BlueJeans

Blue Jeans Relay Listener Service Installation Guide

Introduction

The Relay Listener Service is the client on-premise service that awaits commands from the Relay cloud. These commands include endpoint controls (such as dial and disconnect), status inquiries (whether an endpoint is currently in a call), and Exchange Calendar polling (if enabled). It is supplied either as a Java JAR file or as RPM, DEB, or EXE installer files that include a Java Service Wrapper.

Prerequisites

The Listener Service requires a Java Virtual Machine (JVM) of at least version 7. It has been tested with OpenJDK 7 and Oracle JRE 7, and we recommend installation of the `openjdk-7-jre-headless` package on Ubuntu, or equivalent. For the Oracle JRE, some encryption features require the Java Cryptography Extension Unlimited Strength Jurisdiction Policy File to be installed.

Network Requirements

The Listener Service will make an outbound connection to the AMQP host specified in the file `config.properties` via TLS on ports **5671–5673**. It will perform DNS resolution if the host is given in FQDN format, which will require TCP/UDP on port **53**. The setup wizard makes an outbound connection to **relay.bluejeans.com** via HTTPS on port **443**. It makes no other connections out to the Internet.

Connections into your own internal network to control endpoints may be made on ports **22** (SSH), **80** (HTTP), **443** (HTTPS), **8081** (HTTP), **8443** (HTTPS), or **23456** (HTTP). The port used depends on the API mechanism for each type of endpoint (e.g., Cisco/Tandberg, LifeSize, Polycom, StarLeaf, Tely), and can be customized for each endpoint.

Installation

RedHat, Fedora, or CentOS

1. Download the latest Listener Service RPM installer.
2. Unzip the downloaded ZIP file by running `unzip listenerservice*.zip`.
3. Install the service by running `rpm -Uvf listenerservice*.rpm` as root.
4. A `listenerservice` user and group will be automatically created during installation, and init scripts will be put in place to start and stop the Listener Service much like any other service.
5. Proceed to the configuration steps below.

Debian or Ubuntu

1. Download the latest Listener Service DEB installer.
2. Unzip the downloaded ZIP file by running `unzip listenerservice*.zip`.
3. Install the service by running `dpkg -i listenerservice*.deb` as root.
4. A `listenerservice` user and group will be automatically created during installation, and init scripts will be put in place to start and stop the Listener Service much like any other service.
5. Proceed to the configuration steps below.

Windows

1. Download the latest Listener Service EXE installer.
2. Open the downloaded ZIP file.
3. Start the installer by running `listenerservice.exe` (you may see User Account Control or password prompts).
4. Proceed to the configuration steps below.

Configuration

RedHat, Fedora, CentOS, Debian, or Ubuntu

1. In a terminal shell, go to the installation directory by running `cd /usr/local/listenerservice` (RedHat, Fedora, or CentOS) or `cd /opt/listenerservice` (Debian or Ubuntu).
2. Start the configuration wizard by running `sudo ./setup.sh`.
3. Enter your Relay credentials in the installation wizard.
4. If this Listener Service has already been provisioned, choose it from the list of Listener Services, otherwise, create a new one with a name of your choice.
5. If your Relay enterprise has Enhanced Encryption enabled, you must supply the private key file. If not, you may enable Enhanced Encryption if you wish.
6. If you want to synchronize endpoint calendars from Microsoft Exchange or Office 365, fill in the Exchange user's email/username, password, and domain. Use **Autodiscover** to fill in the service URL automatically. Office 365 has a preset domain and service URL.
   You must also follow the Exchange Calendar Setup or Office 365 Calendar Setup guides, which include additional required steps.
7. Confirm your changes to save the configuration.
8. Start the service by running `service listenerservice start` as root.

Windows

1. Enter your Relay credentials in the installation wizard.
2. If this Listener Service has already been provisioned, choose it from the list of Listener Services, otherwise, create a new one with a name of your choice.
3. If your Relay enterprise has Enhanced Encryption enabled, you must supply the private key file. If not, you may enable Enhanced Encryption if you wish.
4. If you want to synchronize endpoint calendars from Microsoft Exchange or Office 365, fill in the Exchange user's email/username, password, and domain. Use **Autodiscover** to fill in the service URL automatically. Office 365 has a preset domain and service URL.
   You must also follow the Exchange Calendar Setup or Office 365 Calendar Setup guides, which include additional required steps.
5. You may optionally set the installation directory to a non-default folder.
6. The wizard will install the service, save your configuration, and start the service.
7. Reboot your computer, especially if you have not rebooted since installing Java.

Next steps

Now that your Listener Service is installed and running, you can provision endpoints and dial them into meetings. See the Getting Started guide for more information.

Upgrading

RedHat, Fedora, or CentOS

1. Download the latest Listener Service RPM installer.
2. Unzip the downloaded ZIP file by running `unzip listenerservice*.zip`.
3. Install the service by running `rpm -Uvf listenerservice*.rpm` as root.
4. Restart the service by running `service listenerservice restart` as root.

Debian or Ubuntu

1. Download the latest Listener Service DEB installer.
2. Unzip the downloaded ZIP file by running `unzip listenerservice*.zip`.

3. Install the service by running `dpkg -i listenerservice*.deb` as root.
4. Restart the service by running `service listenerservice restart` as root.

Windows

1. Download the latest Listener Service EXE installer.
2. Open the downloaded ZIP file.
3. Start the installer by running `listenerservice.exe` (you may see User Account Control or password prompts).
4. Leave the **Keep existing configuration** option checked.
5. The wizard will upgrade your existing installation and restart the service.

Advanced

Configuration

The Listener Service looks for a file called `config.properties`. Configuration values for this file are supplied by Blue Jeans and the file must be in the same directory as the `listenerservice-jar-with-dependencies.jar` file. It contains the AMQP host (see "Network Requirements" above), the username to use when logging in to that host, an encrypted form of the password to be used, and a unique `listenerServiceId`. See the comments in the file for examples and details.

Enhanced Encryption

We strongly recommend using Enhanced Encryption for storage of endpoint passwords provisioned with our cloud service. Enhanced Encryption uses Public Key Encryption to keep your endpoint passwords a secret, even from Blue Jeans. This requires generating a public/private RSA key pair in DER format and then provisioning your public RSA key with our cloud service.

To generate a random RSA key pair, you can either (a) let the setup wizard create it for you (see "Configuration" above), (b) run the `genssl.sh` script from the Listener Service install directory, or (c) create it manually. Choose one:

(a) If you choose to let the setup wizard enable Enhanced Encryption for you, it will automatically generate your key pair, provision the public key with our cloud service, and configure your Listener Service to use the private key.

(b) If you choose to generate the key pair using `genssl.sh`, it will create your key pair, but you must provision the public key with our cloud service and configure your Listener Service to use the private key.

```
cd /opt/listenerservice
./genssl.sh
```

(c) If you choose to generate the key pair manually, you must run `openssl` yourself, as well as provision the public key with our cloud service and configure your Listener Service to use the private key.

```
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
```

Once you have your `public.der` file, it must be provisioned with your enterprise on our cloud service. You can do this yourself through the Relay administrative site (click your enterprise name in the top-

right corner, and find the **Public Key** box) or the REST API. The key must first be base64 encoded if you created the key manually. For example:

```
base64 < public.der
```

If you used the `genssl.sh` script, you will already have a base64-encoded version of your public key called `public.b64`.

Be sure that your `private.pem` and `private.der` files are readable only by the user that will run the Listener Service (e.g., `chmod 600 private.*`). It is also a best practice to keep a copy of your `private.pem` file in a safe place! If you lose your private key, it will not be possible to recover, decrypt, or re-encrypt any of your provisioned endpoint passwords; they will all have to be provisioned again.

The location of your private key file must also be added to `config.properties`:

```
encryption.private_key_file=/opt/listenerservice/private.der
```

If you opt not to use public key encryption, passwords are stored in an encrypted format that is difficult, but not impossible to decrypt. Using public key encryption ensures that only your own hosts with a copy of your private key on your own premises are capable of decrypting your endpoint passwords.

If you have existing endpoints with passwords provisioned without public key encryption, and then you provision a public key, the endpoints' encrypted passwords will be converted to use public key encryption only when the endpoints are updated. Any update will suffice, even an empty PATCH. This ensures that if there are any errors or problems with encryption setup, all endpoint passwords won't be immediately re-encrypted and potentially lost. It may be advantageous to update a single endpoint first and ensure that everything is working as expected before updating all endpoints.

Configuring the Listener Service for public key encryption does not preclude the default secret-key encrypted passwords from working; the two may coexist. We recommend, however, updating existing endpoints to use public key encryption as soon as practicable after provisioning the public key and verifying functionality.

See the provisioning guide and API documentation for more details about using the REST API.

Logs

Logging messages are saved to the `listenerService.log` file in a directory called `logs` in the Listener Service installation directory. The log file will rotate when it reaches 1MB in size, and up to 10 old log files will be retained. When the Listener Service is run from the command line, logging messages also appear on the console.

Provisioning of endpoints and configuration of calendar polling are performed on the cloud service, not on the listener service; please see the Getting Started guide for these details.