GUIDANCE

Video conferencing services: security guidance for organisations

Guidance to help you to choose, configure and deploy video conferencing services such as Zoom and Skype within your organisation

The COVID-19 lockdown means many organisations are using home working on a greater scale. With more staff now working remotely, video conferencing has an obvious role to play. This guidance helps organisations to select, configure and securely implement video conferencing services.

> **Note**
> For advice on video conferencing services for personal use at home, please refer to our separate guidance for individuals and families.

Choosing a video conferencing service

Look at your existing services

When choosing a service, you will want to ensure that the video calls themselves and any other data (such as messages, shared files, voice transcriptions and any recordings) are protected. Your first step is to find out if a video conferencing service is included in your existing business software implementation. If you've performed some due-diligence or security risk assessment of video conferencing services, you should re-examine these.

Using existing video conferencing services has the following benefits:

- staff will be familiar with administering and using the service, which will reduce training and deployment costs
- you'll use your existing (well-configured) authentication provider
- simple integration with your existing audit and monitoring capabilities
- you can maintain compliance with data handling legislation (including any requirements associated with regulated industries)

Consider new services

If considering a new service, you should perform a security risk assessment across a shortlist of providers. You can do this by following the NCSC's SaaS security guidance, and/or requesting copies of any independent assessments or audits. The results of this assessment, combined with the provider's terms and conditions (and privacy statement), will give you an understanding of:

- how the provider implements basic security controls
- where your data is held

- what they can do with it

If you need video conferencing for more sensitive meetings, you should follow the NCSC's Cloud Security Principles to determine whether a service meets your security needs. We recommend this approach for government use (such as handling OFFICIAL data), regulated industry sectors, and organisations that handle personal data. The principles cover a greater level of detail to help you understand how the service is built and managed by the provider. Some cloud providers publish a response to the principles so you can understand exactly how their service meets the security goals.

Additional considerations

Many video conferencing services include paid options that provide additional features or levels of service. This can include enhanced security, configuration and privacy features.

Some services implement end-to-end encryption so that all data is encrypted in transit and can only be decrypted by the meeting participants. Other services specifically encrypt data between user devices and the service - so allowing them to provide richer functionality that can only be implemented server-side. Whichever model your chosen provider implements, you still have to be able to trust them to have designed and implemented this well, and that the apps and service actually work in the way that they describe.

Cloud services will often store and process data **in** (and route traffic **through**) data centres across several countries and jurisdictions. You should be confident that you know where your data is, who can access it and under what circumstances. Organisations in regulated industries and those that handle government data should refer to Cloud Security Principle 2.1: Physical location and legal jurisdiction.

Deploying and configuring the service

You should aim to set company-wide defaults and controls where possible. You can do this using the service itself, or by configuring the settings in the apps delivered to your managed devices.

Think carefully about which settings to enforce, and which to set as a default that can then be overridden on a per-meeting basis. Default settings should be configured in such a way so as to balance user needs with security. For example, the ability to share screens may be appropriate for some audiences, but not others.

Configuring user accounts

Your staff will need to log into the service to be able to schedule meetings. Some video conferencing services also allow or require users to authenticate to join meetings. We recommend implementing single sign-on where possible, integrating the video conferencing service with your existing corporate identity. This means that the service will inherit the same identity protections as your other corporate services. It will significantly improve the user experience by reducing the number of times that authentication is required.

If you can't deploy single sign-on, you should ensure that you configure the service in line with NCSC's password guidance, and include multi-factor authentication (also known as two factor authentication, or 2FA).

Some of your users will need more privileged accounts, so they can (for example) configure the service, or access logs, transcripts, or recordings. We recommend applying the concept of least privilege using a role-based access control (RBAC). This is described in more detail in the NCSC's Cloud Security Principle 9: Secure user management.

Configuring access to meetings and conferences

Being able to control who can join (or initiate) meetings will help protect the confidentiality of the discussions, and prevent unwanted interruptions. Participants usually join meetings arranged in advance by clicking on a link, or by entering a unique code. We recommend that:

- users from your organisation (and guests that were specifically invited to the meeting) are allowed straight into a meeting
- unauthenticated users should be required to enter a passcode

- unauthenticated users should be held in a waiting area (often referred to as 'the lobby'), and only be admitted into the meeting once their identity has been verified by a trusted participant

Some video conferencing services allow your users to make a call to users inside and outside of your organisation without arranging it in advance. If this feature is available, consider blocking calls that originate from outside of your organisation if they are not in a user's contacts list. If you do not block such calls, we recommend that the service is configured to block calls from unidentified and/or unauthenticated users.

Configuring features available during meetings

Video conferencing services often include extra features such as:

- file sharing
- screen sharing
- instant messenger chat
- automatic call transcript generation
- remote control of another participant's device

If your staff need these features, you will have to decide whether you trust the service enough to protect the extra data that will be sent to/via the service, and whether these features should be enabled by default (or be an 'opt-in' for each meeting).

Many services allow calls to be recorded, and for text chats and shared files to be saved. Ensure you know where this data is stored, and who can access it.

Configuring video conferencing apps and software

The NCSC's third-party apps guidance helps organisations to decide whether to deploy apps on their devices. You should configure the video conferencing service consistently across all platforms you use, whether that's an installed app, a web browser, or 'join audio-only' via a phone call. Your staff should access the service using devices that have been configured as described in the NCSC's devices guidance.

You may be able to configure apps at an organisational level to constrain the app's access to contact lists, location data, documents and photos. If the app can access this data, make sure that you understand what data is shared with the service, that you are OK with this, and are confident that it is appropriately protected. In addition:

- Look to use apps that can be installed from a device's app store, or distributed using enterprise management tools.
- Disable any prompts that encourage users to download an app when joining a call, as it normalises running arbitrary apps from the internet (and hence makes your organisation more susceptible to phishing).
- If you use an always-on VPN on your corporate devices, consider allowing an exception for your trusted video conferencing service to improve performance; a service that uses well-configured encryption and enforces mutual authentication can give you as much confidence over the internet as a well-configured VPN tunnel.
- Take special care if you access the video conferencing service using dedicated devices, such as video conferencing room equipment. These may have different support/patching processes and require different configuration to the apps available for smartphones, tablets and computers.

Other organisations that you work with may use a different video conferencing service to yours. You should ensure that those services can be accessed via the web browser on your users' devices.

We recommend avoiding installing extra apps for those services to reduce the associated configuration and maintenance overhead, and to minimise the need to analyse the security impact of installing those apps.

Helping staff to use services securely

Staff who are perhaps home working for the first time may not have used video conferencing services. Provide clear user guidance that explains how to use them securely, and check that the service works as described.

For staff attending meetings

Ask your users to test that the video conferencing service is working before using it for real meetings - some services include a 'test' feature that can help with this. They should be familiar with how to mute the microphone and turn off the camera. This will give them more control over what they share with others.

We suggest telling your staff:

- to treat the details explaining **how to join the meeting** as if it is as sensitive as the **meeting itself**
- to consider blurring their background or using a background image (if this is a feature is available); this can add a degree of personal privacy when working from a home environment
- how to check when their webcam is active, so they can be confident it is de-activated when not in use
- how the service indicates when the meeting or call is being recorded

Many webcams have a light that comes on when it is in use. In some environments you may prefer a device where the user can slide a physical shutter across the lens, or unplug the camera when not in use.

For staff organising meetings

Meeting organisers (and sometimes their delegates) will have controls over and above those available to other attendees. You should ask users that host meetings with participants from outside of your organisation to hold a test meeting to familiarise themselves with controls such as approving participants in the lobby, removing participants from the call and muting individuals.

When setting up the call, the meeting organiser should consider which features (such as screen sharing and file sharing) are appropriate for the meeting, and whether these should be constrained to a subset of participants.

If meetings are password protected, the meeting organiser should only share that password with participants. For example, they could send an email containing the

password directly to participants only, rather than including it within a calendar appointment (that might be viewable by everybody in your organisation).

During the video conference, we recommend that meeting organisers take responsibility for:

- verifying the identity of all participants on the call
- appropriately approving participants being held in the lobby
- removing participants that have not been successfully identified

PUBLISHED

21 April 2020

REVIEWED

21 April 2020

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Public sector

Large organisations

Small & medium sized organisations

Self employed & sole traders