]pexip[

SECURITY WHITEPAPER

Security Whitepaper version 4.5.2
Date: 04-DEC-2020

Contact details

Email: security@pexip.com

Web: www.pexip.com

Disclaimer

This document is provided for informational purposes only. The information in this whitepaper does not modify existing contractual arrangements, nor constitute legal advice. Its contents may be subject to change over time.

Pexip is an ISO 27001 certified company. Please see this notice for additional information.

Table of Contents

Introduction

As organizations consider the migration of business tools to a Cloud-based model, the question of data security is oftentimes raised. Such considerations may include the nature of types of data required to be shared with the Cloud Service Provider, the means of transfer of the data, how the data is handled at rest, and how that data is protected to maintain integrity. This document seeks to address these concerns for enterprises evaluating the Pexip Service Platform as a means of video enablement.

Pexip has taken extreme care in developing a very secure and reliable cloud services capability. This capability includes having embedded security for video devices hosted in the cloud, as well as secure portals for end-users and reselling partners, by using several different levels of security. Some of these levels are listed below. Due to confidentiality and security protocol however, we will not list all mechanisms currently in use.

Data Types and Storage

The Pexip Cloud Video Service is deployed via a globally-distributed network of resources which constitute the Pexip Service Network. Services are hosted and maintained at geographically-specific Points-of-Presence (PoPs) as well as within Cloud-based Services which have global availability but which can generally be associated to a primary hosting region. Together the various resources employed by Pexip provide for a robust and high-availability Service Network which subscribers of the service can rely upon.

Points of Presence (PoPs)

Pexip currently maintains Points of Presence in the following world locations, with additional PoPs periodically added:

San Jose, CA	Toronto, Canada	Ashburn, VA	Miami, FL	London, United Kingdom
Amsterdam, Netherlands	Frankfurt, Germany	Oslo, Norway	Johannesburg, South Africa	Singapore
Hong Kong, China	Tokyo, Japan	Sydney, Australia		

Pexip PoPs are hosted at Data Centers managed by facility service providers such Equinix, Q9, and SoftLayer. Each of the facilities has multi-factor security for access, including human security, security cameras, photo identity card access, key access to the equipment rack, and the like. Each facility is compliant with a well-known security compliance standard such as SOC2, SSAE16, and ISO 27001. The Pexip Core PoPs consist of redundant Data Centers in Europe, North America, Middle East, Asia and Oceania to handle all media and firewall traversal of devices supported by the Pexip Cloud.

Cloud Services

Pexip maintains some services which are not directly associated with a specific city location. These services include information services for video device provisioning, phone book services, end-user web management tool interfaces, and billing. These services may be hosted from Cloud Service Providers such as the Amazon Elastic Compute (EC2) Cloud. While these CSPs have global accessibility and reach, they are generally associated with the Ireland region of the world.

Other Cloud Services utilized by Pexip include Microsoft Azure and Google Cloud Platform (GCP). There are resources deployed within Azure for the Microsoft Teams Cloud Video Interop (CVI) gateway feature, and in GCP for the Google Hangouts Meet Interop gateway feature. The Azure and GCP locations utilized correlate with existing Pexip PoP locations:

Pexip PoP Location	Ashburn, VA	Amsterdam, Netherlands	Singapore	Sydney, Australia
Microsoft Azure Region	Virginia East US 2	Netherlands West Europe	Singapore Southeast Asia	New South Wales Australia East
Google Cloud Platform Location	N. Virginia us-east4	Netherlands europe-west4	Singapore asia-southeast1	Sydney, Australia australia-southeast1

Information Collection and Use

Pexip collects, uses, protects, and discloses the following information associated with the Pexip Cloud Video Service in accordance with the following discussion, as well as personal data processing found in the Pexip Privacy Policy and the use cookies and similar technologies found in the Pexip Cookie Policy.

Types of Data Stored

Pexip provides a Cloud-based Video Service which enables subscribers the opportunity to register purpose-built video endpoints and software clients to the Cloud for call-control and routing, as well as access to video bridges to facilitate multi-participant collaboration. The Video Service should be considered solely as a secure communications conduit for real-time video and audio traffic between participants, and does not store data regarding participants beyond that which is necessary to uniquely identify them on the Service for the purpose of call processing to initiate, route, maintain, and terminate calls. Call Detail Records (CDRs) are generated by way of the use of the video services, to allow subscribers and their organizations to track call activity, both to confirm appropriate use as well as to permit accurate billing. Pexip itself will use CDRs in aggregate to understand overall macroscopic call trends to aid in decisions on how to evolve the Cloud Service to serve the needs of its customers, and to provide technical support for specific calls when necessary.

To establish the environment necessary for users to consume the Video Service, users will be asked to provide a minimum of information so that they can establish unique identities on the Service for call processing and personal account maintenance. At the individual level, user information includes a name and an e-mail address. At the organization level, information includes contact information for key stakeholders responsible for interaction with Pexip for service announcement, technical, and billing purposes.

Pexip will use the information provided to generate subscriptions on the Video Service for each unique user. Once users begin consuming the Video Service, user credentials, user settings, and call history will be generated which provide a usage profile per individual. Any user credentials, settings, and details generated by the Video Service subsequent to the establishment of the user's unique identity is only locally specific to the Service itself. Access to such data is secure and is only used by authorized persons in support of the Video Service and its subscribers. The following information is a summary of data requested by Pexip. Any additional data accessible by an end-user of the Cloud Video Service is in the form of Call Detail Records which may at most provide high-level visibility to external video parties being communicated with.

Types of data identifying a specific user include:

- First Name, Last Name
- Email address
- Contact Phone Number (only key stakeholders for service, technical, and billing interactions)
- Desired video address

Types of data generated and stored during use of the Video Service may include:

- Type of video device and software level
- Inside and outside IP address assigned to the video device
- Start and stop time for video calls
- Parties the video device initiated calls to, and received calls from
- Media statistics for the video calls (bandwidth use, packet loss, jitter)
- Signaling and media paths used in call establishment and tear-down

Data Encryption and Storage

The default posture for Pexip communications and storage of subscriber data is for security and encryption. For all web-based interactions with the Service, all such communications use HTTPS which is a widely-used communications protocol for secure communication. HTTPS also utilizes the SSL/TLS protocol, thus adding the security capabilities of SSL and TLS when communicating with and managing devices, users, and additional services on the Pexip cloud platform. To ensure privacy and confidentiality, registered subscribers of the Pexip Service define their unique username and password[1]. The sign-up pages are only available over a secure HTTP connection using HTTPS with a valid certificate to ensure that user data and passwords are encrypted before being sent to the central server. To further protect the user data, Pexip has ensured that no user passwords can be read by humans or computers as they are encrypted using Digest (MD5) and SHA256 before being stored at the central server. The only way to restore a user password is to utilize the approved password recovery tool.

The Pexip Service Network is a distributed architecture. As such, user data used to maintain the service and process calls can be collected from multiple points on the Service Network via several Pexip PoPs, as well as within the Amazon EC2 Cloud, Microsoft Azure, and Google Cloud Platform. These PoPs, as well as the Amazon EC2 Cloud, Azure, and GCP, were previously discussed. Ultimately customer data is aggregated and stored at specific locations which will be discussed in the discussion to follow.

A. Customer Personal Details
    - Contact Information (e-mail addresses, phone numbers, names)
    - User login credentials for Web Tools

    This information is stored on servers within the following geographical locations:

    - Pexip Data Centers (PoPs) – Oslo, Norway
    - Pexip Data Centers (PoPs) – Ashburn, VA

B. Customer Video Subscription Details
    - Video subscription credentials and addresses
    - Call Detail Records and subscription details

    This information is stored at Pexip PoPs at the following geographical locations:

    - Pexip Data Centers (PoPs) – Oslo, Norway

[1] The Pexip Cloud uses the zxcvbn password strength estimator to validate acceptable passwords for users of the service.

Data Privacy and Protection

At Pexip, we have always taken individuals' right to data privacy and protection very seriously. We have no necessity to process individuals' personal information beyond what is required for the functioning of our service.

GDPR

With GDPR (General Data Protection Regulation), the European Union is protecting the right to privacy for every EU resident, including residents in the EEA countries. GDPR replaces the 1995 EU Data Protection Directive (European Directive 95/46/EC), effective from 25 May 2018. Pexip is, as of May 25 2018, committed to fulfill the obligations of GDPR. Pexip encourages each of our channels partners to independently familiarize themselves with the GDPR. Each Partner is responsible for ensuring that their business complies with the privacy laws of the jurisdictions in which they operate. Using Pexip as a service provider does not guarantee that a Partner complies with GDPR. GDPR have a global impact, a Partner located outside the EU territory may be subject to GDPR if they operate within the territory and are processing personal data of EU residents.

Controller vs. Processor

GDPR defines two main data privacy and protection responsibilities, Controller and Processor:

- **Controller** - the party that determines the purpose and means of processing personal data
- **Processor** - the party that processes personal data on behalf of the controller

The Pexip Service Partner either collects information from their customers as a controller, then Pexip acts as a processor for the Partner, or the Pexip Service Partner acts as a processor on behalf of its controller, then Pexip acts as a sub-processor.

Privacy Policy

The Pexip Privacy Policy complies with the GDPR requirements, and explains in plain language:
The type of data we collect; How we use the data we collect; Storage of personal data; Personal data and third-parties; Cookies and similar technologies; Protection and security of personal data; Access and control of your personal data.

When enabling a Partner on the Pexip service, the Partner can choose to use their own Terms of Service/Privacy Policy or Pexip's Terms of Service/Privacy Policy directly or white labeled. The processing of personal data is based on acceptance of Terms of Service and Privacy Policy from the user ("the data subject") given at the activation of the user account. If a Partner choose to use their own policies, the Partner is responsible to make agreement with Pexip to ensure both parties are fulfilling the policies if their policies are violating with the Pexip policies. Please note that the Pexip service is defaulted to the Pexip Terms of Service/Privacy Policy if no other policies are enabled on the service for the Partner.

Data Processing Agreements

Pexip's Data Processing Agreement ("DPA") for the Videoconference Service clearly explains and defines our commitments to our Partners regarding GDPR obligations: Pexip acting as the data processor; Compliance with laws; Processing of personal data; Transfer of personal data abroad; Use of Sub-Processors; Security measures and Access control; Data Subjects' Rights; and Partner Audits.

Data Retention

Personally Identifiable Information (PII) data of Call Detail Records (CDRs) are retained for a period of 3 months by Pexip in the Pexip videoconference cloud system. If the Partner downloads and locally processes CDRs, the Partner is responsible to comply with this data retention policy for CDR data.

Data Protection Impact Assessments

Pexip have a formalized process to evaluate the activities where personal data is being processed, and to conduct data protection impact assessment (DPIA) when such processing activities is likely to result in a high risk to individuals' privacy rights.

Personal Data Breach Reporting

Under GDPR, processor must notify the controller without undue delay after becoming aware of a personal data breach resulting from a breach of the processors' security. Pexip is committed to ensure that the Partner of the affected individuals is notified according to the Pexip data breach policy.

Data Subject Rights

GDPR is all around the individuals' rights to have control how their personal data is being processed. There are several rights the data subject can request: the right to access; the right to rectification; the right to be forgotten; the right to restriction of processing; the right to data portability; the right to object; the right to appropriate decision making; the right to lodge a complaint. Pexip shall to a reasonable degree, considering the nature of the processing, assist the Partner for making possible the fulfilment of the Partner's obligations to responding to data subjects' requests.

Data Protection Officer

Data Protection Officer (DPO) duties are managed within Pexip by dedicated resources which governs the Pexip privacy compliance. Privacy questions for Pexip can be directed to privacy@pexip.com.

Privacy Laws

Personal data as described earlier is processed as per the following privacy laws:

- Pexip performs services for our partners which involves processing of personal data and Call Detail Records (CDRs) and thereby acts as a Data Processor pursuant to the General Data Protection Regulation (EU 2016/679) ("GDPR") Article 4 (8).

- Any processing of personal data shall ensure that the parties' obligations under the EU GDPR on Privacy (EU 2016/679) and the Norwegian Personal Data Act of 15 June 2018 no. 38 ("the Personal Data Act") are fulfilled.

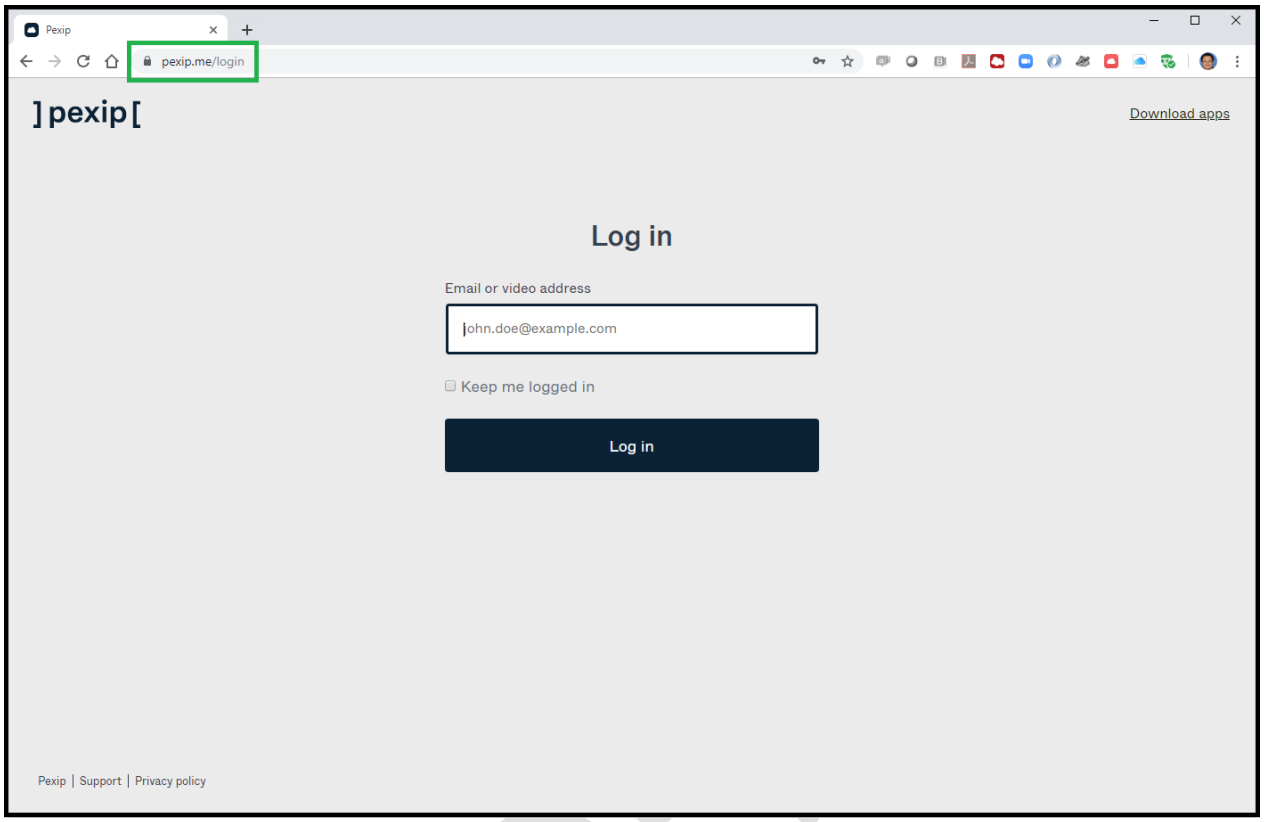
- CDRs, including collection, registration, collocation, storage, disclosure or a combination of these (as described in the Privacy Policy) are accessed from a secure datacenter in Norway, and access complies with the GDPR and the Norwegian Personal Data Act.

Access to Data

Access to the infrastructure and raw data in the Pexip Cloud itself is limited to Pexip Development Operations (DevOps) and Technical Support Escalation staff. These staff members may access elements of the Pexip Service via VPN and subsequent to that, secure terminal sessions via SSH, and Web-based UI sessions via HTTPS. Access to information is controlled by the principle of least privilege, which requires that users have only the minimum access rights necessary to fulfill their responsibilities.

Access to Call Detail Records (CDRs) and video device registration data is accessible both to Pexip staff as well as reseller partners of Pexip for the purposes of supporting end-user subscribers of the Cloud Video Service. These designated persons may access the data via Web-based UI sessions via HTTPS, coupled with a mandatory Two-Factor Authentication (2FA) mechanism employing a scanned Quick Response (QR) Code tied to the user's work e-mail address and a random access code regenerated every 30 seconds. Using such a secure access strategy, it is ensured that only authorized parties can authenticate and gain access to end-user subscriber data.

The primary end-user management interface for accessing user data is a Web-based tool known as MyPages (https://pexip.me). Via this tool, an end-user may review their own profile and usage history, or if set with administrator privileges for their own whole organization, may review the profile and usage history for their entire population of subscribers of the Pexip Service. The MyPages tool provides an authenticated (signed-in) user access to such data via HTTPS.



Sign-in via the MyPages webtool also supports Single Sign On (SSO) capability, where an end-user's e-mail or video address may be validated against a corporate Identity Provider (IdP) to confirm that the user is authorized to have access to a video subscription on the Cloud Video Service. Current SSO capabilities use SAML 2.0 as the foundation technology and have been tested to support G-Suite, PingFederate, Azure AD, Shibboleth, and ADFS Identity Providers.

Video Device Registration

Privacy of communications using SIP TLS and SRTP

The Pexip Service supports direct registrations of software-based (softclients) and hardware-based (endpoints) video devices from several vendors, providing Cloud-based call control, processing, and interworking for signaling and media. The native signaling protocol used by the Service is SIP, and security is enforced by requiring encrypted signaling via SIP TLS. For video and audio media, the payload is encrypted to AES-128 standard, resulting in Secure Real Time Transport (SRTP) media streams.

The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. Pexip ensures privacy of all audio and video calls by enabling (by default) encrypted signaling using SIP TLS and encrypted media using Secure Real-time Transport Protocol (SRTP) for all communications on audio and video.

SIP TLS works in the same way as HTTPS, which we use daily on a secure webmail access or online banking access, meaning that the overall security model of SIP TLS is based on the digital certificate verification process.

For Pexip subscribers this enables endpoints to connect to the Pexip cloud using a connection with TLS (IETF standard 5246) protected socket by using X509v3 digital certificates (IETF standard 5280). The certificates are released, verified and uploaded by Pexip employees to ensure correct validation against clients on the Pexip service.

SIP signaling communication over TLS provides a great value as it hides access to any sensitive information from any unauthorized third party and provides a secure method of exchanging keys for SRTP media encryption which ensures privacy of all data (audio, video and presentations) sent using the Pexip service.

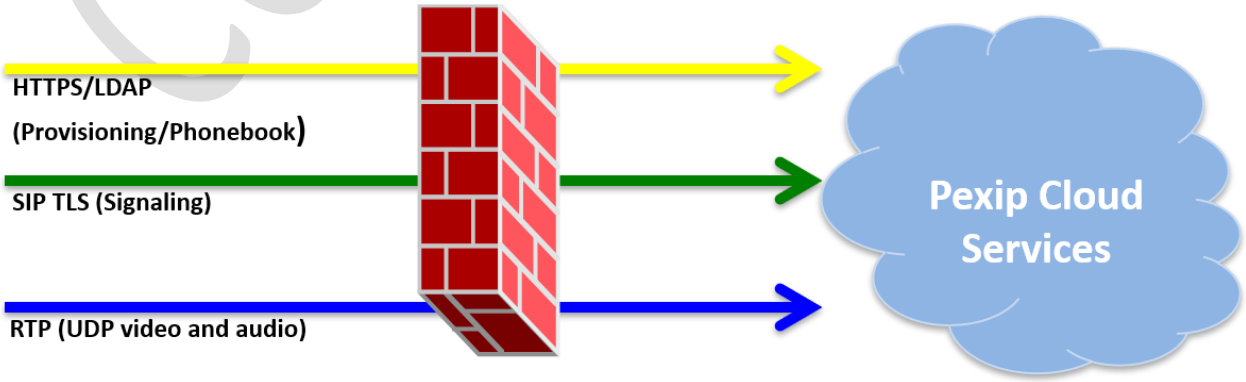
For encryption and decryption of the data flow (and hence for providing confidentiality), SRTP (together with SRTCP) utilizes AES as the default cipher.

Firewall Traversal Support

To enhance security Pexip recommends installing and using any devices on the Service behind a corporate firewall in order to protect the devices from direct Denial of Service attacks (DoS) and other un-authorized access.

The Pexip Call Control Service has been designed to counter with the various SIP attacks on the Internet and protect and filter these attacks from any of the devices that are enabled on the Pexip service and traffic is automatically monitored to identify suspect traffic patterns and violation of service or breach of policy.

The Pexip Service provides native Firewall Traversal Support for softclients and endpoints registered to the Cloud Service. Such video devices are provisioned and configured to seamlessly operate from behind the corporate firewall, eliminating the need to place the device on an Internet-routable public network.



Safe behind the corporate firewall, video devices are protected from intrusion and directed Denial of Service (DoS) attacks. To reduce the complexity of the end-user devices, the Pexip Call Control Service has a dynamic implementation of Traversal Using Relay NAT (TURN) for real-time voice & video traversal. This ensures a secure way of traverse firewalls as well as support for the widest range of software versions of the supported devices and software clients. The Pexip Call Control Service is designed to work with all primary type of firewalls; full cone NAT, restricted cone NAT and port restricted cone NAT.

For details about the ports and services used by the Pexip Service, please visit https://pexip.me/test/firewall to review the Firewall Rules tables to get the latest information. When reviewing the Firewall Rules tables, it is useful to consider the following:

a. Any firewall rules which need to be explicitly configured to permit communications to the Pexip Service Network need only be configured from the inside private network towards the Pexip Cloud on the outside. The Pexip Service Network will not unilaterally contact devices, so no firewall rules explicitly permitting traffic from the outside towards the inside need to be declared. Communication paths between the two networks are initiated from the inside private network towards the Service Network, and are then maintained via a keepalive exchange process.
b. The destination IP address ranges used by the Pexip Service Network belong to Pexip itself. Current services maintained by Pexip, as well as additional services which will be added over time, will be served from these IP address ranges. If firewall rules are defined which accommodate the full set of address ranges conveyed by the Firewall Rules tables, an organization will only have to make the declarations once and they should be future-proofed for changes to the Pexip Service Network as it evolves.

Video Device Parameters and Firmware

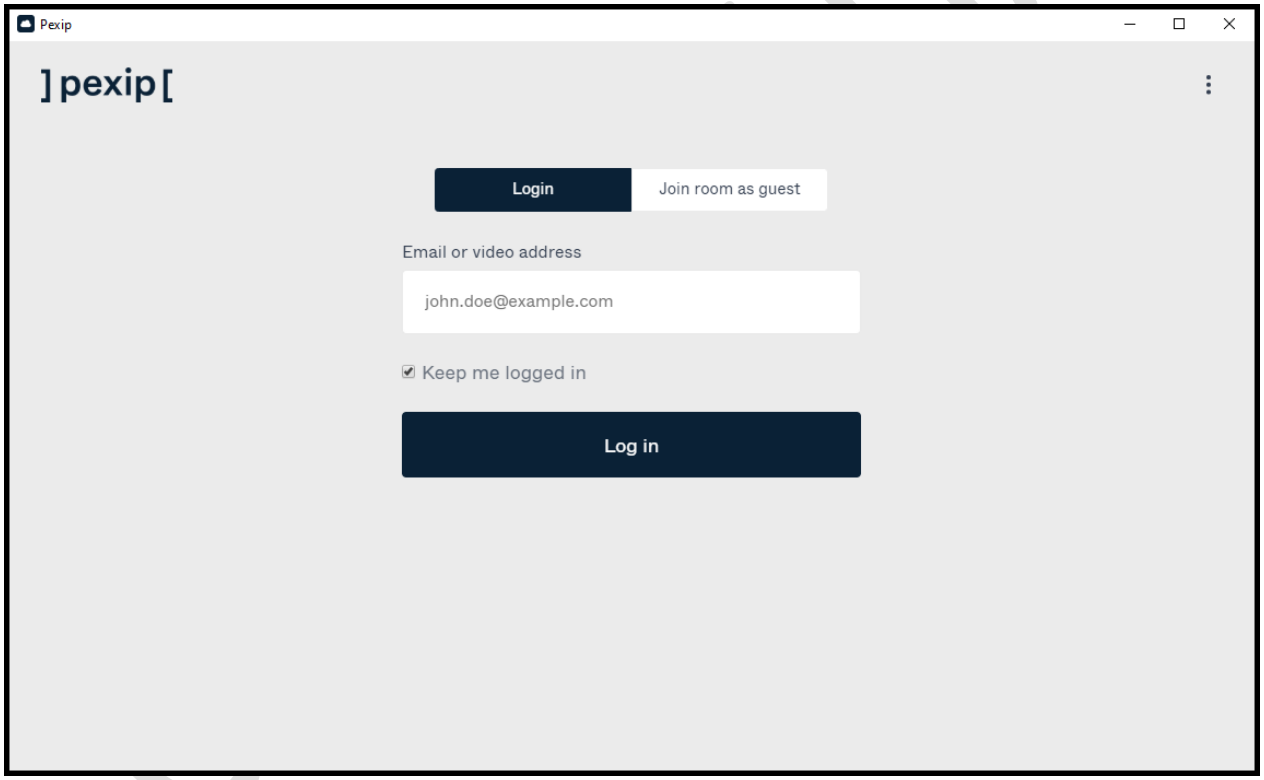
The Pexip Service Network will only configure sufficient settings on a registered video device to provide it with the necessary characteristics to operate on the Cloud Video Service. These settings include parameters to uniquely identify it on the Service Network, and to set its calling profile. Parameters which are set include:

a. Display Name
b. SIP URI video address
c. Encryption support
d. Maximum transmit and receive bandwidth
e. Company Phonebook address
f. Network Time Protocol (NTP) server address
g. PoP (SIP Proxy) to use
h. Heartbeat timing intervals for check-in

The Pexip Service Network leaves the management of video device firmware levels to the end-user, so that the end-user can maintain the User Interface they prefer. The Pexip Service Network does require that the device firmware levels are above the minimum version level required for direct registration support to the Cloud Video Service, and it does recommend that firmware levels used should include fixes for known security vulnerabilities.

My Meeting Video Softclient Sign In

The video software client native to the Pexip Cloud Video Service is a self-authored application named My Meeting Video (MMV), available for the Microsoft Windows and Apple Mac OS Desktop, as well as Android Smartphone/Tablet, and iphone/iPad (iOS) mobile device platforms. Subscribers of the Pexip Service can sign in using their e-mail address or video address, and their password, to register to the Cloud Service to initiate or receive video calls.



Sign-in to MMV supports Single Sign On (SSO) capability, where an end-user's e-mail or video address may be validated against a corporate Identity Provider (IdP) to confirm that the user is authorized to have access to a video subscription on the Cloud Video Service. Current SSO capabilities use SAML 2.0 as the foundation technology and have been tested to support G-Suite, PingFederate, Azure AD, Shibboleth, and ADFS Identity Providers.

Call Scenarios and Security Posture

Communication with external video communities is a core strength and a value of the Cloud Video Service. As such the philosophy of the Pexip Service is to provide the highest likelihood of a successful connection. Given this position Pexip does permit encryption-capable video devices on the Cloud Video Service to communicate with outside parties who cannot support encryption, whether by design or due to capability limitations. It is important to understand the various possible call flows, and the encryption situations that may result.

Point-to-Point Calls

The Pexip Service supports Point-to-Point (PtP) calls within the community of subscribers directly registered to the Cloud Service, as well as calls between a subscriber and an external party.

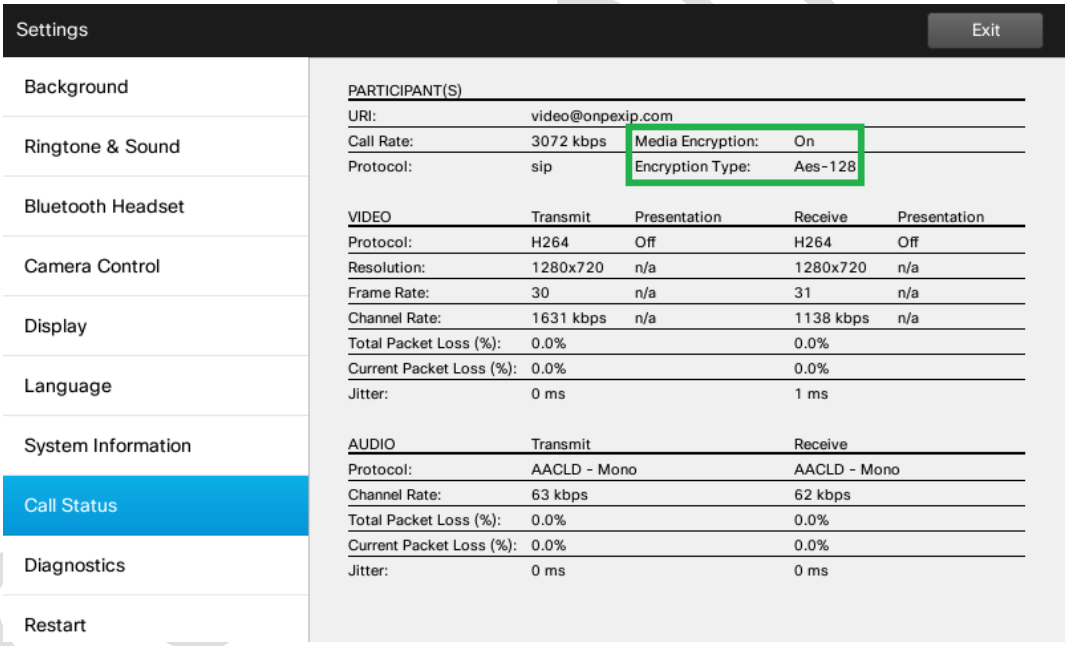
On Net

For PtP calls within the community of subscribers directly registered to the Pexip Service Network, all call-legs are guaranteed to be encrypted. There is a requirement that video devices registered to the Service Network be able to support SIP TLS signaling and that media support SRTP to AES-128 encryption standard. All signaling and media between each stage (hop by hop) in the end-to-end call flow will use encryption.

Off Net

For PtP calls with an external party, the Pexip Service will interwork with external SIP and H.323 video devices. SIP-only calls will be connected via the SIP Proxy Server the Pexip Cloud subscriber is registered to. SIP-to-H.323 calls will be connected via the SIP Proxy Server the Pexip Cloud subscriber is registered to, as well as an interworking gateway which translates between the SIP and H.323 environments. The interworking gateway is capable of supporting H.235 secure signaling, as well as SRTP. If a PtP call with an external party is conducted, if the external party can support encryption, all signaling and media between each stage (hop by hop) in the end-to-end call flow will use encryption. If the external party is not capable of encryption, the call will be allowed to connect, but the call-leg between this external party to the closest stage in the end-to-end call flow will be unencrypted. It is incumbent on the Pexip Cloud subscriber to review their video device's User Interface to understand if encryption is active or not, and then to decide whether the conversation should proceed. Typical indications of the encryption status of a call can be found as a visual cue on the video display as a lock symbol, or via the media statistics page for the device.


Security Watch
04:21 pm
29:51
Pexip TV Station (08493261)
Preview PC
Add
Keypad
Hold
Transfer
End


Settings
Exit
Background
Ringtone & Sound
Bluetooth Headset
Camera Control
Display
Language
System Information
Call Status
Diagnostics
Restart
PARTICIPANT(S)
URI: video@onpexip.com
Call Rate: 3072 kbps
Protocol: sip
Media Encryption: On
Encryption Type: Aes-128
VIDEO Transmit Presentation Receive Presentation
Protocol: H264 Off H264 Off
Resolution: 1280x720 n/a 1280x720 n/a
Frame Rate: 30 n/a 31 n/a
Channel Rate: 1631 kbps n/a 1138 kbps n/a
Total Packet Loss (%): 0.0% 0.0%
Current Packet Loss (%): 0.0% 0.0%
Jitter: 0 ms 1 ms
AUDIO Transmit Receive
Protocol: AACLD - Mono AACLD - Mono
Channel Rate: 63 kbps 62 kbps
Total Packet Loss (%): 0.0% 0.0%
Current Packet Loss (%): 0.0% 0.0%
Jitter: 0 ms 0 ms

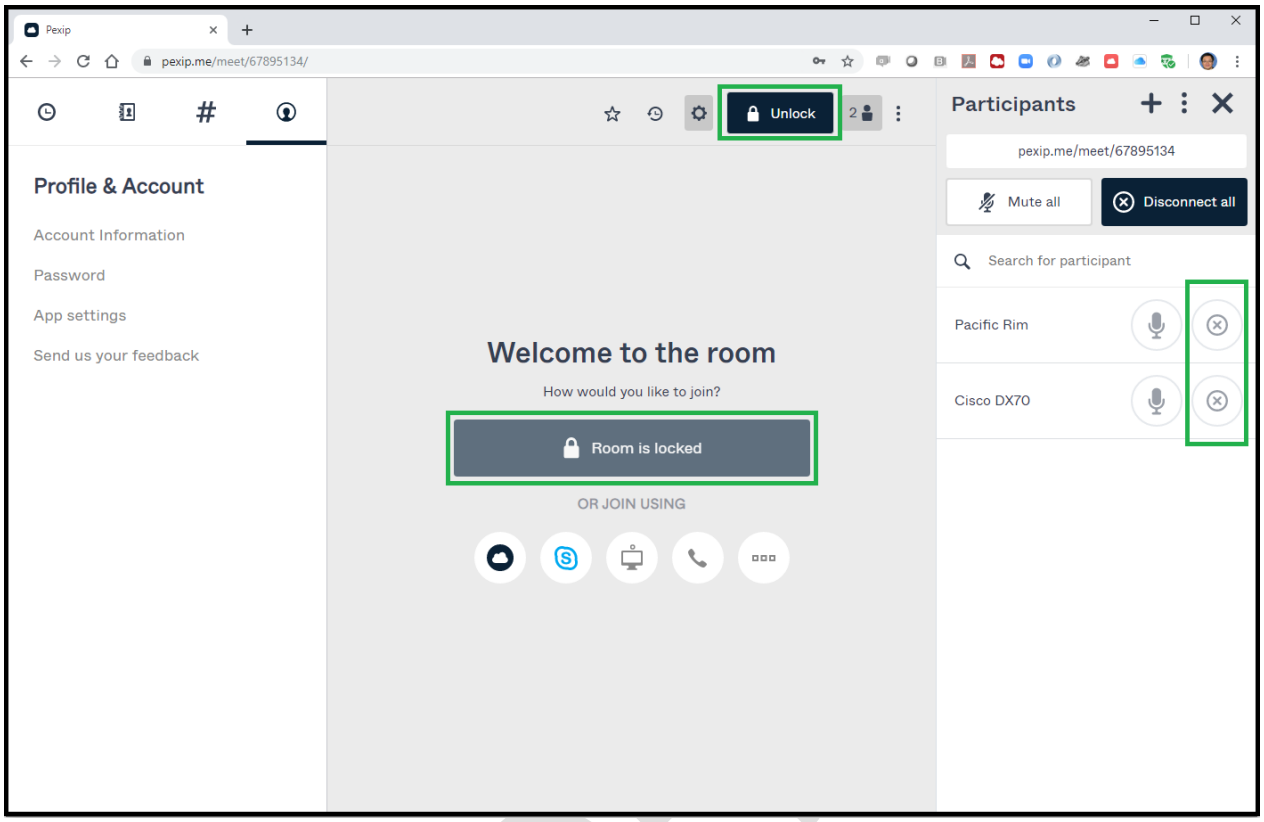
Virtual Meeting Room Calls

In addition to Cloud-based registration of video devices, the Pexip Service also provides for Cloud-based video bridges known as Virtual Meeting Rooms (VMRs). VMRs provide the capability for multiple participants to meet together to collaborate, as well as serve as the platform for interoperability between disparate video-enabled and audio-only communities including standards-based H.323/SIP participants, Skype-for-Business (S4B) participants, WebRTC participants, and PSTN dial-in calling parties.

The current posture for VMRs is to negotiate encryption with participants if the party can support this capability. Each party connected to a VMR port can be considered to be a PtP call between itself and the Multipoint Control Unit (MCU) resource handling the call for the VMR. As such, if the party can support encryption then each of the call-legs between the participant and the VMR will be encrypted. That is, all signaling and media between each stage (hop by hop) in the end-to-end call flow will use encryption. If the party cannot support encryption, the participant and the VMR will be allowed to connect but the connection between the party and the nearest stage in the end-to-end call flow will be unencrypted. PSTN dial-in participants, by virtue of the technology being used, will join VMR calls as an unencrypted audio-only participant.

Securing VMR Calls

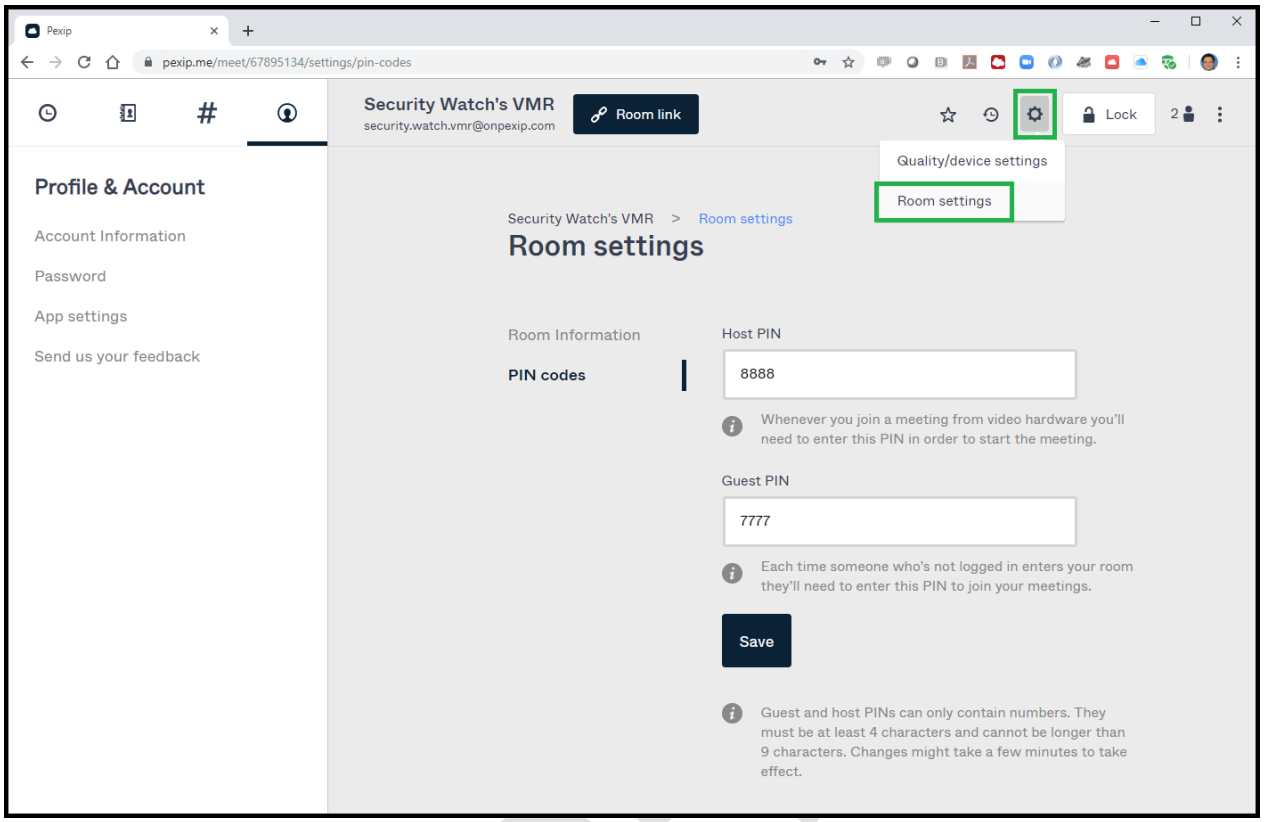
The Pexip Service provides an end-user tool for managing VMRs. This tool, known as MyPages (https://pexip.me) provides an authenticated (signed-in) Host of the VMR to review the participant roster on an active VMR session and provides the capability to eject individual participants and/or to lock the entire session so that no new participants can join. This administrator of the VMR session can review and manipulate the participant roster until they are satisfied that the participants assembled meet the security and attendance requirements for the meeting to proceed, and then lock the session until the meeting is concluded.



VMRs also support the configuration of Host and Guest PIN codes to restrict access. The following combinations are supported:

Host PIN Set	Guest PIN Set	VMR Access
None	None	Everyone joins the VMR directly
Yes	None	Everyone waits in the VMR lobby until the Host enters the PIN
Yes	Yes	Everyone must enter a PIN, and the VMR session begins when the Host is present

The Administrator of the VMR can use the MyPages tool to change the PIN codes at will, so that each new VMR session could have a unique Host and Guest PIN profile. Only participants who have knowledge of the appropriate PIN codes will be able to enter the live VMR session, while other calling parties will only see an intercept VMR landing page asking that a valid PIN be entered. If no valid PIN is entered the calling party will be disconnected after a short time out period.



VMR Participants, On Net

Within the community of subscribers directly registered to the Pexip Service Network, calls from these participants to a VMR are guaranteed to use encryption. There is a requirement that video devices registered to the Service Network be able to support SIP TLS signaling and that media support SRTP to AES-128 encryption standard. All signaling and media between each stage (hop by hop) in the end-to-end call flow will use encryption.

VMR Participants, Off Net H.323/SIP

As discussed earlier regarding PtP calls with an external party, the Pexip Service will interwork with external SIP and H.323 video devices. An external party calling to a VMR as a participant is viewed as a PtP call between the external party and the MCU resource handling the call for the VMR. If the external party can support encryption, this VMR connection will be encrypted along each stage (hop by hop) in the end-to-end call flow. If the external party is not capable of encryption, the call will be allowed to connect, but this VMR connection will be unencrypted on the call-leg between the party and the nearest stage in the end-to-end call flow.

VMR Participants, Skype for Business

Microsoft Skype-for-Business (S4B) users are able to meet with Pexip Cloud Service subscribers by using the capability of the Pexip VMR to act as an interoperability bridge. Both On-Premises and Office 365 (Cloud-based) S4B installations are supported by the Pexip Service, and once the external S4B domain has federated with Pexip's own S4B environment, external S4B users can dial a simple URI address to meet other participants on a VMR. As in other situations involving an Off Net party, the encryption status of this call-leg to a VMR is dependent on the encryption capabilities of the S4B user. It has been observed however, that current modern installations of S4B do typically support encryption.

VMR Participants, Web Browser Based

The Pexip Cloud Service supports web browser-based video users on multiple browser platforms, and allows these users to meet and collaborate with others on VMR calls. Pexip leverages the native support for WebRTC technology in the Google Chrome, Mozilla Firefox, and Opera web browsers, and provides web browser plug-ins for Microsoft Internet Explorer and Apple Safari. The web browser video interface for end-users is via the Web-tool known as MyPages (https://pexip.me), which provides for a common look and feel regardless of the specific browser being used. As the web browser-based video service is managed by a Pexip-authored Web-tool, it can be assured that these calls to a VMR are encrypted and secure.

PSTN Dial-In Parties

The Pexip Service allows PSTN dial-in connectivity to VMRs. Due to the legacy nature of the technology, the traffic from these parties is not secure. The Administrator of the VMR will need to review the participant roster to determine if any dial-in PSTN participants have joined the VMR session, and determine if the participant should be allowed to remain connected or not.

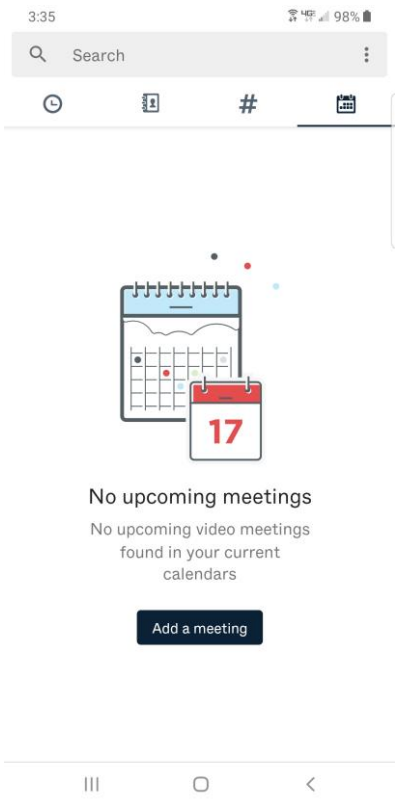
VMR Participant Encryption Summary

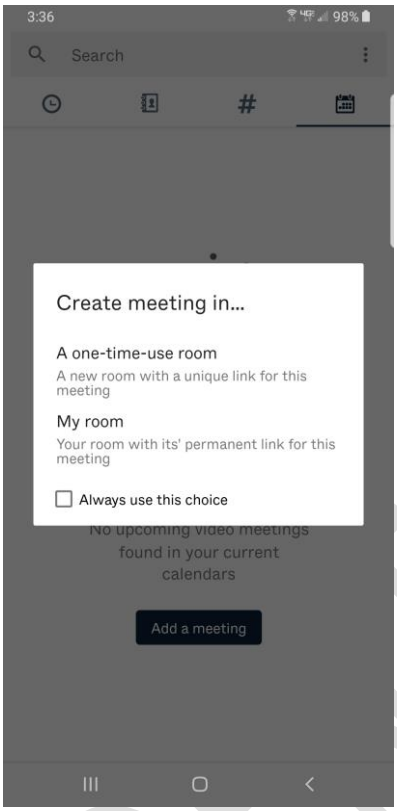
The following table provides guidance on the encryption expectations for various participant categories:

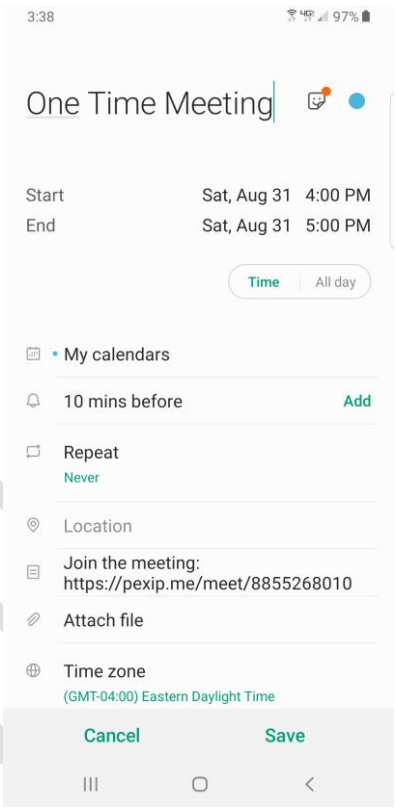
Participant Type	Encryption Status	Encryption Technology
On Net, Registered Softclients and Endpoints	Encrypted	SIP TLS signaling Secure RTP (AES-128)
Off Net, External H.323/SIP Softclients and Endpoints	Dependent on capabilities of external party	SIP TLS or H.323 H.235 signaling Secure RTP (AES-128)
Skype for Business (Lync)	Encrypted	SIP TLS signaling Secure RTP (AES-128)
Web Browser (WebRTC and Plug-In)	Encrypted	Secure HTTP signaling Secure RTP (AES-128)
PSTN Dial-In	Unencrypted	N/A

One-Time Use VMRs (Dynamic Conference IDs)

The Pexip VMR Service also supports the generation of One-Time Use VMRs, where the Conference ID of the VMR is dynamically generated and cannot be predicted *a priori* by parties who have not been invited to the meeting. At the time a meeting invitation is to be generated the Pexip subscriber is given the option of creating an invitation using the dial-in details for their regular persistent/static VMR, or to choose to generate dial-in details for a One-Time Use VMR. Each One-Time Use VMR is an unknown meeting room to parties who do not have the dial-in details, hence making the meeting room private. The One-Time Use VMR can be locked during the live meeting, and the meeting administrator can review the participant list and eject individual parties as before.

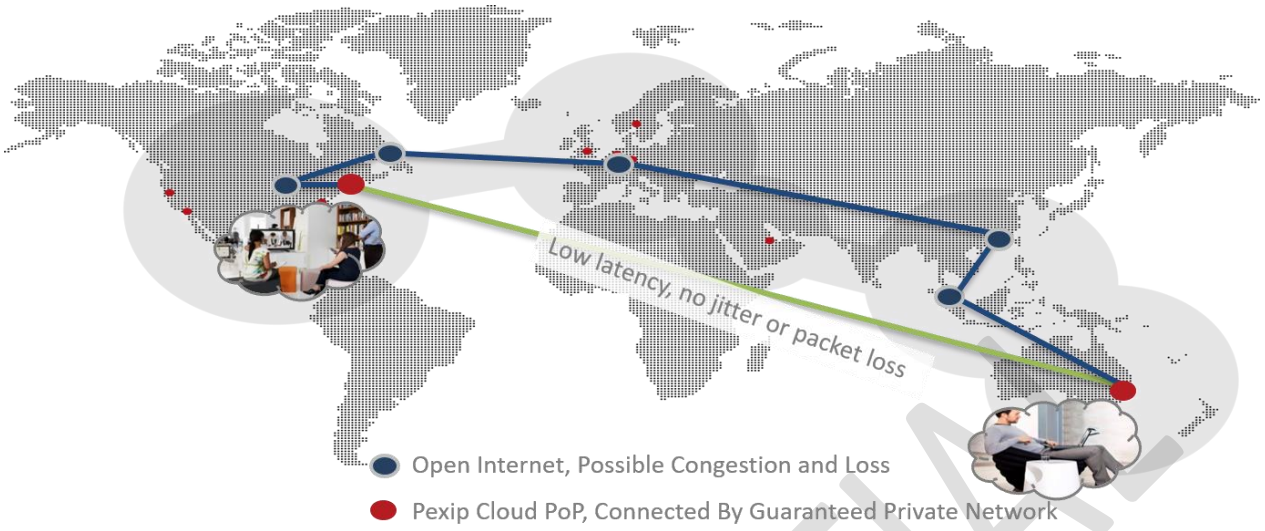






Geographies Traversed by Pexip Cloud Traffic

The Pexip Cloud-based Video Service is deployed via a global network of Points-of-Presence (PoPs) for call-centric video signaling and media, as well as non-call-centric services for phonebook directory, provisioning, billing, and monitoring capabilities. Together, these call-centric and non-call-centric services are orchestrated in unison to deliver robust, high-availability, and high-quality services to a global subscriber population. As traffic has the possibility of traversing international boundaries, it is important to understand the various traffic flows and geography considerations.

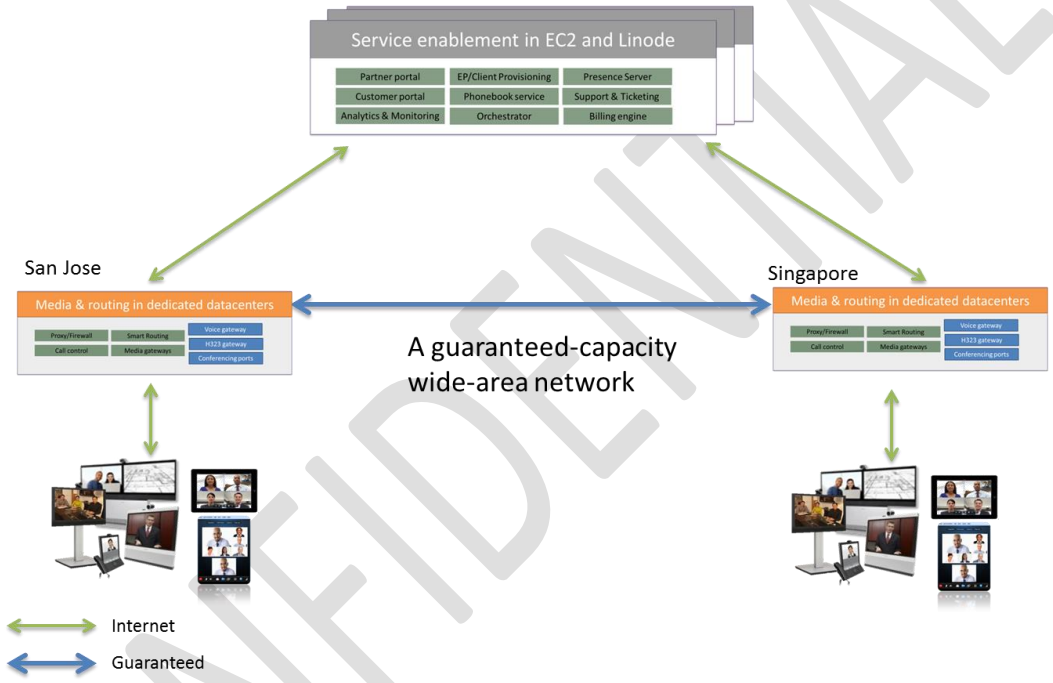


Media-Centric Services

Pexip PoPs are distributed around the globe and provide a number of services including video device registration, call signaling relay, media processing for PtP and VMR calls, and interworking between disparate video technologies. Pexip PoPs are hosted at Data Centers managed by well-known facility service providers such Equinix, Q9, and SoftLayer, and are interconnected via a private dedicated QoS network providing low jitter, delay, and packet loss profiles for traffic. Each of the facilities has multi-factor security for access, including human security, security cameras, photo identity card access, key access to the equipment rack, and the like. Each facility is compliant with well-known security compliance standards such as SOC2 and SSAE16. The Pexip Core PoPs consist of redundant Data Centers in Europe, North America, the Middle East, Asia and Oceania. The Data Centers (our Core PoPs) can operate together or separately to create full redundancy, providing for a robust and high-availability call service.

Non-Media-Centric Services

To provide services for non-media-centric traffic – primarily not time-sensitive transactions – Pexip also maintains information systems which are not localized at a specific PoP but are instead distributed in high-availability Cloud Services. Such Information Systems include the provisioning service for endpoints and softclients, the phonebook service, various web-based portals for account management, and the billing service. Such services are hosted on servers running in the Amazon Elastic Computer (EC2) Cloud. These Information Systems use triple redundancy with 2 availability zones in Amazon EC2. All services are synced and hot swappable.



Typical Traffic Flows

Video Device Registration

A video endpoint or softclient will begin its registration process by contacting the Pexip provisioning service, hosted in Amazon EC2. The provisioning server will process the incoming request, determine which PoP in the world is closest and hence best to register to, and then provide the requesting video device with its unique profile on the Cloud Video Service. Subsequently the video device will contact the appropriate PoP, authenticate itself to it, and register. The video device will maintain connectivity with the PoP via an exchange of keepalive traffic, as well as periodically check in with the provisioning service to determine if there are profile modifications to be applied.

Given the process described above, the following can be said regarding traffic between the video endpoint or softclient to be registered to the Cloud Video Service:

a. Provisioning request traffic will be exchanged between the video device in its local geography, to provisioning servers which are hosted in the Amazon EC2 Cloud. This Cloud service is within the general geography of Ireland.
b. Registration and keepalive traffic will be exchanged between the video device in its local geography, to the PoP closest to it. For video devices within a large country such as the United States or Canada, it is probable that the device and the PoP will share the same national boundaries. For users in other locales, it is possible that the closest PoP resides across one or more national borders.

Point-to-Point Calls

Calls between two registered video devices on the Pexip Cloud Video Service are conducted as relays of signaling traffic handled by one or more devices, and transfer of media traffic between one or more PoPs. The following can be said about this call flow:

a. The first SIP signaling traffic will be between the calling party to the PoP it is registered to.
b. The first relay of SIP signaling will be between the calling party PoP to the closest upstream SIP relay node.
c. The SIP relay node will redirect the signaling to the PoP where the called party was last known to be registered.
d. The final step in the SIP signaling sequence will be to alert the called party. This is SIP signaling traffic between the called party and the PoP it is registered to.
e. An answer will be signaled along the same path, in reverse, as indicated in steps (a) through (d).
f. Media will flow directly between the PoPs, over the guaranteed bandwidth QoS network.

Depending on the location of the calling and called parties, the signaling and media traffic may traverse national boundaries. If the two parties are within a large country such as the United States or Canada where one or more PoPs are located, call signaling and media will stay within the borders of the country. As previously discussed in the section on Call Scenarios, this call flow is considered On-Net and will be guaranteed to use encryption technology along each stage (hop by hop) in the end-to-end call flow.

Direct calls between a registered video device on the Pexip Cloud Video Service and an external party are conducted in a similar manner to two directly registered video devices. Instead of a second PoP the handling of the signaling and media may be processed however, by an interworking gateway within the Service Network if there is a protocol translation required. As the Pexip Service will perform path optimization to provide the best media quality experience, this interworking gateway will be invoked at a geographical location closest to the external party, and hence signaling and media may traverse national boundaries. As previously discussed in the section on Call Scenarios, this call flow is considered Off-Net and will use encryption technology along each stage (hop by hop) along the end-to-end call flow so long

as the external party can support encryption. If the external party cannot support encryption, the signaling and media from the external party to the closest PoP or interworking gateway will be unencrypted, while the signaling and media flows completely managed within the Pexip Service Network will be encrypted.

Virtual Meeting Room Calls

Multi-party video calls conducted on Virtual Meeting Rooms (VMRs) can be looked upon as multiple Point-to-Point calls between participant video devices to Multipoint Control Unit (MCU) resources. These PtP calls are all stitched together via the fabric of the Pexip Service Network to provide a single bridging experience. The overall security of the VMR session is dependent on the types of participants who join the meeting.

a. For VMR sessions where all participant video devices are directly registered to Pexip, all participants use encryption by virtue of the requirement for such devices to use secure signaling and media.
b. For VMR sessions where there are participants who cannot support encryption due to device limitation or by design, the call-leg between each such participant to the VMR is unencrypted.
c. For VMR sessions where there is a PSTN dial-in participant, this technology does not support encryption, and hence this call-leg is unencrypted.

Signaling and media flows for VMR sessions can be analyzed by reviewing the types of participants and geographies they are located at. For calls involving participants located in multiple countries, it is clear that signaling and media traffic will traverse national boundaries. For VMR sessions where the participants are located in a large country such as the United States or Canada where one or more PoPs are located, signaling and media will be contained within the borders of the country.

As previously discussed in the Call Scenarios and Securing VMR Calls section, the VMR session can be managed via the MyPages (https://pexip.me) end-user tool to ensure that only appropriate participants are permitted to continue in the meeting. The VMR Administrator can review the roster of meeting participants, remove the participants who should not be present, then lock the VMR session to prevent new users from joining.

Live Streaming and Recording Feature

The Pexip VMR Service provides the capability for subscribers to configure integration with external 3rd-party streaming and recording services. Using this feature a VMR meeting administrator can efficiently deliver meeting content to a mass audience, as well as record and distribute it for archival purposes. Security compliance groups within the Enterprise interested in the security posture of this streaming and recording feature can be assured that:

(1) The Pexip Streaming and Recording feature simply serves as a mechanism by which a user can send media traffic from a Pexip Virtual Meeting Room (VMR) to a compatible Streaming Ingestion Service so that it can reach a mass audience. If the Ingestion Service also supports recording, the Streaming and Recording feature can also be used to record and archive the VMR meeting session.

The Streaming and Recording capability is not enabled by default for a Company and the video subscribers under that Company. The end-client must order the Streaming and Recording capability to be enabled for configuration setup, and then each individual video subscriber would need to manually set up the Streaming and Recording integration to a supported Streaming Ingestion Service prior to being able to use the Streaming and Recording capability.

When the Streaming and Recording capability is used on a live VMR meeting, there is a clear visual indication on the VMR session itself ensuring that everyone on video in the meeting knows that the session is being streamed and possibly recorded.

When the Streaming and Recording capability has been enabled and the video subscriber has set themselves up to be able to stream to a supported Streaming Ingestion Service, the video subscriber must consciously start the streaming session manually (ad-hoc) or by scheduling the start and stop times for the streaming session. Even in the case of a scheduled start/stop time for a streaming session, the video subscriber must press a button to confirm and begin the streaming session. There is no situation where the streaming session begins automatically; someone is always consciously choosing to start the streaming session.

(2) The Pexip Streaming and Recording feature uses the MCU platform supporting the Pexip VMR Service to send out to compatible Streaming Ingestion Services using Real-Time Messaging Protocol (RTMP) or Secure RTMP (RTMPS) traffic.

More information about RTMP and RTMPS can be found here. RTMP and RTMPS are common protocol types used for streaming purposes.

Each of the Services the Pexip Streaming and Recording Service has been validated with are listed here. Each of these Services has their own security and privacy policies that users would have to agree to. These are not influenced by Pexip.

(3) The Pexip Streaming and Recording feature's tightest integration is with YouTube Live! This is because YouTube, owned by Google, is familiar to a great many people who are familiar with its use, and there are well-documented instructions on how to use it for Streaming and Recording.

The steps to set up Streaming and Recording integration from Pexip MyPages with the YouTube Live! Service are documented here. Integration steps for other Streaming Ingestion Services are documented here.

The instructions from YouTube itself detailing how to set it up for Streaming and Recording are here.

The Streaming and Recording integration between Pexip MyPages and YouTube Live! sets up the recorded YouTube videos as having an Unlisted Privacy setting. This means that the video subscriber who owns the content from the VMR meeting session has a YouTube URL to distribute as they see fit for the intended audience. The video cannot be found via a search on YouTube unless the owner later decides the make the video Public. The owner also has the option of signing into YouTube and marking the video completely Private, or downloading and then deleting the recorded video so that it no longer exists in YouTube's Cloud. The owner can then take the downloaded video and archive/distribute the recording as they see fit. More about YouTube video privacy settings can be found here.

(4) If none of the common Streaming Ingestion Services listed in Section (2) above are acceptable, the video subscriber/client can choose to use their own Streaming Ingestion Infrastructure that they manage and have direct control over. If the video subscriber/customer using the Streaming and Recording feature wants to provide their own Streaming Ingestion Service rather than one of the Cloud-based options we have tested with and know we can support, they can configure MyPages and its Streaming and Recording capability to send the media stream from the VMR to an Enterprise's private Streaming Ingestion Service so long as it is publicly reachable over the Internet. The video subscriber/customer would need to manually configure a custom Streaming and Recording profile in MyPages to point to the private Streaming Ingestion Service.

Microsoft and Google Gateway Services

The Pexip Service provides video gateway services for Microsoft and Google video environments which provide the capability for external calling parties using non-native video technologies to join meetings. To elaborate, if it was desirable to hold a meeting on a Microsoft Skype for Business or Teams bridge, or a Google Hangouts Meet bridge, while still allowing external parties to join using traditional standards-based SIP/H.323 video devices, the Pexip Service can facilitate this call workflow. In these workflows, the Pexip Service continues to operate under the understanding that the gateway capability simply provides a secure conduit for information exchange, with no sensitive information persisting once the call is over.

(1) The only data which is collected or generated follow the guidance as discussed in the "Data Types and Storage" section of this paper.

(2) The encryption status of calling parties follow the guidance as discussed in the "Call Scenarios and Security Posture" section of this paper for "Point-to-Point Calls". That is, if the calling party is "On Net" and registered to the Pexip Service then encryption is enforced and guaranteed along each stage (hop by hop) in the end-to-end call flow. For "Off Net" entities if the calling party supports and negotiates encryption the Gateway Service will honor it. If the "Off Net" calling party does not support encryption capabilities the Gateway Service will still connect the call, but the end-to-end connection will not be secure.

(3) Guidance on geographies traversed by signaling and media follow the discussion in the "Geographies Traversed by Pexip Traffic" section of this paper, with the following additional detail:

Gateway Service Type	Calling Party Requirements	Signaling and Media Handling
Microsoft Skype for Business	Endpoint registered to the Pexip Service	Endpoint signaling and media follow guidance in the "Geographies Traversed by Pexip Traffic" section of this paper. Gateway transcoding resources located at Pexip PoPs discussed in "Data Types and Storage" section.

Gateway Service Type	Calling Party Requirements	Signaling and Media Handling
Microsoft Teams	Endpoint or softclient registered to the Pexip Service	Endpoint signaling and media follow the guidance in the "Geographies Traversed by Pexip Traffic" section of this paper. Microsoft requires Teams Connectors to be located in Azure. Currently Pexip has Teams Connectors and gateway transcoding resources located in: • West Europe (Amsterdam) • US East 2 (Virginia) • Australia East (New South Wales, close to Sydney) • Southeast Asia (Singapore) These locations closely mirror existing Pexip PoP locations, so that the network path bridging the Pexip Service Network to Azure has minimal exposure over the open Internet. Signaling and media traffic will use the closest geographical PoP and Azure resources.
Microsoft Teams	External party with own call control service	External calling parties still take advantage of the Pexip Service Network, in that to access the Gateway Service they will locate and ingress the Service Network at the closest Pexip PoP location. They will then travel over the Pexip protected QoS network before egressing at the closest set of Azure resources which support the gateway service to Microsoft Teams.

Gateway Service Type	Calling Party Requirements	Signaling and Media Handling
Google Hangouts Meet	Endpoint or softclient registered to the Pexip Service	Endpoint signaling and media follow the guidance in the "Geographies Traversed by Pexip Traffic" section of this paper. Gateway transcoding resources are located in Google Cloud Platform locations aligned with the Azure locations used for the Microsoft Teams Gateway Service. These locations closely mirror existing Pexip PoP locations, so that the network path bridging the Pexip Service Network to GCP has minimal exposure over the open Internet. Signaling and media traffic will use the closest geographical PoP and GCP resources.
Google Hangouts Meet	External party with own call control service	External calling parties still take advantage of the Pexip Service Network, in that to access the Gateway Service they will locate and ingress the Service Network at the closest Pexip PoP location. They will then travel over the Pexip protected QoS network before egressing at the closest set of GCP resources which support the gateway service to Google Hangouts Meet.

Development and Quality Assurance Philosophies

One of the most important aspects of a global service is the process by which the operator of the service manages new development and maintenance of the service. This not only has an impact on the reliability and functional continuity of the service, but also to its security. As the service features are developed and evolved, all efforts are undertaken to prevent introduction of new vulnerabilities or compromising the existing security posture.

Development Process

Pexip strongly believes in the power of automation to enhance the development process. Any new feature, improvement, change, or bug fix is not considered complete until the tests to validate that function are written and committed into our development environment right alongside the feature or function itself. This means that any bug that has been identified and resolved in code is not considered completely fixed until a test case to ensure that the bug is never encountered again is written right alongside the code fix. This practice allows us to be more dynamic with our development environment without compromising the quality of the software.

When a new piece of code is committed into our software codebase, that code is automatically tested to both validate that it works as expected, and to ensure that it does not break another component within our platform. If any failure in the test case is identified, that issue is immediately flagged and the developer responsible for that piece of code is notified to investigate. All these test results are also published to an internal dashboard that highlights the current state of all tests being run, all tests which are queued to be run, and the issues that have been encountered during the latest test runs.

Each night, the Pexip Infinity software undergoes a complete platform build process, and the build is deployed inside our Development Engineering, Quality Assurance, and internal testbed systems. This deployment undergoes a variety of automated tests overnight, including capacity and scale tests, call quality tests, and interoperability tests. The next day, this same platform build will be used by Pexip technical teams for production internal meetings. Any issues encountered during these tests are automatically reported to the appropriate developer or team for triage.

Weekly builds of the Pexip platform are also automated and deployed for longer soak and scale tests. These tests include thousands of call connections and call durations of multiple days to ensure continued, stable operation of the Pexip platform. As before, any errors or issues that are encountered during these tests are automatically reported to the appropriate developer or team to ensure quick triage.

Pexip releases beta builds of future software releases as often as possible, approximately one to two releases per month. These versions are loaded into public-facing demo systems to be exercised – beta software is never loaded into our production service – in addition to our regular internal labs and test facilities. Regular production internal video calls, customer demonstrations, and other meetings occur on

these systems, exposing the beta release to real-world use-cases and network conditions. This allows real-world, unfiltered usage to identify any issues that have not, or which cannot be recreated within our lab environments. If any issues are found, those issues are reported via our internal bug tracking system and assigned to the appropriate engineer or team for remediation.

When a new Pexip software version is released, any vulnerabilities that are resolved within that software version are publicly posted on the Pexip documentation site at https://docs.pexip.com in the form of a security bulletin. This document outlines the vulnerabilities that were identified, the severity of those vulnerabilities, any mitigations that need to be done in order to reduce or eliminate the impact of those vulnerabilities, and the final resolution. All releases are also scanned prior to launch to prevent introduction of viruses in customer environments or within the Pexip Cloud Service itself.

Service Release and Maintenance Process

The Pexip Development Operations team is responsible for running and maintaining the Pexip Cloud Service, an organization that maintains independence and a different management structure than those that develop the Pexip Infinity software platform.

The process for making changes or implementing new features into the Production Pexip Cloud Service is stringent to protect the quality of the service. All changes must be made and validated within two separate Quality Assurance environments – Alpha and Beta – before promotion into Production. If a change being tested passes Alpha testing it moves forward into the Beta test environment for another round of evaluations. If the testing fails at this stage, the change is flagged for review and remediation before being scheduled for testing at the Alpha stage again. Only when testing at both Alpha and Beta stages have passed does the change become a candidate for deployment to the Production Pexip Cloud Service. The process and results of Production implementation must be documented, approved, and executed by separate individuals. After implementation during a suitable maintenance window, the changes are then tested yet again to ensure proper operation, and subsequently customer usage and Technical Support Tickets are closely monitored. If a high priority issue is encountered that can be linked to a recent change, the change will be reverted under an emergency change process.

All changes and outages to the service are documented online on the Pexip Status Page at https://status.pexip.com, and postings to the page are communicated out to customers, partners, and Pexip employees via email based on who is identified as the main customer and partner contacts.

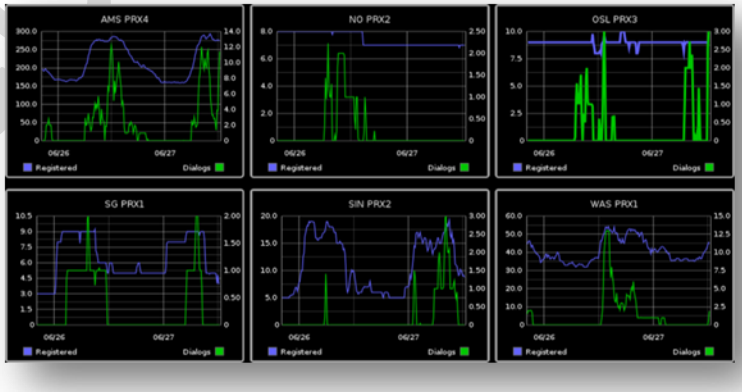
Service Network Monitoring and Maintenance

Network Security and Intrusion Detection System

The Pexip Service Network employs Intrusion Detection System (IDS) solutions from OSSEC and Suricata as part of its strategy to secure its infrastructure deployed around the globe. OSSEC is employed on servers to monitor host devices at each PoP location, while Suricata is employed to monitor the network.

The Pexip physical and virtual servers which comprise the infrastructure behind the Pexip Service Network are installed at reputable and highly secure 3rd-party Data Centers. As discussed in an earlier section regarding Pexip PoPs, these Data Center vendors include well-known providers such as Equinix, Q9, and SoftLayer. The use of carrier-independent service providers, carrier-neutral Data Centers, and Internet exchanges like Equinix, provides peering with most Telcos and ISPs around the world, ensuring the best possible "last mile" connectivity from the customer locations to our services. These Data Center vendors also ensure the highest-grade secure facilities, restricting physical access as well as maintaining the highest security certifications like SOC2, SSAE16, and ISO 27001, while offering operational reliability with an average uptime of more than 99.9999%.

Within each Data Center, Pexip maintains physical and virtual servers hosting various services, along with other devices to manage and secure the PoP. The services and devices within each PoP are closely and continually monitored by an Operations Team 24x7x365, including tracking of traffic volume, video device registration activity, and usage patterns. Trending patterns are logged and studied to help Pexip architect and evolve the Service Network to accommodate growth in usage volume and subscriber counts, but in addition suspicious changes to historic load patterns are tracked and scrutinized to identify potential issues and threats to the Service. Operations monitoring and logging also includes close watch of activity like access to tools, the creation/modification/termination of subscriptions, traffic loads on PoP devices, system CPU loads, and disk I/O rates. Notification alarms are dispatched to Pexip technical staff when events occur which are beyond configured thresholds. The available monitoring information is aggregated and can be accessed through automated tools as well as be used as part of a security audit when anomalous activity is detected. Logs are produced daily for every production device in the Pexip Service.



Security Patching

Services within the Pexip Cloud run on a number of different Operating System platforms, and consist of both in-house authored applications as well as those provided by vendors for deployed hardware. All Servers are behind firewalls that protect the Service Network from the open Internet. Anti-virus and anti-malware detection software is always kept current. Pexip closely monitors the devices and resources which comprise the Service Network for unusual activity such as traffic spikes, gross changes in device registration counts, and suspicious access attempts. Access to infrastructure is limited to a few people responsible for DevOps and Technical Support Escalation, and are full-time Pexip employees.

To keep abreast of any potential threats in the software or 3rd-party component of the service, Pexip follows the Common Vulnerabilities and Exposures (CVE) system that provides a reference-method for publicly known information-security vulnerabilities and exposures. CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems and enables Pexip to make it easier to collect data across separate vulnerability capabilities (tools, repositories, and services) with this common enumeration. Using CVE-compatible tools, services, and databases gives Pexip better coverage, easier interoperability, and enhanced security.

In addition to monitoring CVE notifications, Pexip also maintains visibility on security announcements from the vendors for software and equipment deployed in the Pexip Service Network. As security notifications from the various vendors are disclosed, Pexip assesses the threat and level of exposure, and then takes appropriate action to remediate the issue.

Servers are patched with security updates when vulnerabilities are reported from the well-known industry sources and vendor announcements. Vulnerabilities are ranked in terms of criticality and exposure, then scheduled for patching based on this assessment. For urgent patches, a maintenance window will be scheduled so corrective action will be taken as quickly as possible, with a time window based on least-disruption to the global population of Pexip subscribers. This time window is typically chosen such that it is outside the normal business hours of as many global theatres as possible. For non-urgent patches, the corrective action is rolled into the next regularly-scheduled maintenance window for the Service. In all situations, the maintenance window is announced on a public-facing website at https://status.pexip.com so that the Pexip Community may make appropriate arrangements.

Conclusion

The Pexip Cloud Video Service has been designed and deployed with security considerations to serve a global population of subscribers mindful of privacy and the protection of personal data. Users of the service can be assured that Pexip protects the communications and data of its subscribers with utmost vigilance, and considers this a fundamental goal while maintaining and growing the Service. Pexip will continue to listen to the security needs of its subscribers and will continually evolve the Service to provide additional security capabilities to promote confidence in the integrity and privacy of communications.

For questions and concerns regarding security matters, please contact security@pexip.com.

For feature enhancement proposals, please contact feedback@pexip.com.