BlueJeans

Relay

Getting Started

BlueJeans

What is Blue Jeans Relay?

Blue Jeans Relay is a software solution that integrates customer-premise components and applications with the Blue Jeans cloud.

Relay Touch, the first solution powered by Blue Jeans Relay, integrates calendar applications, conference room systems, and everyday tablet computers to make joining a Blue Jeans meeting easy and automatic.

With scheduled meetings displayed on the Relay Touch app, participants can touch to join meetings from most H.323- and SIP-based conference room system, with no need to dial, pair, or enter a meeting ID.

BlueJeans

Components of Relay

Deploying Relay involves three components:

The **Listener Service** is an on-premise program which controls your Endpoints on your behalf. It connects to the Relay server.

Your **Endpoints** will be provisioned in the Relay server with network and calendar information.

Tablets in conference rooms will show meetings and allow single-tap joining with the **Relay Touch** app.

BlueJeans

Signing Up for Relay

To start using Relay, you will need a Relay username and password.

You can ask your Blue Jeans Customer Success Manager to send you these credentials.

Alternately, you can submit a request at http://bluejeans.com/features/relay to get these credentials.

Relay comes standard with all Blue Jeans accounts.

BlueJeans

What Do I Need to Get Started?

In addition to your Relay credentials, you will need:

- a host operating system on which to install the Listener Service on your network
- access to configure your Google Calendar, Exchange, or Office 365 calendar server
- a compatible video conferencing endpoint
- an Android 4.2 tablet on which to install the Relay Touch app

Refer to Requirements for more information.

BlueJeans

Relay Deployment Services

While Blue Jeans Relay is free for Blue Jeans customers, configuration is required to make the software to work with your calendar application, conference room systems, and Blue Jeans service. The Blue Jeans Relay download package includes the software to install on your on-premise server, plus step-by-step configuration instructions. Once your account is provisioned, software installed, and tablets procured for each conference room, most deployments can be configured in about an hour.

You can also purchase a **Relay Deployment Services Package** to receive four hours of configuration assistance from a Blue Jeans specialist. If you have already purchased Advanced Services or Deployment Services as part of your Blue Jeans service, you can receive this configuration assistance at no extra charge.

1 Listener Service Requirements

The Listener Service is a Java program, and can run in a variety of operating systems, including

- Debian/Ubuntu Linux
- RedHat/Fedora/CentOS Linux
- Windows Server 2008 or later

Java 7 or later is required. Both Oracle and OpenJDK distributions are supported. The Oracle JRE requires the Unlimited Strength Jurisdiction Policy Files for Java 7 and Java 8. On Linux, you can use openjdk-7-jre-headless.

A 1.5GHz CPU and at least 1GB RAM is recommended. You can use a physical machine, a virtual machine, or even a Raspberry Pi!

2 Listener Service Provisioning

To configure a Listener Service, you will first need to provision a Listener Service ID.

Log in to the Relay administrative site with your Relay username and password.

Go to **Listener Services** on the left side, then click the **+ add** button. Fill in a descriptive Name and click the save button in the top left.

After you save, the **ID** will appear for your Listener Service. Copy this ID to use when you configure your Listener Service installation.

3 Listener Service Installation & Upgrade

Once your host OS is set up, download the Listener Service installer from the Blue Jeans Downloads page.

Start with the appropriate installation command below:

Debian or Ubuntu

```
sudo dpkg -i listenerservice*.deb
/opt/listenerservice/setup.sh
sudo service listenerservice restart
```

RedHat, Fedora, or CentOS

```
sudo rpm -Uvf listenerservice*.rpm
/usr/local/listenerservice/setup.sh
sudo service listenerservice restart
```

Windows

Run listenerservice.exe as an administrator.

Java executable JAR

Unpack listenerservice.jar and setup.sh to a directory.

After configuration, start the service by running

```
java -jar listenerservice.jar
```

Upgrading

Download the installer and run the above installation commands. It's a good idea to backup config.properties and private.der from your installation directory.

4 Listener Service Configuration

Once the installation is complete, you must configure the Listener Service so it can log in to the Relay server.

On Windows, the installer prompts you for configuration. On other operating systems, run **sh setup.sh** in the installation directory.

Alternately, you can manually edit **config.properties** in the installation directory (usually /opt/listenerservice or /usr/local/listenerservice):

a. Set **listenerServiceId** to the ID you previously provisioned.

b. Set **amqp.username** to your Relay username.

c. Set **amqp.password** to your encrypted Relay password, which you can get by running

```
sudo -u listenerservice java -jar listenerservice.jar
  --encrypt-password <username> <password>
```

d. Restart the Listener Service to apply your changes.

```
sudo service listenerservice restart
```

5 Listener Service Enhanced Encryption

Relay can optionally use Public Key Encryption to secure your Endpoint passwords. Only you will be able to read these passwords, because your private key will never leave your LAN host.

If you've installed the Listener Service using the .deb or .rpm packages, setup.sh will prompt you to enable Enhanced Encryption. Alternately, you can run genssl.sh to generate your key pair. It will save your private key to private.der, and your base-64-encoded public key to public.b64.

If you've installed some other way, here are the steps to generate a key pair using OpenSSL:

```
openssl genrsa -out private.pem 2048
openssl pkcs8 -topk8 -in private.pem -outform DER -out private.
   der -nocrypt
openssl rsa -in private.pem -pubout -outform DER -out public.der
chmod 600 private.der private.pem
chown listenerservice:listenerservice private.* public.*
base64 < public.der > public.b64
```

Upload your public key with the instructions on the next page.

5 In the Relay administrative site, click on your Enterprise name in the top-right, and paste the base64-encoded public key into the **Public Key** field. Click the save button. From now on, each Endpoint password you set will use this public key.

In config.properties, set **encryption.private_key_file** to the private.der file path and restart the Listener Service.

```
encryption.private_key_file=path/to/private.der
```

Don’t share or lose your private key!

6 Listener Service Configuration Tips

Location

Listener Services should be located close (in network terms) to the Endpoints they will control. For multiple geographies, it is best to host a Listener Service in each geography, and set the Endpoints to use the closest one.

Exchange Integration

When setting up multiple Listener Services in a Microsoft Exchange environment, enable Exchange polling only on the Listener Service (or cluster, see below) closest to Exchange for optimal performance. If multiple Listener Services poll multiple Exchange servers, it is imperative that all Exchange servers return the same calendar data.

Alternative Transport

The Listener Service makes brief outbound connections on port **443** (HTTPS) and persistently connects to the Relay cloud on a port in the range **5671–5679** (AMQP over TLS). If you can't open the latter ports, you can try the experimental STOMP over Websockets transport. To enable, set up the Listener Service normally, then

6 manually edit the **config.properties** file and append:

```
transport=webstomp
```

Then restart the Listener Service, which will now connect outbound only via HTTPS.

Clustering

For high availability and load balancing, the Listener Service may be deployed in clusters where each Listener Service is active and shares the work load. If one stops working, the others continue.

To the Admin UI, each cluster appears as a single Listener Service. All Listener Service instances in a cluster must be configured identically, and they will share a single Listener Service ID.

To set up a cluster, install the Listener Service on each host in the cluster. After configuring the first one as a new Listener Service using the setup program, configure the others, but choose the name of the existing Listener Service when prompted instead of creating a new one.

Alternatively, **config.properties** may be copied from the first host to the others. Always restart the Listener Service after making any changes to config.properties.

7 Endpoint Requirements

Relay has been verified on these Endpoint product lines.

- Cisco/Tandberg, excluding CTS
- Polycom HDX, RealPresence Group, VSX
- Lifesize Express, Icon, Room, Team
- Tely
- StarLeaf GT Mini

Refer to Requirements for more details, including verified Endpoint models.

To provision your Endpoint, you will need to know its

- IP address
- username and password
- manufacturer and model
- calendar information (see the Google Calendar, Exchange, and Office 365 setup guides)

8 Endpoint Provisioning

In the Relay administrative site, go to Endpoints and click the **+ add** button.

Pick a descriptive **Name** and select the **Listener Service** you provisioned.

Set the **Control Protocol** to the type of your Endpoint.

Fill in the **IP Address**, **Username**, and **Password** of your Endpoint.

Set the **Calendar ID** and **Calendar Type** according to the Google Calendar, Exchange, or Office 365 setup guide.

You should leave the other fields at their default values unless you need to deal with a specific issue.

Press the save button, and you should be able to use the **Join meeting** link to dial the Endpoint into a Blue Jeans meeting. Type in a Meeting ID and Passcode, and see if the call connects.

9 Joining Meetings From an Endpoint

Using Relay, scheduled meetings can be displayed and joined from the built-in touchscreens and on-screen displays of certain Endpoints:

- Cisco/Tandberg
- Cisco IX
- Lifesize Icon

To enable, select an Endpoint with one of these Control Protocols, and enable **Push Meetings To Endpoint**.

If you have another system managing your Endpoint, such as TMS, CTS-MAN, or Lifesize UVC Manager, you should disable its calendar scheduling feature for this Endpoint to avoid scheduling conflicts with Relay.

10 Joining Meetings From the Tablet App

For Endpoints that cannot display scheduled meetings from Relay, you can install the Relay Touch app on an Android tablet in the conference room.

Relay Touch displays the list of scheduled meetings and allows the user to join with one touch, mute/unmute the Endpoint's microphone, and hang up.

To set up Relay Touch, you will need a tablet with Android 4.2 Jelly Bean or later. A wifi internet connection is required. A charging cable and security enclosure are recommended.

Search for **Relay Touch** on the Play Store to install the app.

11 Tablet Configuration

Once the Relay Touch app is installed, start the app and log in with your Relay username and password.

Pair the tablet with an Endpoint, either by choosing an existing one or provisioning a new one. Once you have chosen the Endpoint, you can dial a test call.

If you are provisioning a new Endpoint, set up calendar integration using the Relay administrative site.

Scheduled meetings for the Endpoint should appear. If the calendar invitation contains a Blue Jeans meeting URL in the description or location, the meeting icon will turn blue, and you can tap it to join instantly. Meetings displayed are limited to the last 30 minutes through the next 14 hours.

To reconfigure the app later, tap the tablet's menu button (☰ or ⋮) or long-press the back button, then tap Settings.

12 Endpoint Bulk Uploading

The Relay administrative site provides for bulk inserts and updates of Endpoints via a CSV file. To use this feature, click the “bulk upload” link from the Endpoints section. Follow the steps that appear. You’ll first download a CSV containing your existing endpoints, or one with only headers if you haven’t added any endpoints yet.

Just as with Endpoint provisioning, most of the time you’ll leave the port, signalingprotocol, dialstyle, addressstyle, and customdata fields blank/empty.

When adding a new endpoint, you will also leave the id field blank. To leave a password unchanged when modifying an endpoint, leave the password field blank. To use an empty password when adding a new endpoint, leave the password field blank. Remember, you can always change the password using the Relay administrative site as well.

12 Several of the fields have only certain values that are permitted; notably controlprotocol, signalingprotocol, dialstyle, addressstyle, and calendartype. Valid values can be found in the API documentation for Endpoint. At the time of this writing, the valid controlprotocol values are TANDBERG_HTTP, POLYCOM_HTTP_HDX, POLYCOM_HTTP_REALPRESENCE, LIFESIZE_SSH, and LIFESIZE_HTTP_ICON and the valid values for calendartype are GOOGLE and EXCHANGE (also used for Office 365). These exact values must be used, or CSV uploads will fail. When in doubt, you can create a "dummy" endpoint using the web form, and then find it as an example in the CSV file that you download in the first step.

When making edits to existing endpoints, be sure to leave the id field intact.

13 Health Monitoring

You can monitor the health of the Relay API server by sending an HTTPS GET request to

`https://relay.bluejeans.com/api/system/health`

The response status code will be **200** if all services are OK, and **503** otherwise. See the system.getHealth API documentation for more details.

You can remotely monitor the health of your Listener Services by sending an HTTPS GET request to

`https://relay.bluejeans.com/api/system/listenerhealth`

with your Relay username and password in Basic Auth. Inspect the JSON response for health information. See the system.getListenerHealth API documentation.

You can locally monitor the health of your Listener Services by opening a socket connection to your Listener Service host on port 8880. It will immediately echo **OK** if the service is running and connected to the Relay server, and **FAIL** otherwise.