BlueJeans

TECHNICAL GUIDE

BlueJeans Network Security and Privacy

BlueJeans understands an organization's need for secure communications. The BlueJeans meetings platform provides the essential security features of an enterprise-grade video meetings service.

TABLE OF CONTENTS

Cloud Architecture Security

Global Data Center Security

The BlueJeans service was built from the ground up by BlueJeans and consists of software that runs on cloud-compute clusters from a leading global server vendor. The service is hosted in multiple ISO27001 certified top-tier co-location data centers around the world, and in each of these PoPs, dedicated cages and racks are protected with 24x7x365 security and multiple levels of biometric access controls. Access to the cages is restricted to BlueJeans Operations personnel.

Infrastructure and Network Security

BlueJeans employs a wide range of security management practices to provide a secure and reliable service to customers. This includes network firewalls throughout the infrastructure to create security zones for different applications and services. BlueJeans also deploys proxy servers that terminate all 3rd party/customer traffic at a proxy layer. All web traffic passes through industry-leading load balancers to protect against a suite of application attack vectors.

Beyond the firewall, proxy servers and load balancers, BlueJeans also periodically scans for network, port, and application-level vulnerabilities. Vulnerability scans are conducted by a leading 3rd party SaaS provider, in addition to some special-purpose, in-house scanning tools. Furthermore, all of the 3rd party applications and operating system software is checked for security advisories and is patched periodically.

Routers, firewalls, load balancers, and proxy application servers are all configured to mitigate numerous types of DOS attacks. BlueJeans also engages with 3rd party consultants to perform penetration testing of the service. All of their findings are reviewed and appropriate actions are then taken to address and mitigate vulnerabilities found in the service.

Web Application Security

This section covers the security features that can be enabled at the user level.

User Account Security

All user accounts are secure using the following technologies and security measures:

- Each BlueJeans account is secured with a standard username and password, or via SSO SAML
- 2.0 assertion from your IDP
- Authentication requests are always sent over HTTPS
- Passwords are SHA-256 salted/hashed in the database and can never be viewed in plain text
- Passwords are never sent via email or any other form of electronic transmission (the “Forgot Password” feature only allows for resetting the end-user’s password)

In-Meeting Security Features

BlueJeans meetings come with optional security capabilities that users may set as default or enable when required.

Meeting ID

A randomized nine-digit number uniquely identifying a meeting.

Participant Passcode
A second-level of authentication that can optionally be enabled for each meeting.

Publish Meeting Option
An option that allows a meeting to remain hidden on the end-user's personal meeting room. Participants must either join these meetings directly from an email invitation or by entering the Meeting ID and/or password via the bluejeans.com homepage.

Encrypt Meeting Option
An option that forces a BlueJeans meeting to only allow end points with sufficient encryption capabilities enabled. Please see Media Handling & Encryption for additional details on encryption.

Expel Participant
During the course of a meeting, any participant can quickly be removed from the meeting with a click of a button.

Lock Meeting
During the course of a meeting, the session may be locked down to only include those participants that are in attendance.

Admin-Level Security

Group Administrator Security Features
As a Group Administrator, BlueJeans allows security policies to be created for all users in your organization. These include:

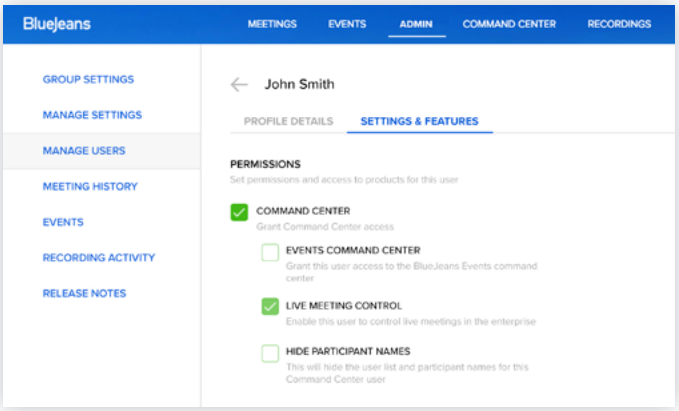
- User Authentication Options (standard User Password configuration or SAML Single Sign On)
- User Password Requirements
- Change Password Options
- Failed Login Notifications
- Enable Video Connection Type (set supported and default endpoints for your Group)

BlueJeans also offers the option to obscure personally-identifying information (such as participant names and IP addresses) in the Command Center console so that IT personnel can monitor and support meetings while respecting the privacy of paricipants.

Remote Moderation and Live Meeting Control
Group Administrators can offer moderation and technical support in either of two ways:

- In-Meeting Moderator: Join any live meeting
- Remote Moderator: Manage the meeting from the Live Meeting Control console in Command Center. Controls include mute/unmute participants, lock the meeting, and push layouts.

Remote Moderation is an ideal option to protect the confidentiality of sensitive conversations and documents. Live Meeting Control is enabled first for an enterprise and then on a per-admin user basis, giving complete control over access to this powerful feature.



Privacy and Customer Data Storage

Only the most basic user data is stored in the BlueJeans database. BlueJeans stores the following user information:

User Profile Details

- Username (Facebook login includes Facebook username, Linkedin login includes Linkedin profile URL)
- Password (SHA-256 salted hash)
- Email Address
- First Name
- Middle Name
- Last Name
- Title
- Company Name
- Profile Picture

Billing Details

The BlueJeans Service currently leverages a third-party, PCI-compliant partner to handle all billing aspects of the service. This means no user credit card or billing information resides in the BlueJeans database. Because the service is used by thousands of companies globally, BlueJeans is also compliant with the EU-U.S. Privacy Shield Framework.

More information about this as well as the privacy policy can be found here: http://bluejeans.com/privacy-policy

Media Handling and Encryption

BlueJeans takes the utmost care with your communications, and does not record or capture any video or desktop-sharing streams without interaction and consent from customers. It is recommended that an organization employ the proper steps to ensure that software-based video clients are secured on the desktop, and that no malware may intercept media at the hardware level. BlueJeans supports standards-based encryption (AES-128) that is available on most video endpoints today.

BlueJeans connections using BlueJeans client applications or web browsers for video are encrypted by default in BlueJeans meetings, as are many other solutions such as Cisco Jabber or Microsoft Lync.

If using room based video endpoints, such as Polycom, Lifesize, Cisco, etc. to connect to BlueJeans calls, they will encrypt upon connection to BlueJeans provided that they have this feature enabled and the proper security licenses from those vendors.

Most video room systems encrypt by default as long as both sides of the call support it. However, it is recommended that you check your system to require encryption for all calls, or to encrypt by default. As mentioned in the “In Meeting Security Features” section above you can select, “Enforce Encryption” when scheduling a BlueJeans meeting to ensure only encryption capable devices can join the meeting. This will help ensure that your room systems connection to BlueJeans using either H.323 or SIP will be a standards based encrypted connection.

Recording and Video Content Storage and Encryption

The BlueJeans service also includes the unique capability of uploading and sharing full-motion video content in your meetings, as well as the ability to record and share your meetings. The security of both of these features is important to our customers and to us. Here it's a little bit more about the security of each.

Recordings are stored in secure containers in the cloud. These videos are encrypted at rest (AES-256bit) and are only accessible to the recording originator. They may be shared by the recording originator using email addresses through the web user interface. These can be viewed as an encrypted (AES-128bit) playback stream using a web browser or downloaded to an on premise media server or storage device. Users may choose to delete their recordings from BlueJeans at any time, again using the web user interface.

Uploaded shared video content is also stored in secure containers. The video content sharing stream is also encrypted (AES-128bit) when shared in a meeting. Users may also choose to delete their uploaded video content from our service as well.

Service Organization Controls (SOC) 2

In addition to the security measures taken around our service infrastructure as well as the in meeting security features of the product, BlueJeans has taken important steps to ensure the integrity of our internal operation is also addressed.

BlueJeans has completed the Statement on Standards for Attestation Engagements (SSAE16) Service Organization Controls (SOC) 2 Type 2 Report. Completion of this is a very important step for not only BlueJeans Network as a company, but also for our customer. This attests to our commitment as a service provider to our users that we have implemented formal documented procedures and controls across our organizations.

Policy, Communications, Procedural, and Monitoring control activities, as well as Disaster Recovery and EU-U.S. Privacy Shield Framework are covered under this report.

Compliance with the General Data Protection Regulation (GDPR)

The GDPR unifies data privacy requirements across the European Union (EU) and establishes data privacy as a fundamental right for EU citizens. Data security and user privacy have always been priorities for BlueJeans. To better support GDPR-compliant use of BlueJeans by our customers, we have modified the software, systems and processes to enable enterprise customers to proactively address requests by EU Nationals regarding personal data and systemized our response to user requests to correct, export or delete personal data. We continue to review our systems and processes to prioritize privacy by design and by default.

If you have further questions or concerns about the security of the BlueJeans Network service, please feel free to contact us at **sales@bluejeans.com** and we will be happy to assist.