]pexip[

EBOOK

Control access to your video meetings

Our how-to guide for ensuring secure meetings in regulated industries

What's Inside?

Securing video communications is paramount, particularly in industries that handle controlled or classified information. Whether you work in defense, intelligence, or other highly regulated verticals such as finance or healthcare, controlling access to your most sensitive discussions is mandatory for your organization. This eBook delves into the details of access control in video conferencing, offering a comprehensive guide to safeguard your virtual interactions.

Table of Contents

Implementing access control in video conferencing

Fundamentally, protecting your data means controlling who may access your data. This is the central principle of Zero Trust: no one should ever be able to do anything with or to your data that you have not authorized. And make no mistake: video data is data. In fact, video data is some of the most valuable data in your organization.

In the video world, Access Control comprises three things:

- Admission to a video session
- The type of data discussed or shared in that session
- What each participant is allowed to do within the session

To the extent possible, access control elements, such as admission to a specific session, should be automated. Certain elements, such as restricting the type of conversations individuals may engage in, cannot yet be automated. However, even in these cases, your communications platform can provide technological features, such as audiovisual notifications, to assist your personnel in this critical data management task.

Access Control Factor	Potential Video Service Implementation
Identification	Smartcard, facial scan
Authentication	LDAP, PKI, Database
Authorization	Policy stack, Dial Plan

When developing an access control plan for your organization, there are two important factors you must consider:

1. **It is critical to understand the types of information your environment supports or may support in the future.** In the defense world, this is often performed for you and your users via the classification documentation process, but this is a critical step for all organizations, regardless of industry or vertical. Even within the classified world, you will likely find that there are topics (for example, acquisition discussions) that require specialized access control beyond the usual color scheme.

2. **You must identify the accompanying risk associated with each supported information type.** This is arguably even more critical to developing a proper access control plan. Simply identifying the type of information is insufficient for helping you determine what the rules and policies governing access to that information; you must also categorize each data type and subtype based on the impact of compromise to that information. Recognize, too, that the Confidentiality, Integrity, and Availability of data may be impacted differently, leading to different risk assessments based on usage or purpose.

Common access control methods

There are several methods employed to control access to your video sessions. Here is an overview of some common access control methods you may deploy depending on your level of risk.

Low risk environments

These include personal and friendly video chats. They may occur at home or in your place of business, often between colleagues or partners, but they do not incur significant data risk to you or your organization due to their nature. An example might be a quick check-in on a colleague on maternity leave, or planning for an office holiday party.

- **Password protection:** Passwords are a simple and effective method to create a first layer of security, requiring participants to login to the video service using a username and password.
- **Invitation-only access:** Meetings can be restricted to only those who have been invited, limiting participation to pre-approved individuals.

Moderate risk environments

These include typical business meetings in which no confidential information is exchanged. In addition to the methods mentioned above, moderate risk environments may require these additional forms of access control:

- **Single sign-on (SSO):** Integrates with existing authentication systems to streamline access control.
- **PIN code access:** In addition to a login password, virtual meetings can be PIN protected to provide an additional layer of security.
- **Waiting rooms:** Participants are placed in a virtual waiting room until the host admits them.

High risk environments

These are meetings in which private and/or confidential information is exchanged. In addition to the methods mentioned above, high risk environments may require these additional forms of access control:

- **Multi-factor authentication (MFA):** Requires two or more verification methods, such as a code sent to a mobile device.
- **Policy engine:** This gives the organization the opportunity to control access over how network resources and organizational data are used. This can be done through:
    - **Role-Based Access Control (RBAC):** a security mechanism that assigns permissions based on the roles within an organization, rather than assigning permissions to specific users directly. Each role is equipped with certain access rights, and users are then assigned to these roles, effectively granting them the permissions associated with those roles.
    - **Attribute-Based Access Control (ABAC):** a security model that grants or denies access to resources based on attributes associated with the user, the resource, the environment, and the action being taken. Unlike role-based access control, which uses predefined roles to determine access, ABAC uses policies that evaluate attributes to make decisions. This allows for more granular, context-aware access control that can consider a wide range of attributes, such as location, time of day, or transaction history, thus offering a more dynamic and flexible approach to securing resources.
- **One-time meeting link:** This ensures that meeting links are only valid for a single use-case and not available for re-use in a series of meetings, for example.

Unacceptable risk environments

These are meetings at the highest security level, in which risks to security could be catastrophic in impact. In addition to the methods mentioned above, unacceptable risk environments may require these additional forms of access control:

- **Biometric authentication:** A security mechanism that uses biometric features such as fingerprints or facial recognition to access the meeting.
- **External identity provider (IDP):** An external service that manages user identities and can be integrated with the video conferencing system to authenticate users.

Technical overview

Access control in video conferencing requires various technical measures to ensure robust security and control over video meeting data. Here is an overview of some of these mechanisms.

Encryption

End-to-end encryption (E2EE) ensures that only the communicating users can read messages. This prevents potential interceptors, including service providers, from accessing the content of the meetings.

Identity and Access Management (IAM)

IAM frameworks help manage user identities and regulate access. This involves integration with directory services like lightweight directory access protocol (LDAP) or active directory, and the use of single sign-on (SSO) and multi-factor authentication (MFA).

- **SSO:** By integrating the video platform with identity providers using standards like SAML 2.0 and OpenID Connect, users are able to log in using their existing corporate credentials. This simplifies the process and ensures that only authenticated users can access meetings.
- **MFA:** MFA offers an additional layer of security when verifying user identities. This could involve sending a code to a user's mobile device or requiring biometric verification, to enhance security beyond name and password.

Secure meeting URLs

Generate unique, expiring URLs for each meeting as a mechanism to prevent unauthorized access. Meeting IDs can be randomized and set to expire after a certain period.

Audit logs

Maintain detailed logs of meeting access and activities to monitor and review any unauthorized access attempts or suspicious behavior.

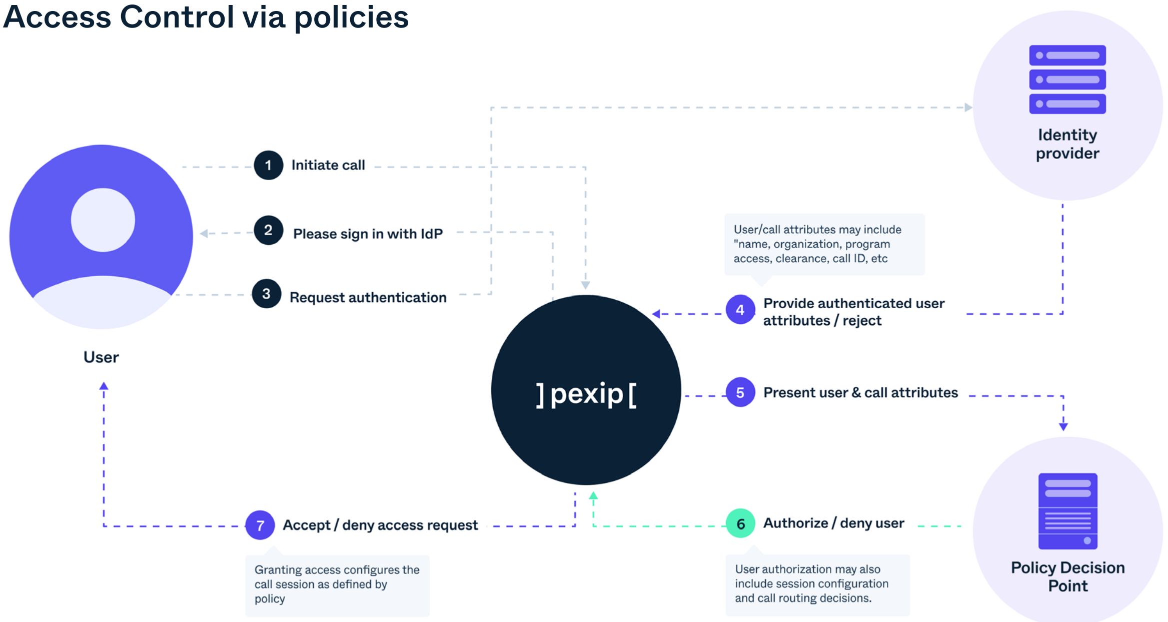
Self-hosting

Hosting the video conferencing solution on-premises or in a private cloud can ensure that the organization maintains full control over the video conferencing data. For extreme security environments, the video conferencing solution may be hosted in an air-gapped environment.

Network and transport layer security

This is employed to encrypt data as it travels over the network, ensuring that the communication channel between participants and servers remains secure.

Access Control via policies


Identity provider
1 Initiate call
2 Please sign in with IdP
3 Request authentication
User
]pexip[
4 Provide authenticated user attributes / reject
5 Present user & call attributes
6 Authorize / deny user
7 Accept / deny access request
Policy Decision Point

User/call attributes may include "name, organization, program access, clearance, call ID, etc

Granting access configures the call session as defined by policy

User authorization may also include session configuration and call routing decisions.

USE CASE

Secure meetings in the defense industry

Scenario: A national defense contractor needs to hold highly confidential video meetings with multiple stakeholders, including military officials and subcontractors.

Key challenges:

Ensuring that only authorized personnel can join the video meetings

Protecting sensitive/ confidential information from cyber threats

Maintaining compliance with defense industry regulations

Solution:

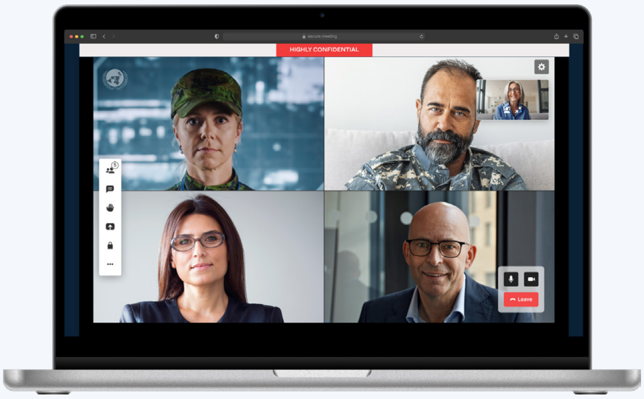
Implementing a multi-layered access control strategy using Pexip Secure Meetings:

1 **Self-hosted:** To maintain full data control, the national defense contractor opts to host the video solution on-premises, within the organization's zero-trust security architecture.

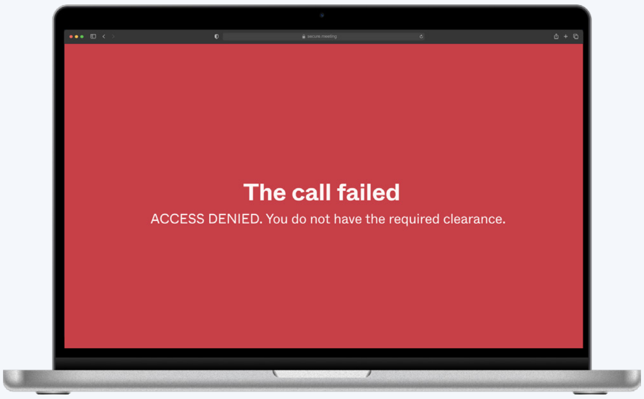
2 **Authentication and authorization:** The defense contractor utilizes single sign-on (SSO) and role-based access control (RBAC) to verify participants' identities and assign appropriate permissions for their video meetings.

3 **In-meeting reminder:** Given the varying grades of confidentiality in the defense contractor's video meetings, they employ a dynamic on-screen warning – which can be adjusted to the level of confidentiality required.

Authorized users



Non-authorized users



The call failed

ACCESS DENIED. You do not have the required clearance.

Implementing access control with Pexip

Pexip offers a comprehensive platform for secure meetings, featuring advanced access control mechanisms to meet the needs of highly regulated industries.

Authentication and authorization

Pexip integrates with existing identity management systems, allowing users to authenticate through their organization's identity provider. By enabling multi-factor authentication, users can verify their identities through additional methods such as SMS codes or authentication applications.

Administrators can also define roles or attributes within the Pexip platform, giving specific permissions to each role or based on the attribute. For example, a host can have full control over the meeting, including the ability to start and stop the meeting and manage participants, while attendees of the meeting have restricted permissions.

Encryption

Pexip's end-to-end-encryption ensures that only the intended recipients can decrypt and view the meeting content. This is critical for maintaining the confidentiality of sensitive information shared during meetings.

Secure meeting management

Pexip generates unique meeting IDs for each session, which can be configured to expire after a set time, so that links cannot be reused. Pexip also allows meeting hosts to enable waiting rooms, where participants must wait until the host admits them. In addition, Pexip offers invitation-only access to restrict meetings to pre-approved participants.

Monitoring and compliance

Pexip provides detailed audit logs that capture all access attempts and meeting activities. These logs help organizations monitor usage, detect unauthorized access, and ensure compliance with security policies and regulations.

Network security

Pexip uses transport layer security to encrypt data in transit, ensuring secure communication between clients and servers. This protects the data from interception as it travels across the network.

Secure deployment

Pexip can be deployed in a self-hosted environment, allowing for secure configuration of all network and security settings. This includes the use of firewalls, VPNs, and other security measures to protect against unauthorized access and data leaks.

Pexip offers enhanced security and control

Pexip Secure Meetings provides organizations with enhanced control and security over their communications. By managing their own infrastructure and implementing robust security measures, these security-conscious users can ensure that their video meetings are secure, compliant, and protected from evolving cyber threats.

For more detailed information and guidance on configuring and securing a self-hosted Pexip deployment, you can review our Pexip Infinity documentation.

]pexip[

www.pexip.com