



JIVE AND GoToCONNECT SECURITY AND PRIVACY OPERATIONAL CONTROLS

LogMeIn Jive and GoToConnect Security and Privacy Organizational Controls

Publication Date: 02/04/2020

1 Products and Services

GoToConnect powered by Jive is LogMeIn's all-in-one Unified Communications as a Service (UCaaS) solution for enterprises and businesses, which combines the power and reliability of LogMeIn's Jive cloud Voice-over-Internet Protocol (VoIP) phone systems and its GoToMeeting* web, audio and video conferencing service into one simple, reliable and flexible collaboration solution.

This document describes the security and privacy controls of (i) Jive, a cloud-based phone service designed to replace traditional on-premise, Private Branch Exchange (PBX) phone equipment; offering a robust suite of communications features and easy account management from a web browser or mobile application and (ii) GoToConnect; (in each case, the Service).

The following are features and offerings within the Service:

- Jive Business Continuity (JBC) is an optional, premium service/hardware offering installed on a customer's premise which provides local phone service, in the event of a network outage, via an independent third-party whose services are separately procured by a customer.
- Contact Center is designed to help users manage call queues and incoming customer calls through interactive voice responses, automatic call distribution and customer relationship management integrations.
- PBX Administration Portal allows users with administrator permissions to view and make universal changes to system settings from any device with an Internet connection.
- Visual Dial Plan Editor is a call flow editing tool to set up wait times or direct calls to specific voicemail boxes, auto attendants and ring groups.
- PSTN Replacement Services are services provided through partnerships with some of the world's leading telecommunications providers.

*For more information about the GoToMeeting Service and its security and privacy organizational controls, please consult the GoTo Collab Suite documentation available at www.logmeininc.com/trust.

2 Product Architecture

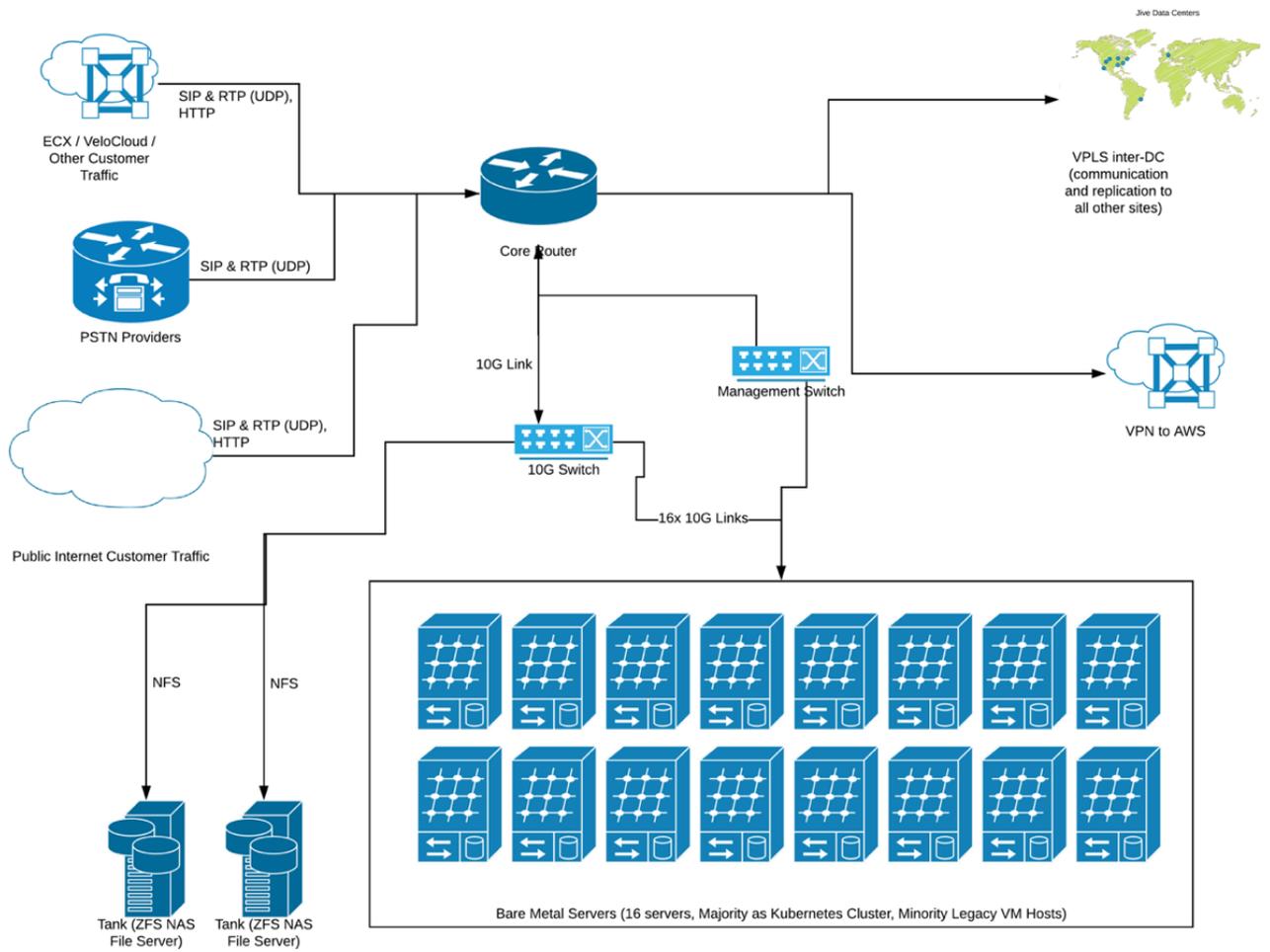


Figure 1- Jive Infrastructure

3 Jive Technical Security Controls

LogMeIn employs industry standard technical security controls appropriate to the nature and scope of the Services in order to safeguard its infrastructure and the data residing therein.

3.1 Logical Access Control

Logical access controls are in place, designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or “least privilege”) access to specified LogMeIn systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

The GoToConnect integrated Service offering utilizes LogMeIn’s proprietary identity management platform for customer provisioning, offers Single sign-on (SSO) using Security Assertion Markup Language (SAML), and integrates directly with LogMeIn’s GoToMeeting platform via API. This permits robust administrative controls, including allowing Customer account administrators to configure password policies, force password resets, and require utilization of SAML for login.

Service PBX administrators (Super Administrators) can grant or deny specific permissions in the PBX Administration Portal. These group permissions include the ability to configure the PBX, edit E911 addresses/locations, view reports, view and pay invoices, as well as create, update, and delete settings and accounts for:

- Users;
- User Groups;
- Extensions;
- Devices;
- Hardware;
- Sites; and
- Phone Numbers (delete and create managed through number ordering).

User level permissions are not directly configured as they are derived from the user, device, and line relationships.

For more details on group permissions, please reference the Jive Administrator PBX Guide [1].

3.2 Perimeter Defense and Intrusion Detection

LogMeIn employs industry standard perimeter protection tools, techniques and services that are designed to prevent unauthorized network traffic from entering its product infrastructure. The LogMeIn network features externally facing firewalls and internal network segmentation. Critical system files are protected against malicious and unintended infection or destruction.

3.3 Data Segregation

The Service leverages a multi-tenant (and multi-PBX) architecture, logically separated at the database level, based on a user's or organization's Service account. Only authenticated parties are granted access to relevant accounts.

3.4 Physical Security

Datacenter Physical Security

LogMeIn contracts with datacenters to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording;
- Multi-factor authentication to highly sensitive areas;
- Heating, ventilation, and air conditioning temperature control;
- Fire suppression and smoke detectors;
- Uninterruptible power supply (UPS);
- Raised floors or comprehensive cable management;
- Continuous monitoring and alerting;
- Protections against common natural and man-made disasters, as required by the geography and location of the relevant datacenter; and
- Scheduled maintenance and validation of all critical security and environmental controls.

LogMeIn limits physical access to production datacenters to authorized individuals only. Access to an on-premise server room or third-party hosting facility requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by Technical Operations. LogMeIn management reviews physical access logs to datacenters and server rooms on at least a quarterly basis. Additionally, physical access to datacenters is removed upon termination of previously authorized personnel.

3.5 Data Backup, Disaster Recovery, Availability

In order to provide redundancy, call failover, scalability, and high availability, the Service uses a containerized microservice mesh which allows for rapid deployment and scaling of services to satisfy the needs of LogMeIn's customers. This full-mesh design allows for microservices to self-discover and self-recover in the event of an outage at any specific datacenter or in the event of an issue localized geographically on the public Internet. Services are designed to fail-over between datacenter's automatically.

The infrastructure is connected between datacenters in the form of "clusters" with interconnectivity of a Virtual Private LAN Service (VPLS)/mesh network. VPLS connections can fail-over to a Dynamic Multipoint Virtual Private Network (DMVPN) in case primary links go offline. Each site has multiple peering connections with the public Internet. All production datacenter's are connected in such a manner that internal applications can reach services from any location. Each datacenter is hosted in private hardware (rack blades).

Connectivity to the Public Switch Telephone Network (PSTN) is made from each datacenter location to multiple PSTN Partners/providers via Session Initiation Protocol (SIP) trunks through the public Internet.

In order to provide high availability, LogMeIn operates a network of datacenter's in a fully interconnected mesh. These datacenter's operate with a capacity of N+1 datacenters, meaning that the Service has been designed to sustain the failure of the equivalent of one datacenter worth of capacity, and still have the ability to maintain uptime by automatically forwarding traffic to additional datacenter sites.

3.6 Malware Protection

Anomalous activity alerting capabilities are actively deployed and monitored on the Service. Alerts indicating potential malicious activity are sent to appropriate response teams for resolution or mitigation.

3.7 Encryption

LogMeIn maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other reputable standards groups. The cryptographic standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

In-Transit Encryption

The Service provides end-to-end data security measures. The Service is designed to ensure that communication data is not exposed in unencrypted form with communication servers or during transmission across public or private networks.

Internet Engineering Task Force (IETF) standard Transport Layer Security (TLS) protocols are used to protect communication between endpoints. All network traffic flowing in and out of LogMeIn datacenters, including all Customer Content [4], is encrypted in transit.

For their own protection, LogMeIn recommends that customers configure their browsers to use strong cryptography by default whenever possible and to ensure that operating system and browser security patches are kept up-to-date.

When TLS connections are established LogMeIn servers authenticate themselves to clients using public key certificates. TLS is also supported for signaling between physical phones and the Service infrastructure to secure the traffic and communication when supported by Customer equipment. Media is transmitted using Secure Real-time Transport Protocol (sRTP) utilizing shared keys transmitted over Session Initiation Protocol Secure (SIPS) to secure audio traffic. Provisioning information containing the physical phones credentials from the Service's infrastructure to the phones are also secured using TLS.

3.8 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted on no less than a monthly basis. Dynamic and static application vulnerability testing, as well as penetration testing activities for targeted environments, are also performed periodically. These scanning and testing

results are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams.

3.9 Logging and Alerting

LogMeIn collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

4 Organizational Controls

LogMeIn maintains a comprehensive set of organizational and administrative controls to protect the security and privacy posture of the Service.

4.1 Security Policies and Procedures

LogMeIn maintains a comprehensive set of security policies and procedures aligned with business goals, compliance programs, and overall corporate governance. These policies and procedures are periodically reviewed and updated as necessary to ensure ongoing compliance.

4.2 Standards Compliance

As a public company, LogMeIn complies with applicable legal, financial, data privacy, and regulatory requirements, including the requirements of the following standards:

- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. BSI Cloud Computing Catalogue (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS) compliance for LogMeIn's eCommerce and payment environments
- TRUSTe Verified Privacy Certification

4.3 Security Operations and Incident Management

LogMeIn's Security Operations Center (SOC) is staffed by the Security Operations team and is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with LogMeIn's critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating procedures. It is designed to manage, identify and resolve suspected or identified security events across its systems and Services. Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management when appropriate. Employees can

report security incidents via email, phone and/or ticket, according to the process documented on the LogMeIn intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.

4.4 Application Security

LogMeIn's application security program is based on the Microsoft Security Development Lifecycle (SDL) to secure product code. The core elements of this program are manual code reviews, threat modeling, static code analysis, dynamic analysis, and system hardening.

4.5 Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibility and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

4.6 Security Awareness and Training Programs

New hires are informed of security policies and the LogMeIn Code of Conduct and Business Ethics at orientation. This mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team.

LogMeIn employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire onboarding kits, awareness campaigns, webinars with the CISO, a security champion program, and the display of posters and other collateral, rotated at least bi-annually, that illustrate methods for securing data, devices, and facilities.

5 Privacy Practices

LogMeIn takes the privacy of its Customers and end users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1 Privacy Policy

LogMeIn discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on our public website [2]. The company may, from time to time, update the Privacy Policy to reflect changes to its information practices and/or changes in applicable law, but will provide notice on its website for any material changes prior to any such change taking effect.

5.2 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. The Service is compliant with the applicable provisions of the GDPR. For more information, please visit www.logmeininc.com/trust.

5.3 CCPA

LogMeIn hereby represents and warrants that it will be in compliance with the California Consumer Privacy Act (CCPA) and will implement and maintain the necessary controls to adhere to the applicable provisions of CCPA no later than January 1, 2020. For more information, please visit www.logmeininc.com/trust.

5.4 EU-U.S. and Swiss-U.S. Privacy Shield

LogMeIn, Inc. and its US affiliates participate in the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks regarding the collection, use and retention of personal information from European Union member countries and Switzerland [3]. Certification is reviewed annually by TRUSTe and any findings are promptly addressed by LogMeIn.

5.5 Return and Deletion of Customer Content

Customers may request the return or deletion of their Content through standardized interfaces at any time. If these interfaces are not available or LogMeIn is otherwise unable to complete the request, LogMeIn will make a commercially reasonable effort to support the Customer, subject to technical feasibility, in the retrieval or deletion of their Content. Customer Content will be deleted within thirty (30) days of Customer request. Upon expiration or termination of a Customer's account, Customer's Content shall automatically be deleted thirty (30) days after the effective date of the account expiration or termination. Upon written request, LogMeIn will certify to such Content deletion.

5.6 Sensitive Data

While LogMeIn aims to protect all Customer Content, regulatory and contractual limitations require us to restrict the use of Jive for certain types of information. Unless Customer has written permission from LogMeIn, the following data must not be uploaded or generated to the Service:

- Government issued identification numbers and image of identification documents.
- Information related to an individual's health, including – but not limited to – Personal Health Information (PHI) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related laws and regulations.
- Information related to financial accounts and payment instruments, including – but not limited to – credit card data. The only general exception to this provision extends to explicitly identified payment forms and pages that are used by LogMeIn to collect payment for the Service.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.7 Tracking and Analytics

LogMeIn is continuously improving its websites and products using various third-party web analytics tools, which help LogMeIn understand how visitors use its websites, desktop tools,

and mobile applications, what they like and dislike, and where they may have problems. For further details please reference our Privacy Policy [2].

6 Third Parties

6.1 Use of Third Parties

As part of LogMeIn's internal assessment and processes related to vendor and third party management, vendor evaluations may be performed by multiple teams depending upon relevancy and applicability. The Security team evaluates vendors that provide information security-based services including the evaluation of third party hosting facilities. Legal and Procurement may evaluate contracts, Statements of Work (SOW) and service agreements, as necessary per internal processes. Appropriate compliance documentation or reports may be obtained and evaluated at least annually, as deemed appropriate, to ensure the control environment is functioning adequately and any necessary user consideration controls are addressed. In addition, third parties that host or that are granted access to sensitive or confidential data by LogMeIn are required to sign a written contract outlining the relevant requirements for access to, or storage or handling of, the information (as applicable).

6.2 Contract Practices

To ensure business continuity and that appropriate measures are in place to protect the confidentiality and integrity of third-party business processes and data processing, LogMeIn reviews relevant third party's terms and conditions and either utilizes LogMeIn-approved procurement templates or negotiates such third-party terms, where deemed necessary.

7 Contacting LogMeIn

Customers can contact LogMeIn at <https://support.logmeininc.com/> for general inquiries or privacy@logmein.com for privacy-related questions.

8 References

- [1] LogMeIn, Inc., Jive Admin Guide, LogMeIn, Inc., June 2019.
[Online]. Available: <https://support.goto.com/jive/help/admin-guide-jive-admin-guide>
- [2] LogMeIn, Inc., "LogMeIn Privacy Policy," LogMeIn, Inc., January 2018.
[Online]. Available: <https://secure.logmein.com/policies/privacy.aspx>.
- [3] LogMeIn, Inc., "LogMeIn EU-U.S. Privacy Shield Notice," LogMeIn, Inc., November 2017.
[Online]. Available: <https://www.logmeininc.com/legal/privacy-shield>.
- [4] LogMeIn, Inc., "Terms of Service for LogMeIn and Goto Services," LogMeIn, Inc., February 2018. [Online]. Available: <https://www.logmeininc.com/legal/terms-and-conditions>.