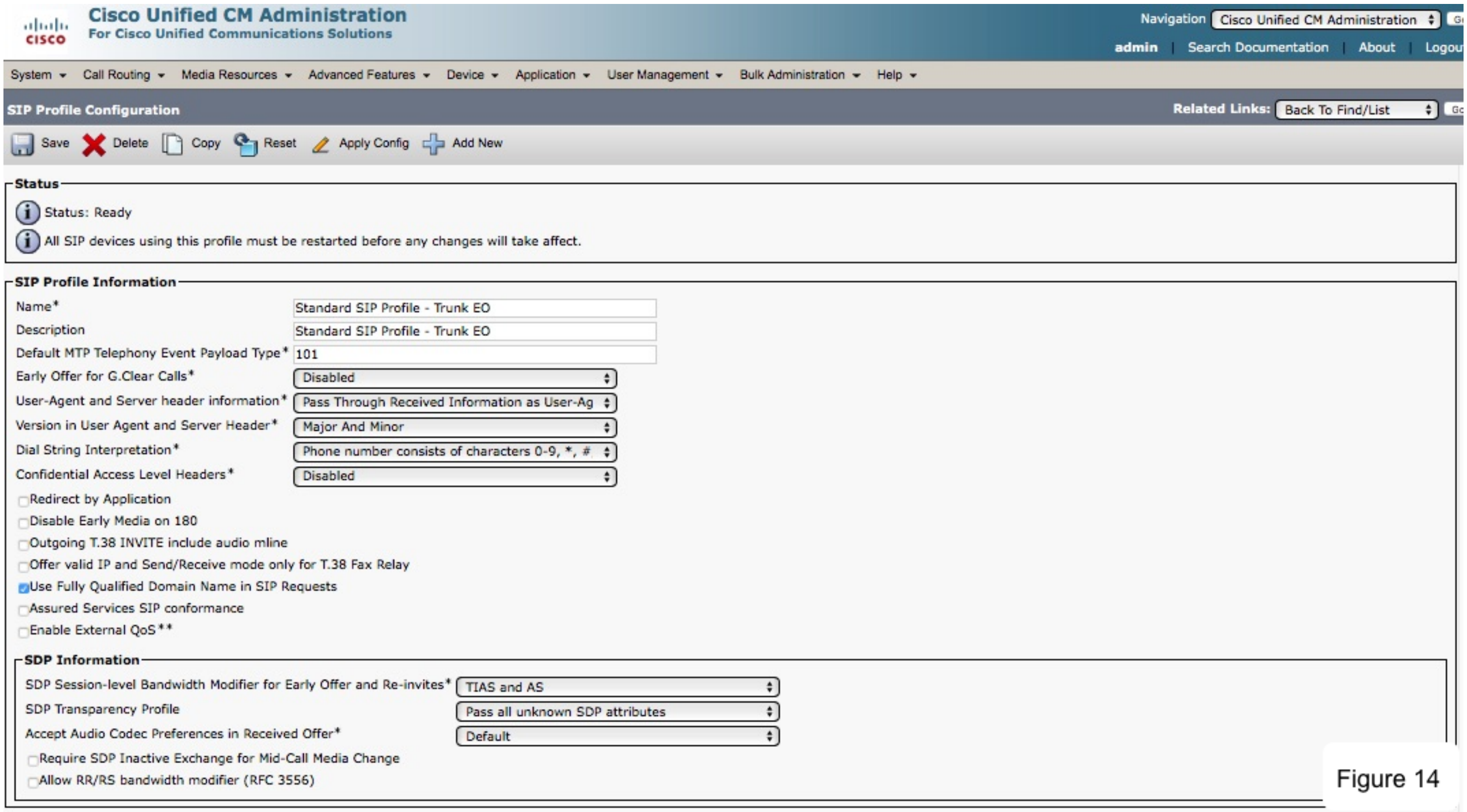


Figure 14

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.

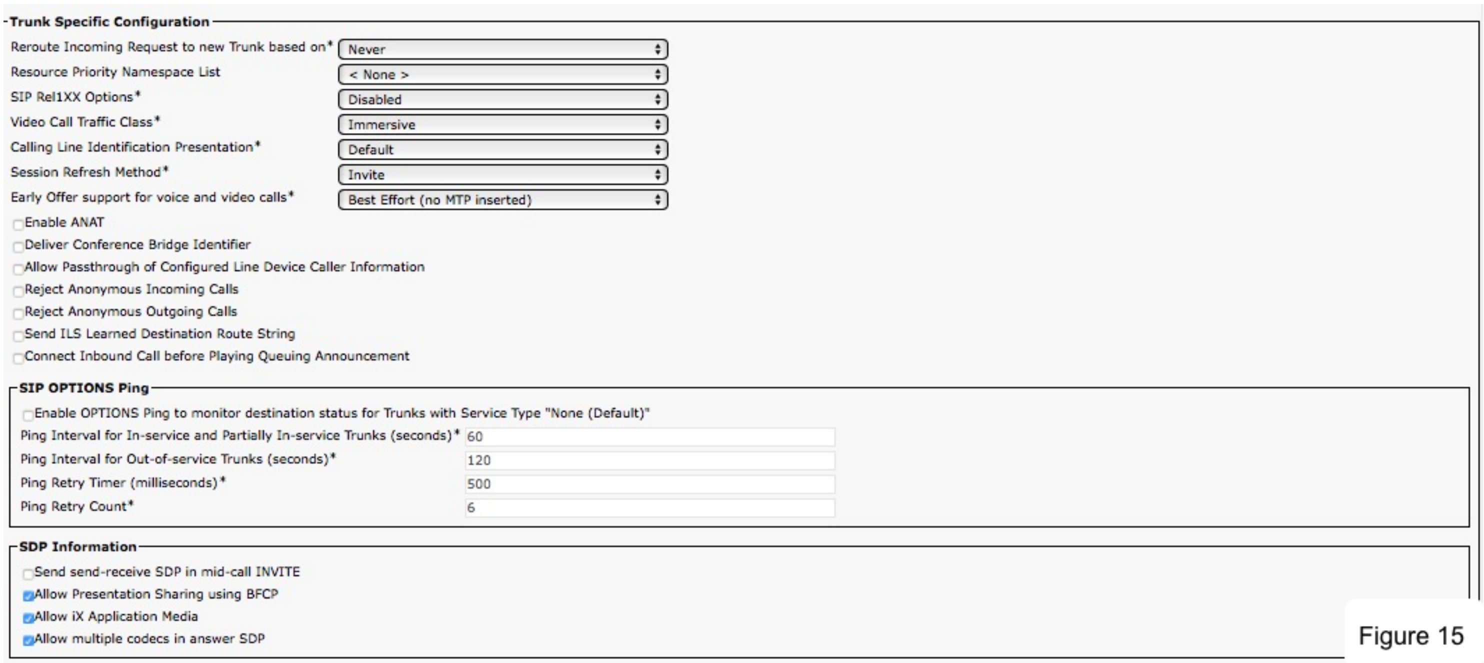


Figure 15

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

Figure 17

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)

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.

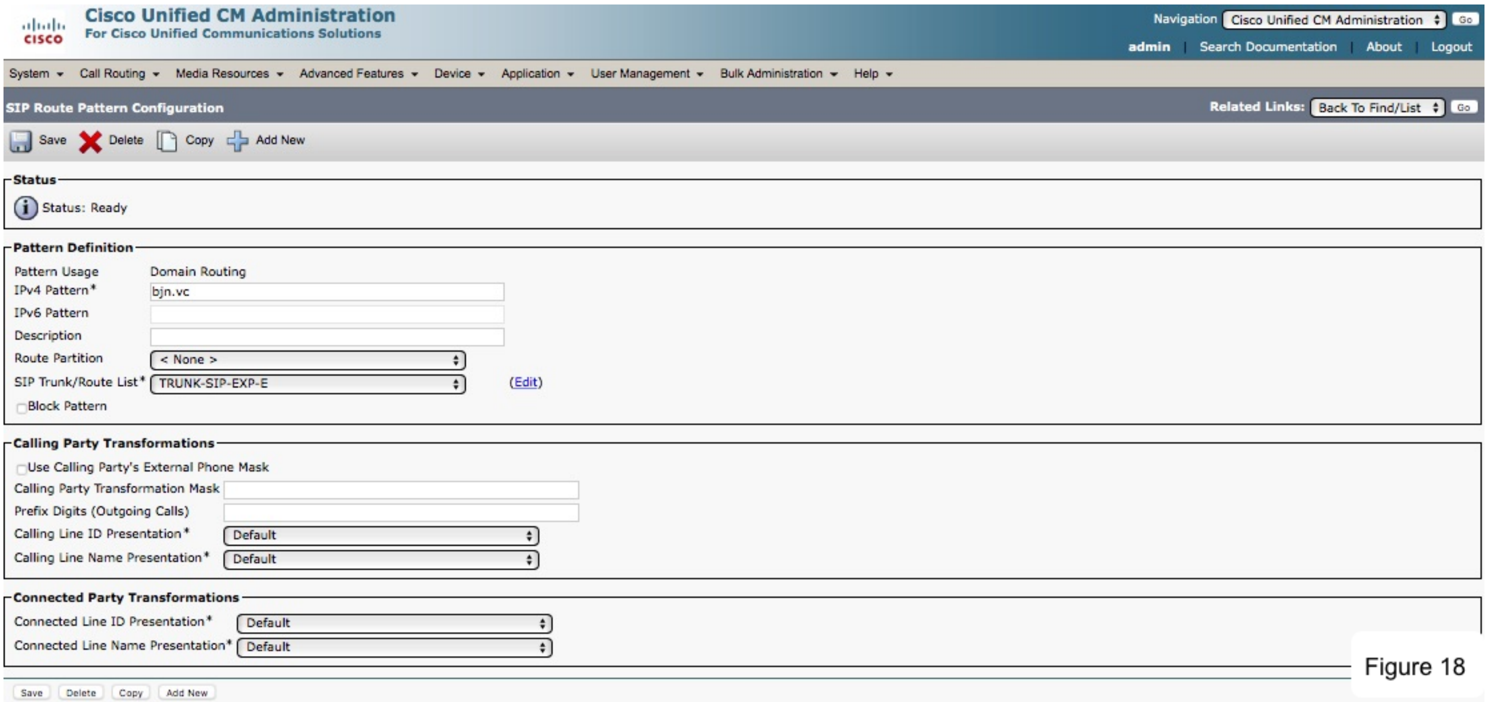


Figure 18

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)

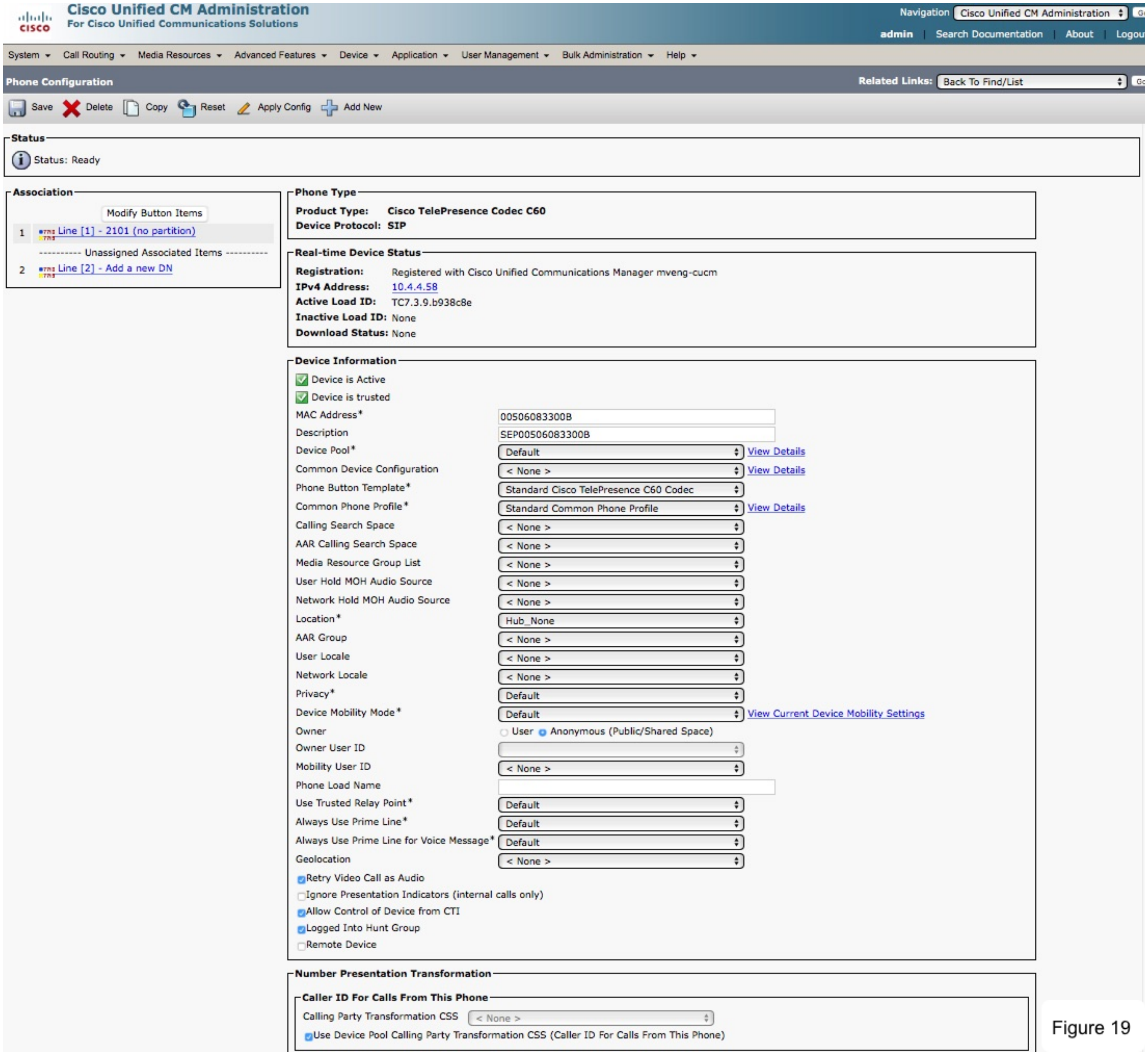


Figure 19

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.

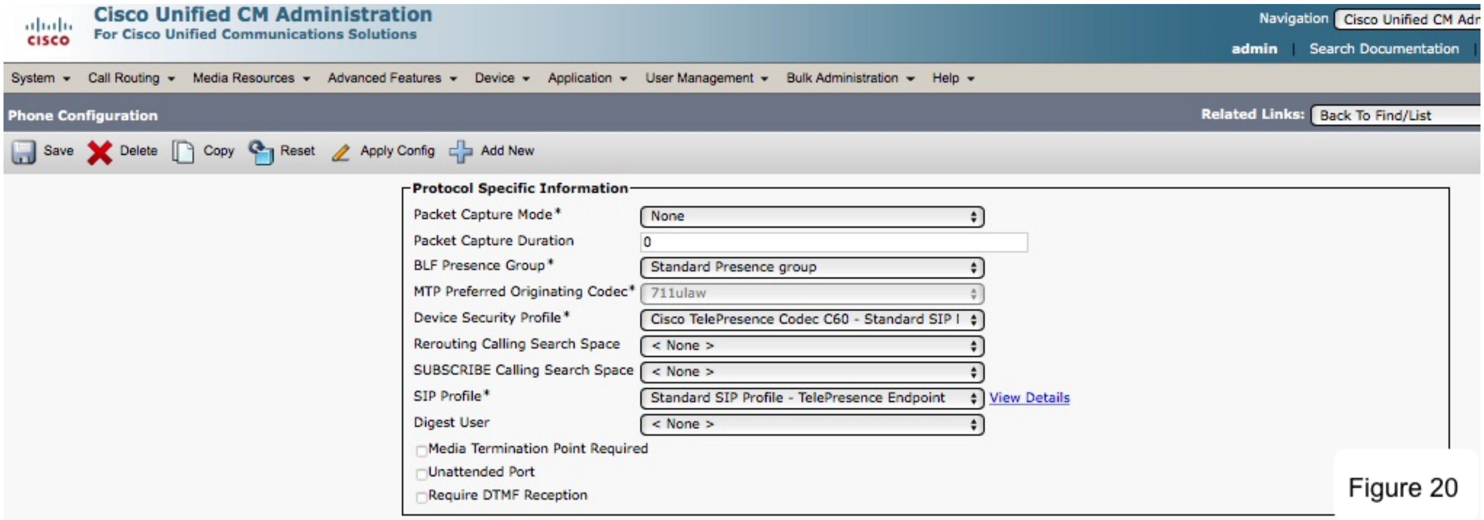


Figure 20

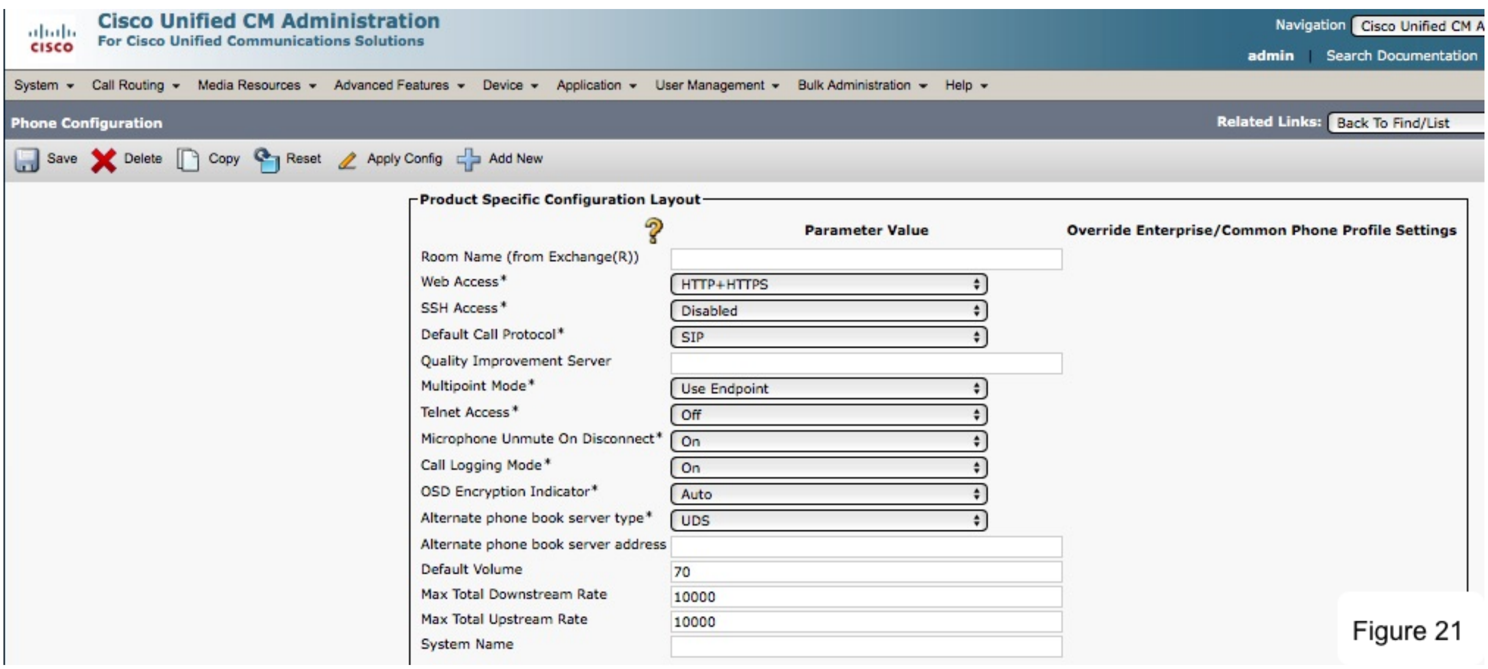


Figure 21

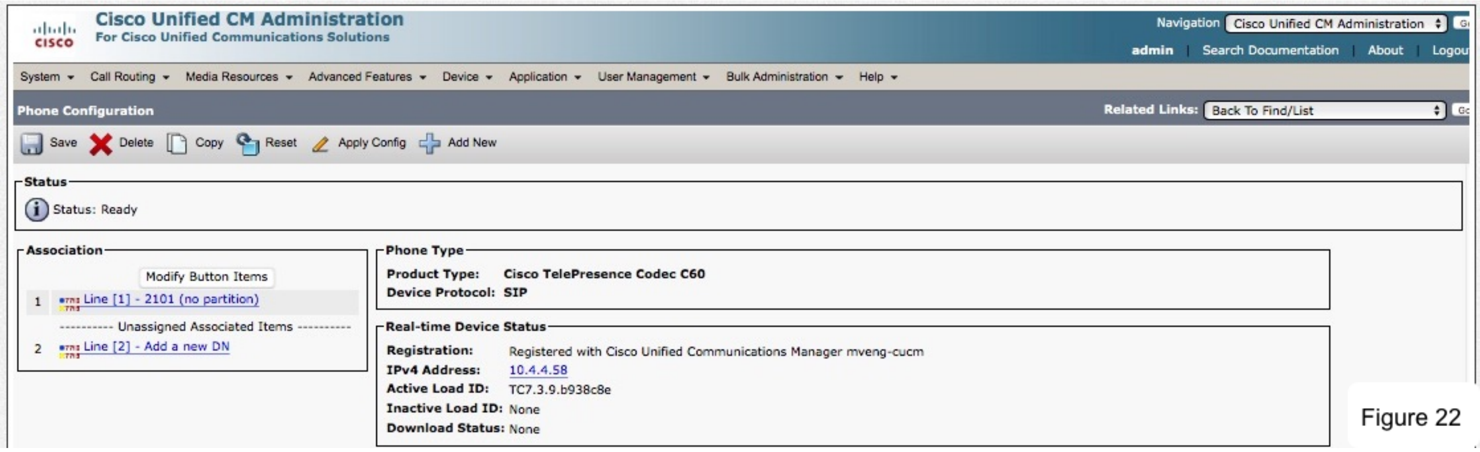


Figure 22

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

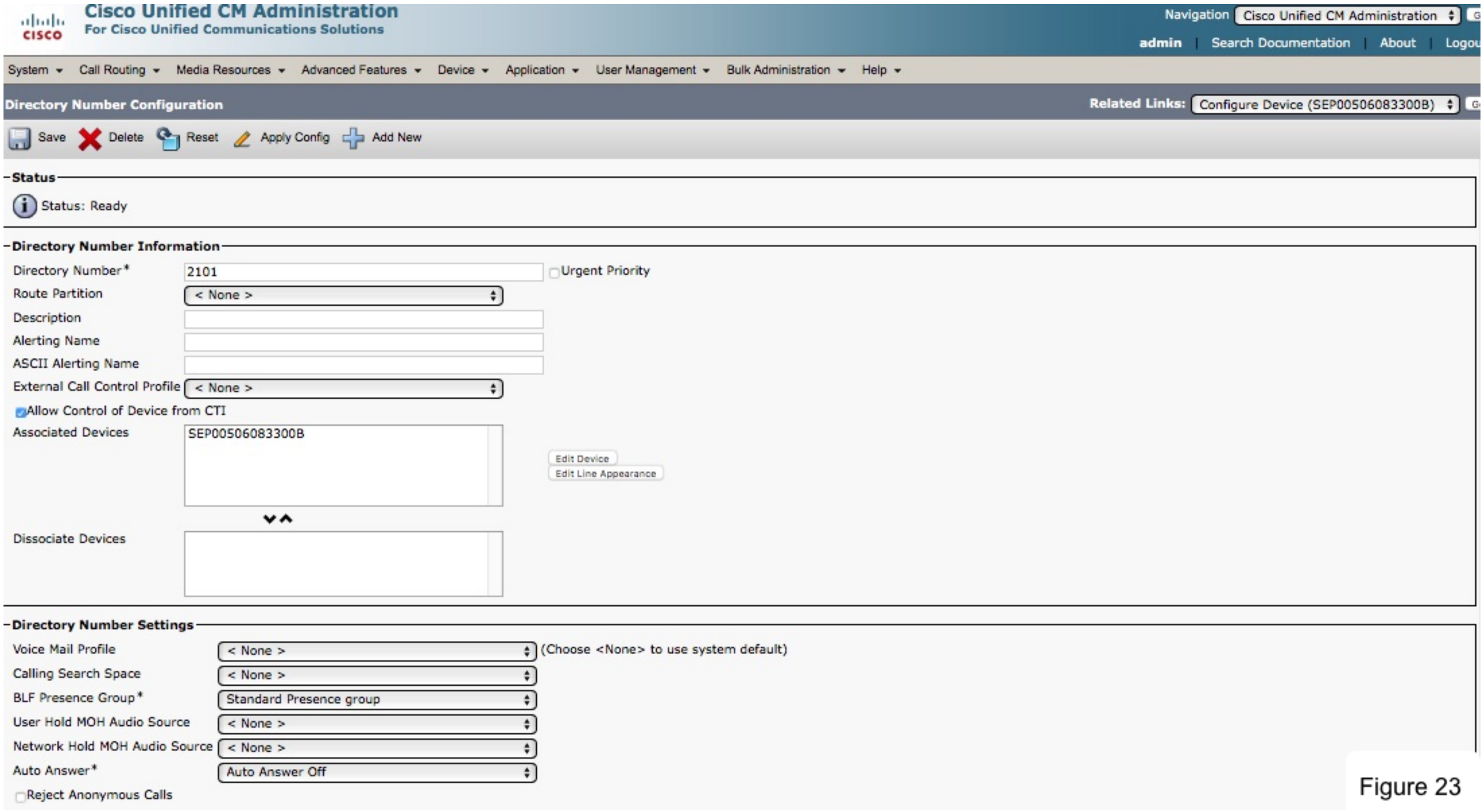


Figure 23

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.

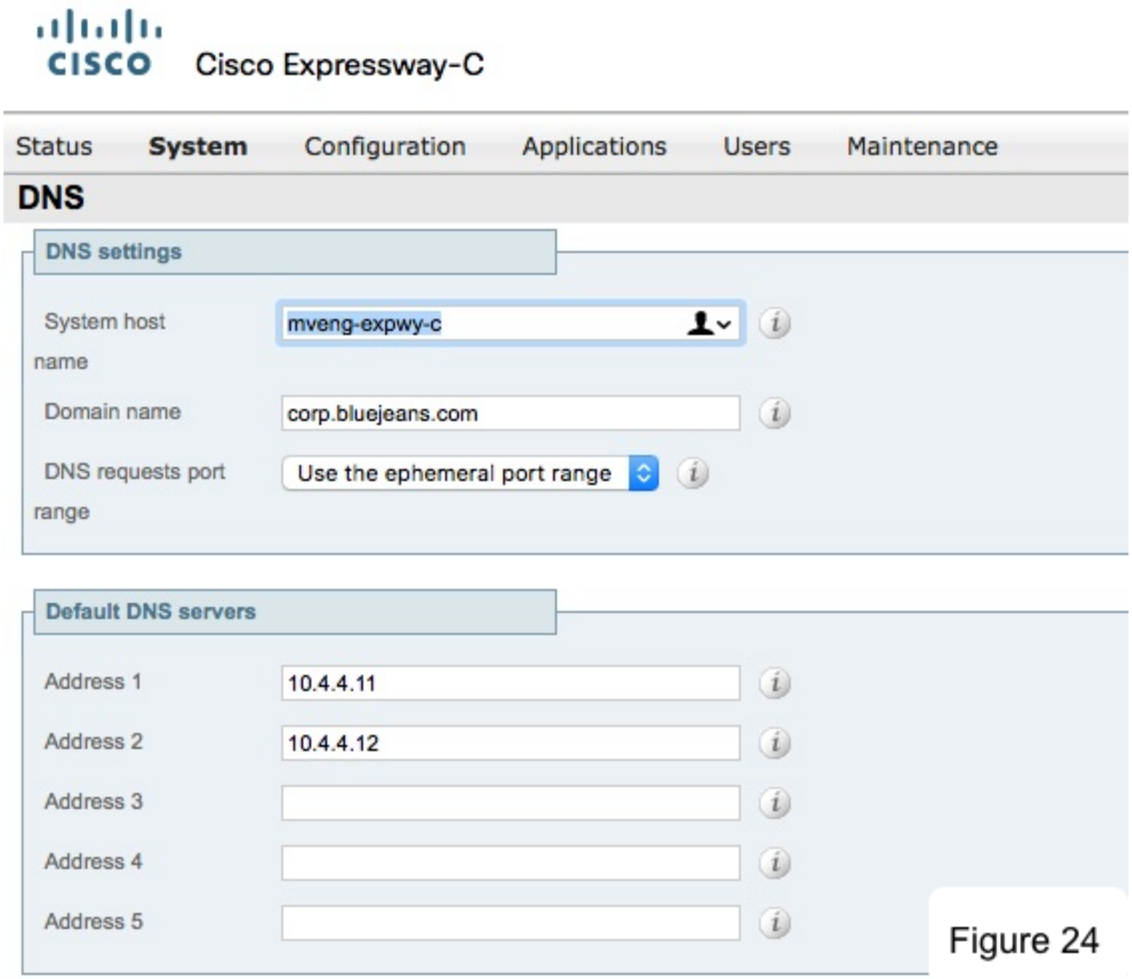


Figure 24

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)

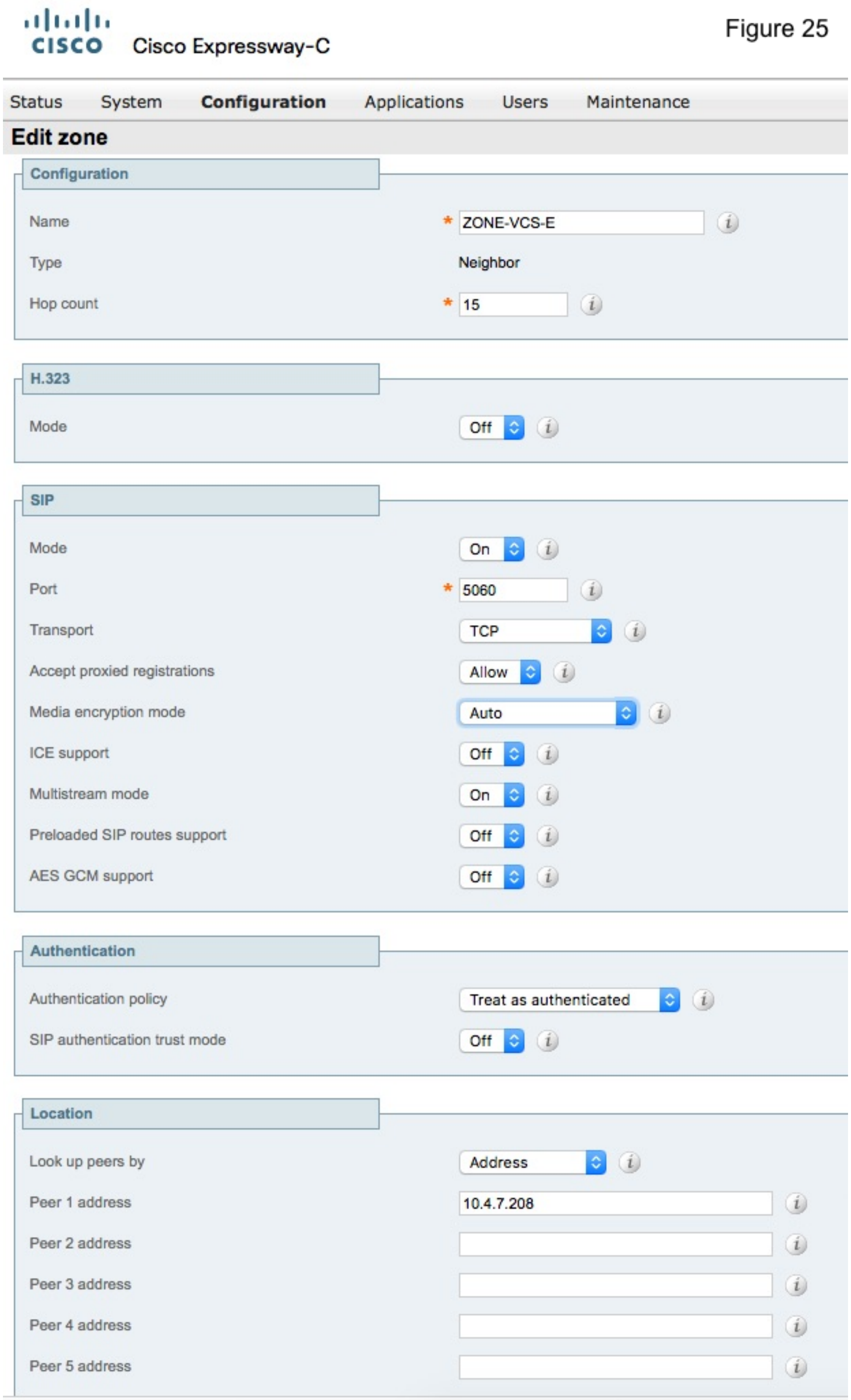


Figure 25

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

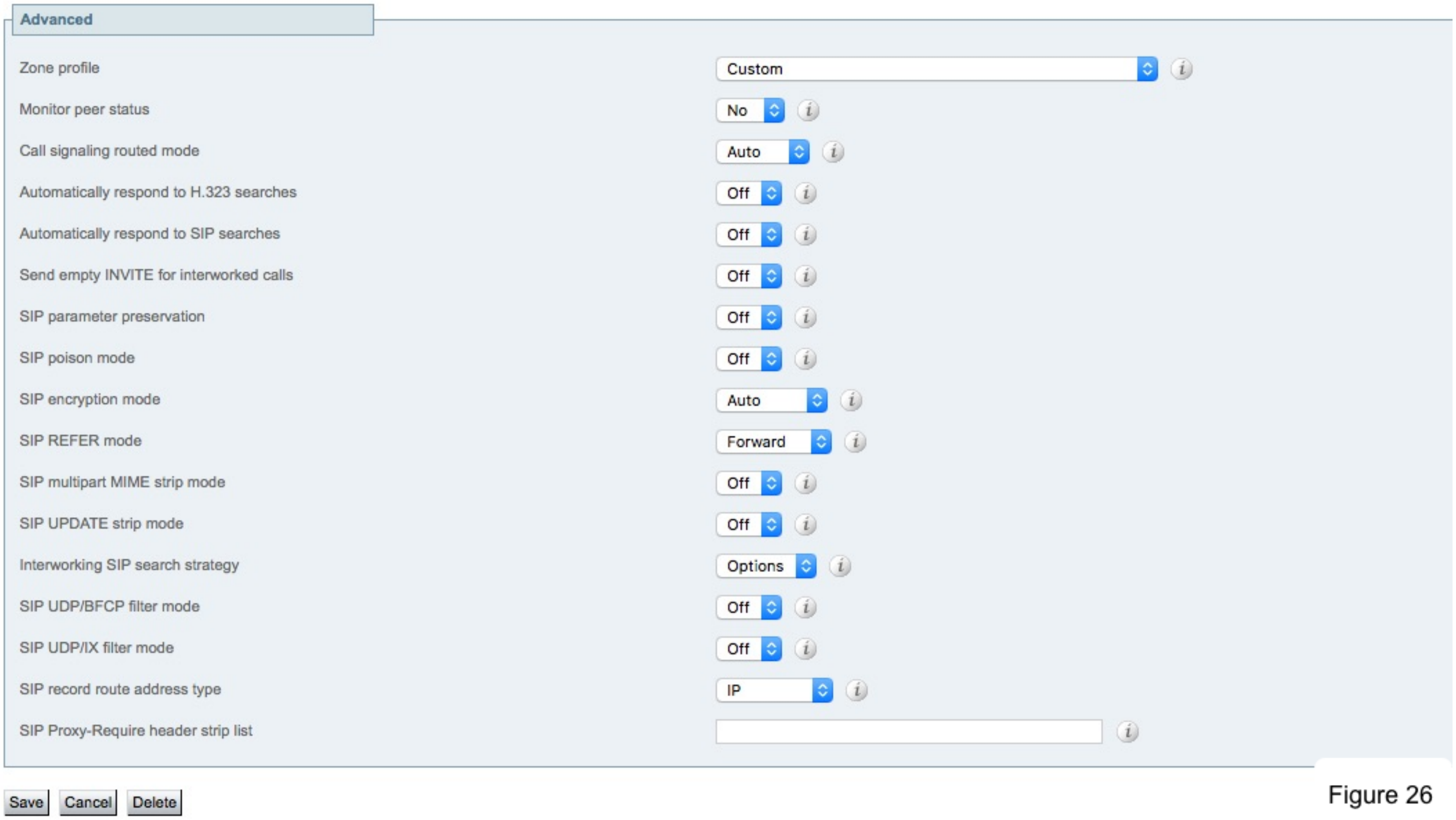

Advanced
Zone profile
Custom
Monitor peer status
No
Call signaling routed mode
Auto
Automatically respond to H.323 searches
Off
Automatically respond to SIP searches
Off
Send empty INVITE for interworked calls
Off
SIP parameter preservation
Off
SIP poison mode
Off
SIP encryption mode
Auto
SIP REFER mode
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

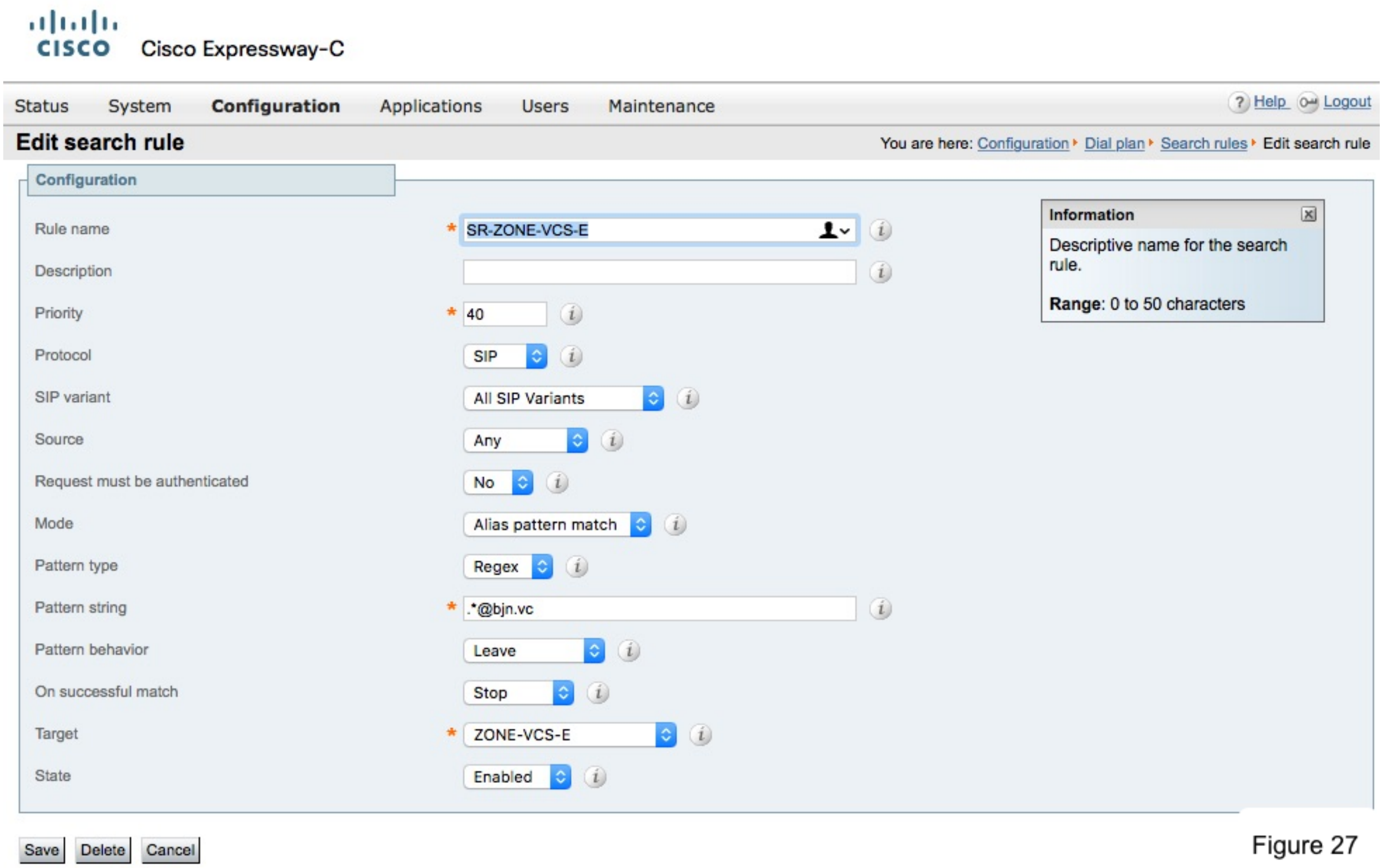


Figure 27

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

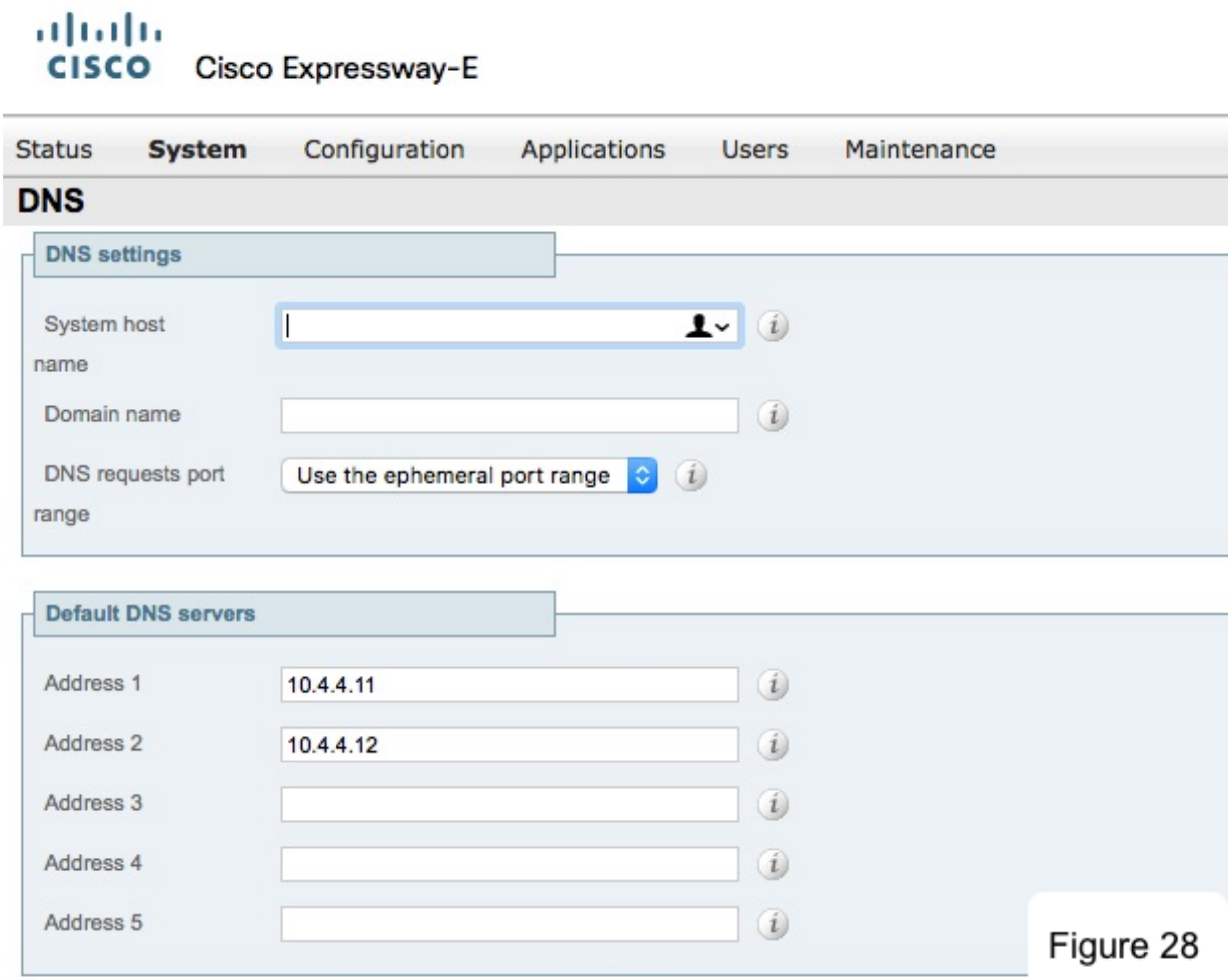


Figure 28

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

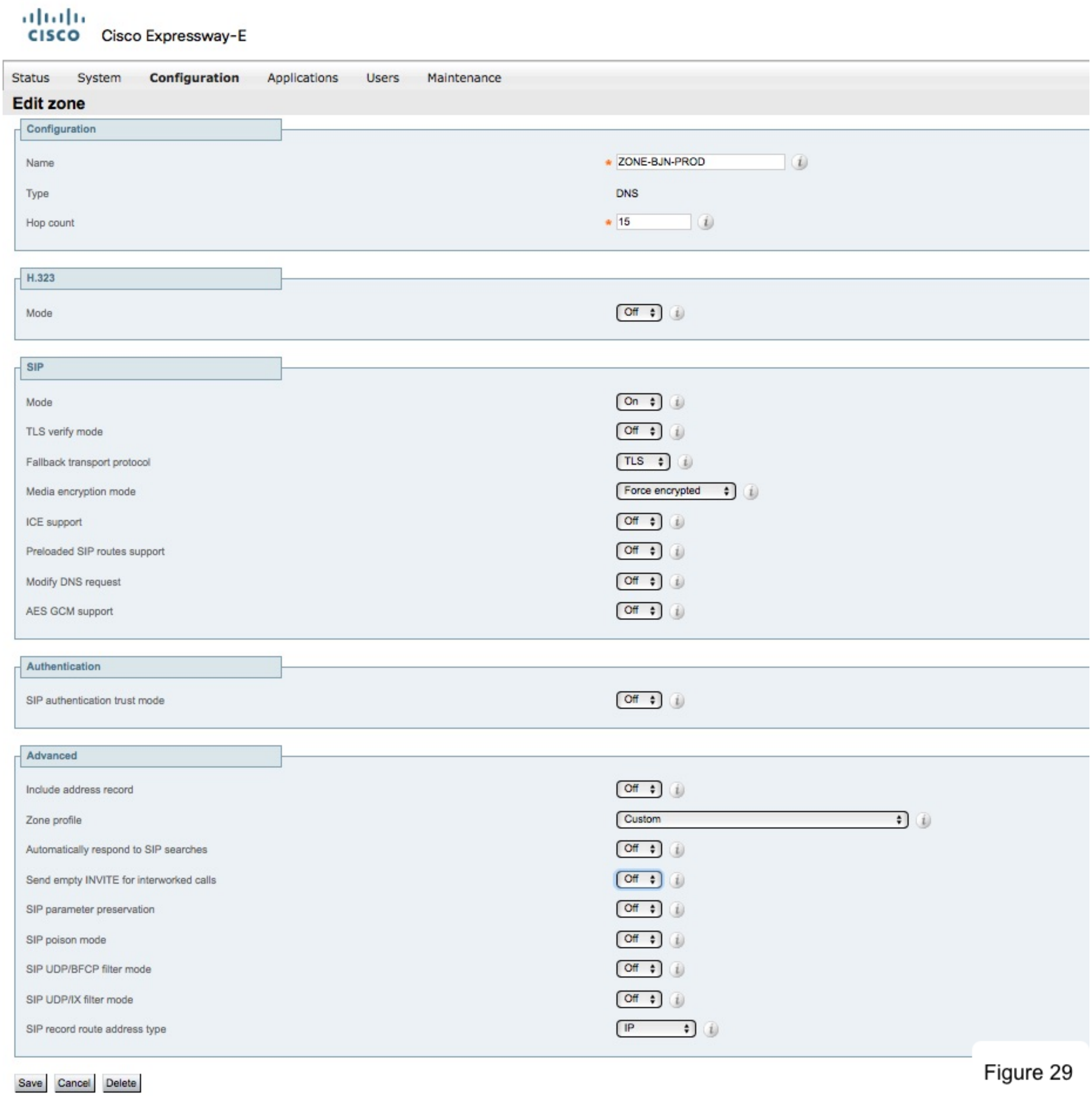


Figure 29

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

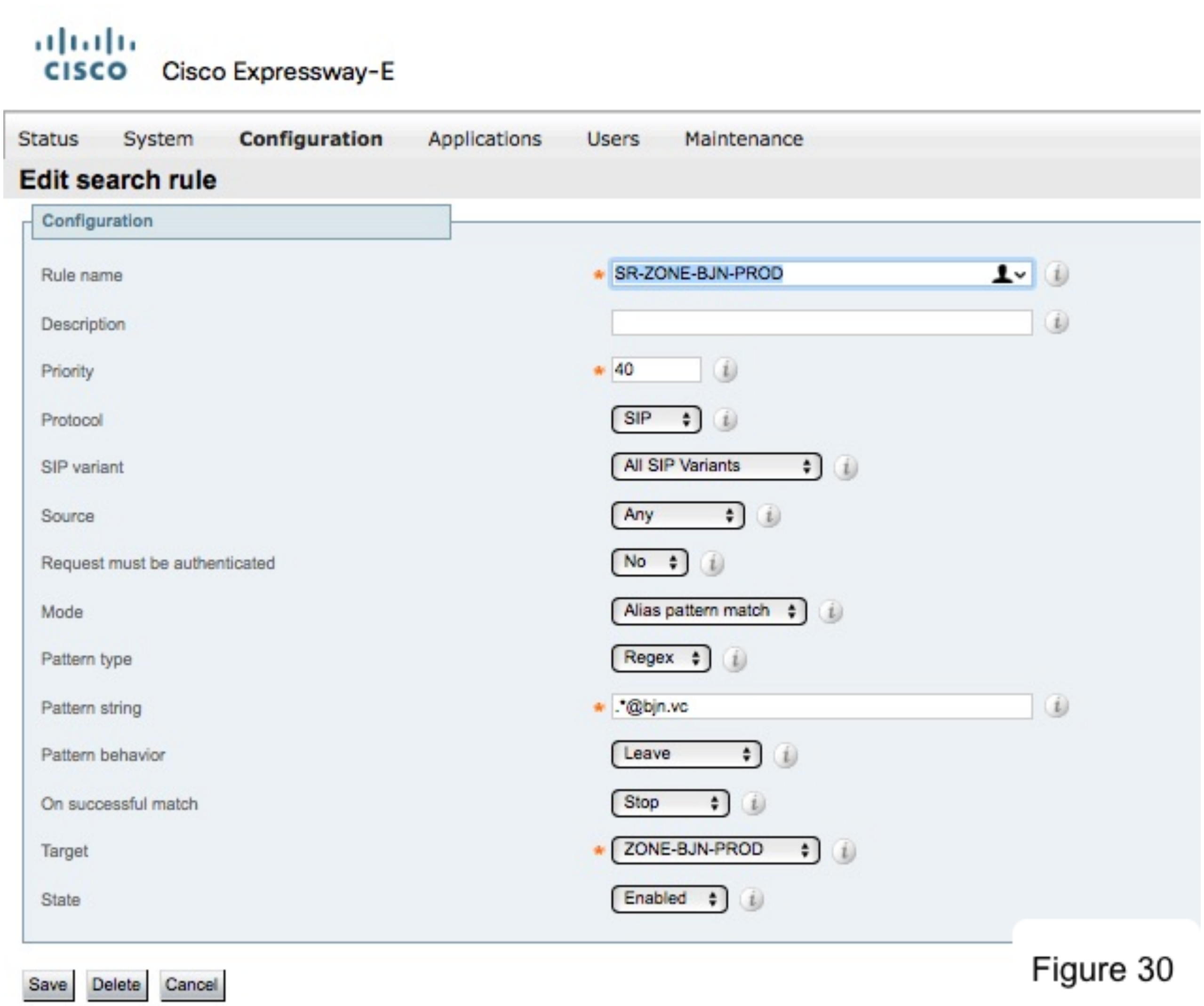


Figure 30

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 Authenicated: 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

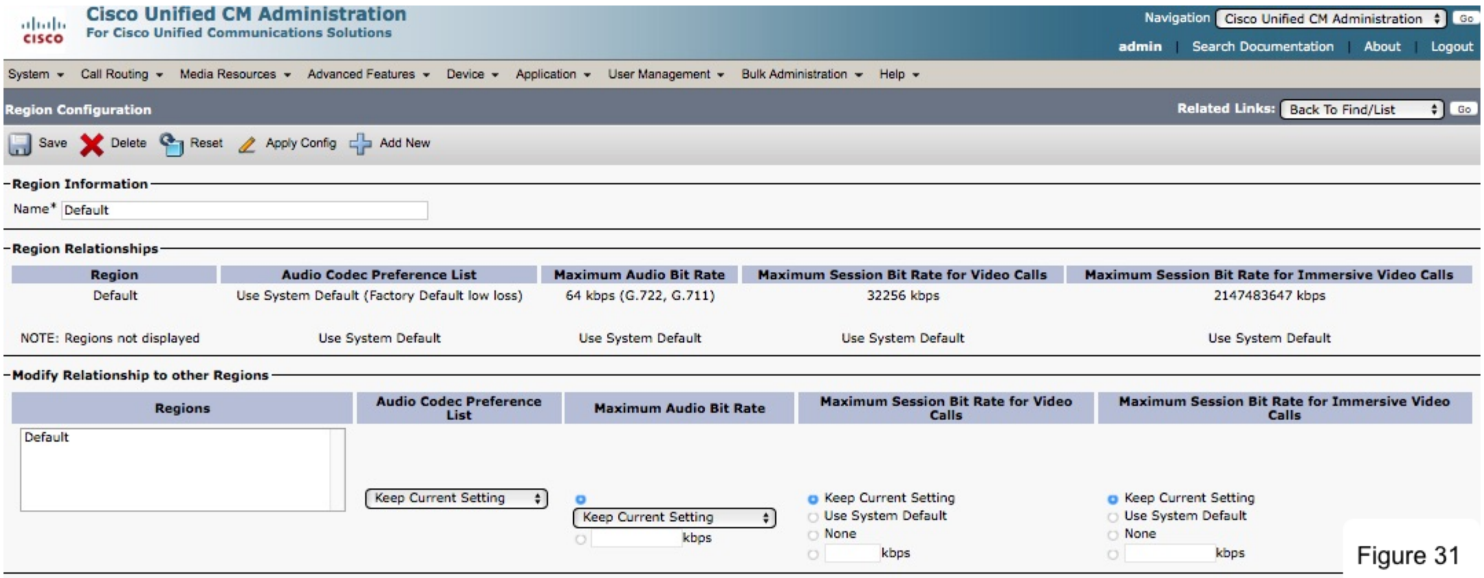


Figure 31

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.

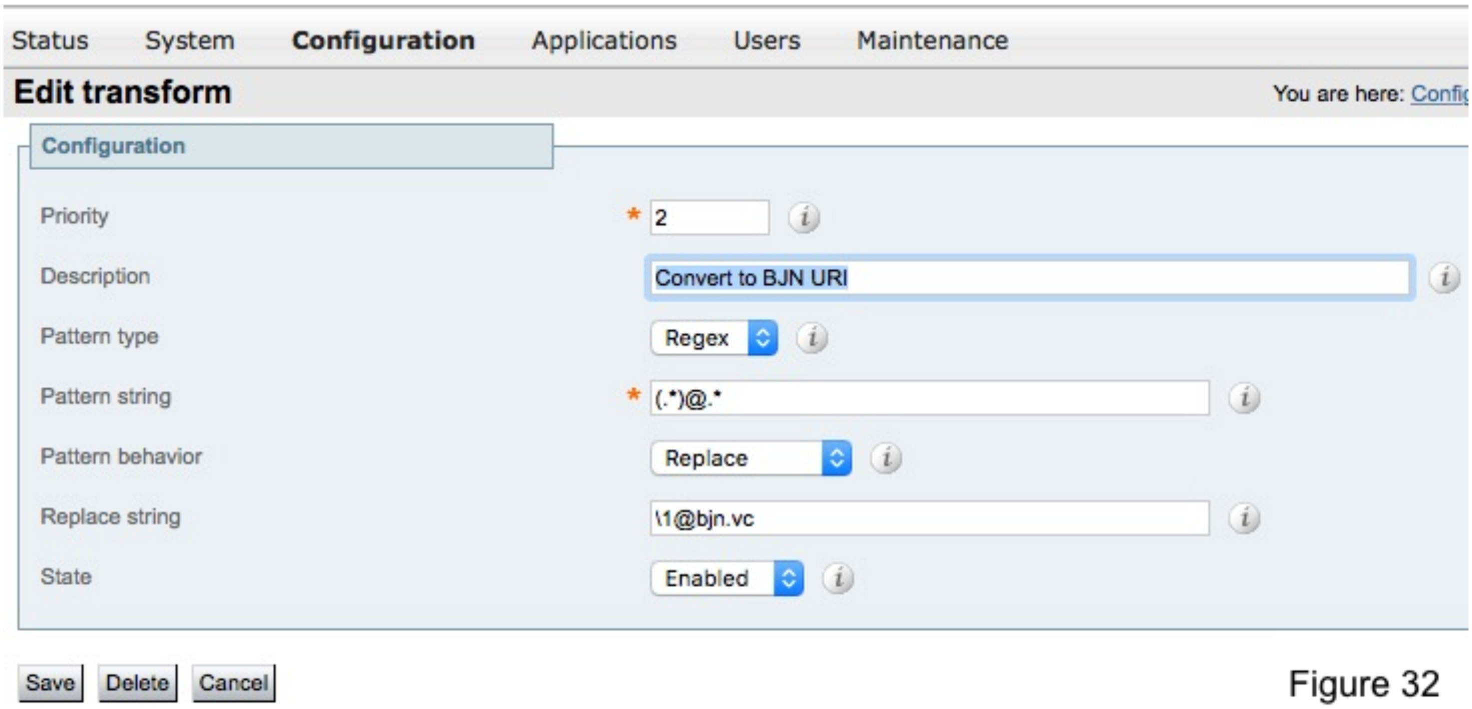


Figure 32

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

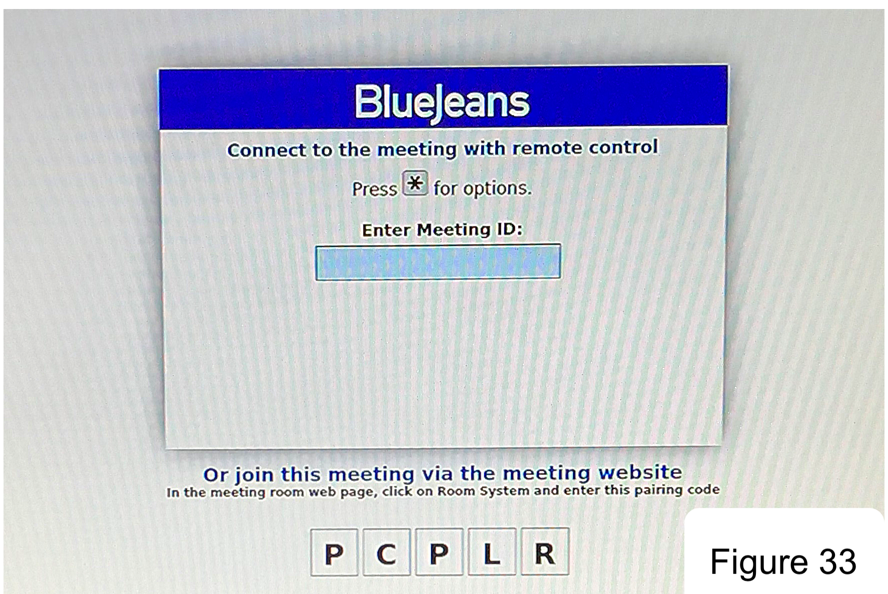


Figure 33

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

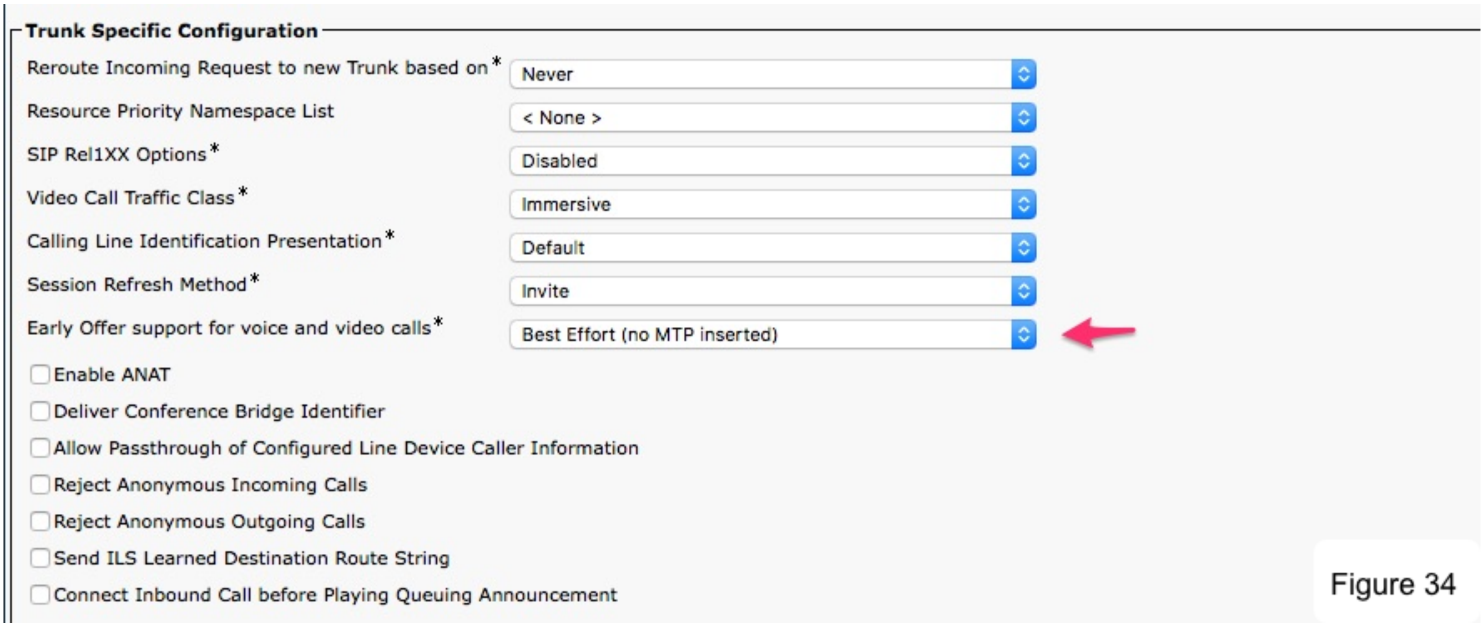


Figure 34

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

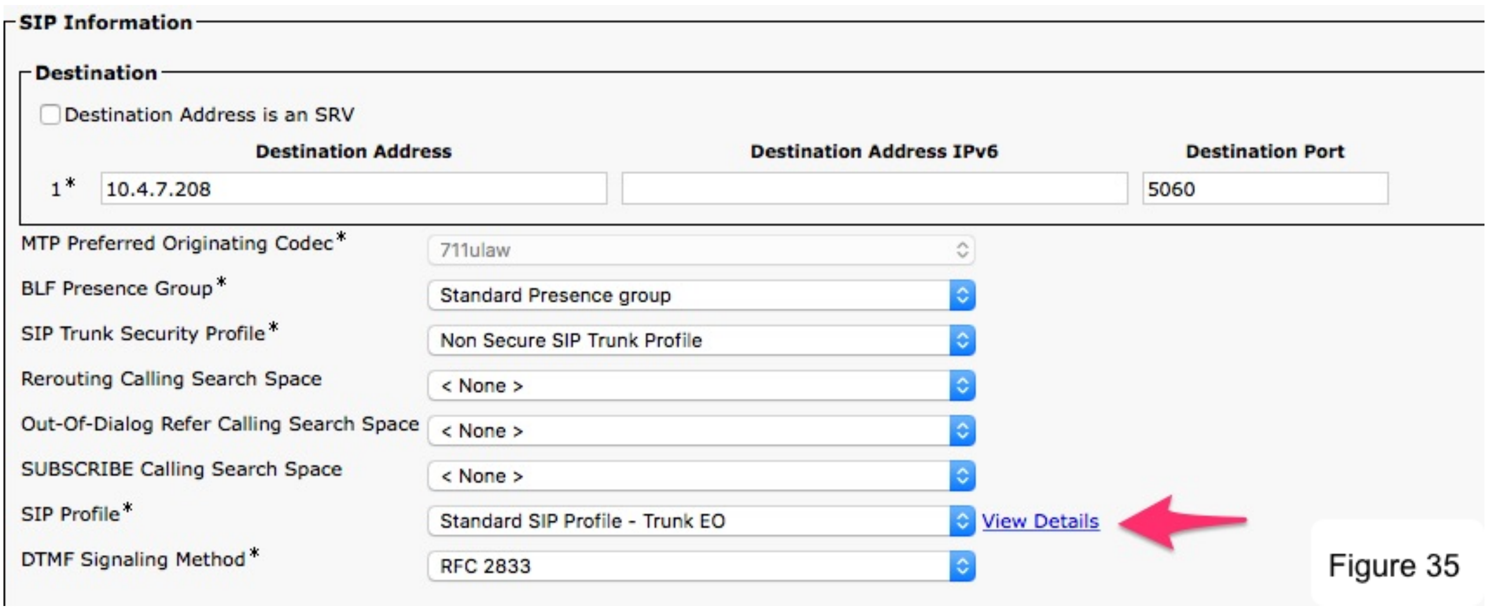


Figure 35

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

Figure 36

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 the 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

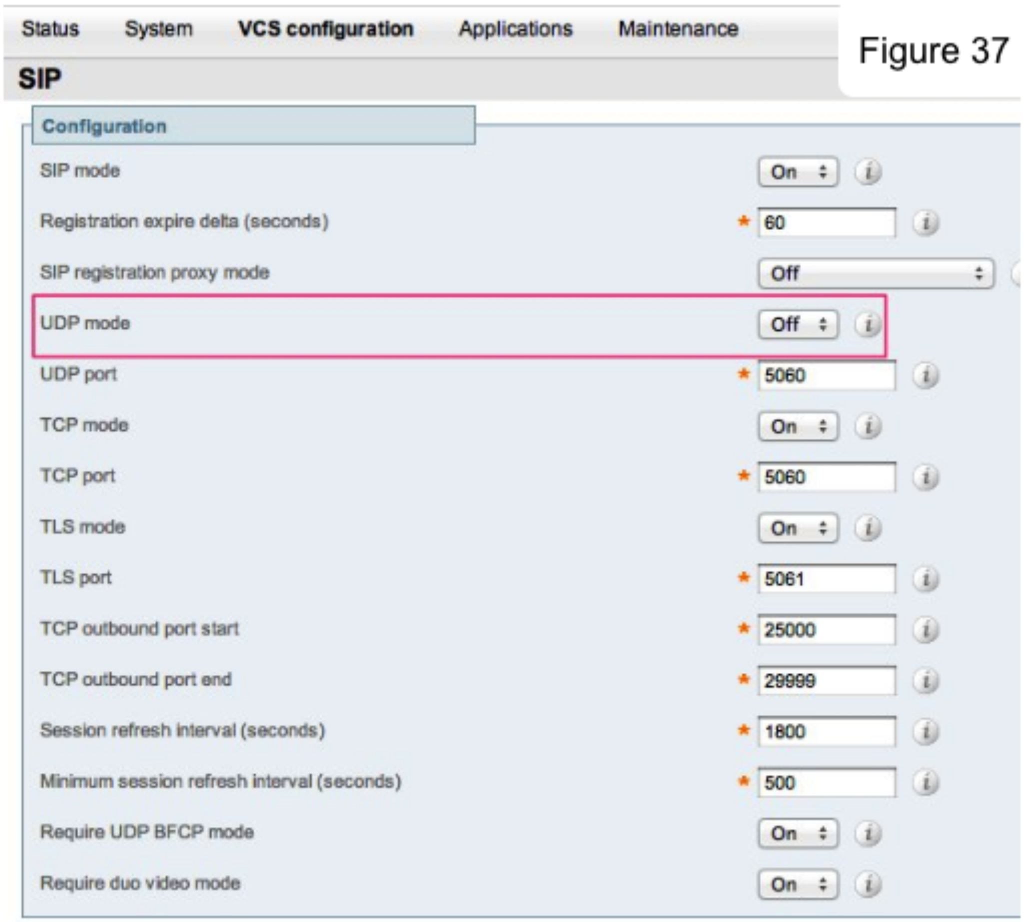


Figure 37

Issue: There is a delay in reaching the BlueJeans IVR Welcom 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

Issue: Content share cannot be seen or in some cases sent properly. Investigating the VCS can see RTP received, but protocal 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 cab 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 (0r 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 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 expereincing the issue