



Infinity Connect

Guide for Administrators

Software Version 29

Document Version 29.a

July 2022

]pexip[

Contents

| | |
|--|----------|
| Introduction | 4 |
| Infinity Connect clients | 4 |
| Which clients should I use in my deployment? | 5 |
| Infinity Connect guides for end users | 5 |
| Making calls from Infinity Connect clients | 5 |
| Receiving calls to Infinity Connect clients | 6 |
| Branding the Infinity Connect clients | 6 |
| Enabling and disabling use of Infinity Connect clients | 6 |
| Comparison of Infinity Connect and other video endpoints | 7 |
| Installing and using Infinity Connect | 8 |
| About the Infinity Connect web app | 8 |
| Accessing a conference or making a call | 8 |
| Hardware requirements | 8 |
| About the Infinity Connect desktop client | 8 |
| Hardware requirements | 9 |
| Installing the Infinity Connect desktop client | 9 |
| Registering the Infinity Connect desktop client | 10 |
| Accessing a conference or making a call | 10 |
| About the Infinity Connect mobile clients | 10 |
| Prerequisites | 10 |
| Protocols | 10 |
| Installing the Infinity Connect mobile client for Android | 10 |
| Installing the Infinity Connect mobile client for iOS | 11 |
| Accessing a conference or making a call | 11 |
| Infinity Connect client settings | 11 |
| Using Infinity Connect in-call controls | 15 |
| Buttons, menus and keyboard shortcuts | 15 |
| Text-based controls | 27 |
| Registering and provisioning the Infinity Connect desktop client | 28 |
| Client authentication options | 29 |
| Setting up appropriate DNS records | 29 |
| Provisioning the Infinity Connect desktop client with registration and/or branding details | 29 |
| Using Infinity Connect to share content | 36 |
| Sharing your screen | 36 |
| Sharing images and PDFs | 38 |
| Using Infinity Connect for presentation, chat and conference control only | 40 |
| Locking a conference and allowing participants to join a locked conference | 40 |
| Locking using the Administrator interface | 41 |
| Locking using Infinity Connect | 41 |
| Locking using DTMF | 41 |

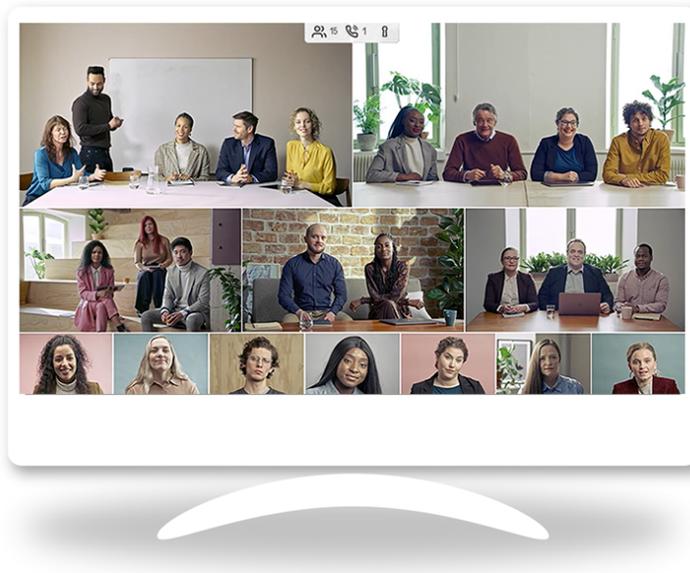
| | |
|---|-----------|
| Allowing waiting participants to join a locked conference | 41 |
| Rejecting a request to join a locked conference | 42 |
| Administering Infinity Connect | 43 |
| Customizing and branding the Infinity Connect clients | 43 |
| Creating and uploading a branding package | 43 |
| Editing an existing branding package | 45 |
| Removing a web app branding package (revert to default branding) | 45 |
| Applying branding to the desktop clients | 45 |
| Obtaining diagnostic information from Infinity Connect | 47 |
| Creating preconfigured links to launch conferences via Infinity Connect | 48 |
| Security considerations | 48 |
| Links to the web app | 48 |
| Links to the desktop and mobile clients | 49 |
| Links to the legacy Infinity Connect clients | 50 |
| Setting up DNS records and firewalls for Infinity Connect client connectivity | 51 |
| DNS records | 51 |
| Firewall configuration | 51 |
| Using Infinity Connect from outside your network | 51 |
| Further information and connectivity examples | 51 |
| Switching to the legacy Infinity Connect web app | 54 |
| Switching between current and legacy web app | 54 |
| Comparison of current and legacy Infinity Connect clients | 54 |
| Troubleshooting Infinity Connect error messages | 56 |
| Infinity Connect release notes | 61 |
| Infinity Connect web app release notes | 61 |
| What's new? | 61 |
| Fixed issues | 61 |
| Known limitations | 61 |
| What's new in previous versions | 61 |
| Fixed issues in previous versions | 64 |
| Infinity Connect desktop client release notes | 64 |
| What's new? | 65 |
| Fixed issues | 66 |
| Known limitations | 67 |
| What's new in previous releases | 67 |
| Fixed issues in previous releases | 68 |
| Infinity Connect mobile client release notes | 68 |
| What's new? | 69 |
| Fixed issues | 69 |
| Known limitations | 70 |
| What's new in previous releases | 70 |
| Fixed issues in previous releases | 71 |

Introduction

Pexip Infinity is a self-hosted, virtualized and distributed multipoint conferencing platform. It can be deployed in an organization's own datacenter, or in a private or public cloud such as Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP) or Oracle Cloud Infrastructure, as well as in any hybrid combination. It enables scaling of video, voice and data collaboration across organizations, enabling everyone to engage in high definition video, web, and audio conferencing.

It provides any number of users with their own personal Virtual Meeting Rooms (VMRs), which they can use to hold conferences, share presentations, and chat. Participants can join over audio or video from any location using the endpoint or client of their choice, including:

- Professional video conferencing room systems (SIP and H.323 devices)
- Desktop/mobile (with the Pexip Infinity Connect suite of clients)
- Web browsers (WebRTC - no downloads required)
- Traditional audio conferencing (PSTN dialing)



Pexip VMRs maintain the same customized address and are always available for spontaneous 1-to-1 or group meetings.

VMRs can also be accessed through a Virtual Reception IVR service, which allows all participants to dial a single number to access Pexip Infinity, and then use the dial tones on their endpoint or phone to select the conference they want to join.

The platform also includes the Infinity Gateway service, which allows end users to place calls to other endpoints that use different protocols and media formats, or to seamlessly connect into an externally-hosted conference, such as a Microsoft Teams or Skype for Business meeting, or Google Meet.

Pexip's Media Playback Service allows you to play prerecorded video content (such as adverts and informational videos) to consumers. When the media finishes playing, the user can be transferred to another service, such as a VMR conference, or they

can be disconnected.

It automatically transcodes all the popular video and audio codecs and supports standard protocols including SIP, H.323, and WebRTC. It supports all standards-based devices including those from Cisco, Poly, Lifesize, Sony, Radvision, Yealink, and Avaya. It also supports software clients such as Microsoft Skype for Business, Skype for Business Online (Office365) and Surface Hub.

Infinity Connect clients

The Infinity Connect suite of clients allows users to join conferences (Virtual Meeting Rooms, Virtual Auditoriums and so on) within the Pexip Infinity deployment.

In addition to sharing audio and video, Infinity Connect users can also control the conference, view presentations, share content, and exchange chat messages with other conference participants. Infinity Connect can also be used in conjunction with the Infinity Gateway to make person-to-person calls, or join conferences hosted on other platforms, such as Skype for Business meetings.

All Infinity Connect clients can make calls to Pexip Infinity services. The Infinity Connect desktop client can also register to Pexip Infinity in order to receive calls and use directory services.

Infinity Connect clients are available for almost any device:

- The [Infinity Connect web app](#) is included as part of all Pexip Infinity deployments. It is used to access Pexip Infinity services from all of the major web browsers.

- The [Infinity Connect desktop client](#) is an installable client, supported on Windows, OS X, and Linux.
- The [Infinity Connect mobile clients](#) are available for Android and iOS devices.

All Infinity Connect clients are available for free with the Pexip Infinity platform (although, as with any other endpoint, you must still have a license with sufficient call capacity before you can place calls).

Which clients should I use in my deployment?

The Infinity Connect suite of clients all offer identical conference join and control features, and have the same high-quality video experience. You can use a combination of some or all Infinity Connect clients within your deployment, depending on your requirements. In general, we recommend the following:

- Users connecting from outside your organization and who do not have their own video device should generally use the Infinity Connect web app to access VMRs. This means that they won't need to download or install anything in order to access meetings, but will still have the same high-quality user experience and functionality of participants using the Infinity Connect desktop client. You'll need to make sure that at least one Conferencing Node is accessible externally, and you'll also need to [set up appropriate DNS records](#) for connections from both inside and outside your network.
- Users connecting from inside your organization should also use the Infinity Connect web app, unless you want them to be able to register to receive incoming calls — in which case they need to use the Infinity Connect desktop client.
- The Infinity Connect desktop client should be used if you want to take advantage of the additional registration (to receive incoming calls) and internal directory service features. Administrators can also set up [Call Routing Rules](#) that apply to registered devices only, meaning that you can permit registered Infinity Connect desktop client users to make calls that Infinity Connect web app users cannot.

If you are deploying the Infinity Connect desktop client in your environment, we recommend that you make use of [provisioning](#), and you'll also need to [set up appropriate DNS records](#).

- The Infinity Connect mobile client is aimed at users who want to be able to control a conference and view presentations while in a meeting using a video device that does not support those features — for example, a video conferencing endpoint in a meeting room.
- The Infinity Connect mobile client can also be used to join a meetings as an audio or video participants, but because of the nature of mobile devices this may result in intensive battery use.

Infinity Connect guides for end users

This guide covers topics that are only relevant to an administrator.

We publish a series of quick guides aimed at end users of the Infinity Connect desktop client, the Infinity Connect web app, and the Infinity Connect mobile client. These guides are available in PDF format from <https://docs.pexip.com/admin/download.pdf.htm#enduser>.

Making calls from Infinity Connect clients

For an Infinity Connect client to make a call, it must be able to connect to a Conferencing Node that can route that call on its behalf.

Infinity Connect web app clients connect directly to a Conferencing Node or Reverse Proxy (via the host's FQDN or IP address). When a call is placed from the client, it is treated as an **incoming call request** by the Conferencing Node, and routed accordingly. For more information, see [Service precedence](#). All other Infinity Connect clients typically use DNS SRV records to find a Conferencing Node to connect to.

You must ensure that your deployment has appropriate internal and external DNS configured to allow clients located inside and outside your internal network to resolve the Conferencing Node address successfully. The actual address clients use when attempting to locate a host Conferencing Node depends on the domain being called and the client's own configuration. For more information, see [Setting up DNS records and firewalls for Infinity Connect client connectivity](#).

Receiving calls to Infinity Connect clients

For an Infinity Connect client to receive a call, it must register with a Conferencing Node. The client's **Registration Host** setting specifies the domain, FQDN or IP address of the Conferencing Node that it should register to; therefore, you must ensure that the address used is reachable from the client from the internal or external network as appropriate, and that any FQDNs can be resolved via DNS lookups. For more information, see [Registering and provisioning the Infinity Connect desktop client](#).

Currently, only the Infinity Connect desktop client can register to a Conferencing Node.

Branding the Infinity Connect clients

The branding and styling of the Infinity Connect clients (web app and desktop) can be customized. This changes the look and feel of the Infinity Connect client regardless of which service is being accessed. See [Customizing and branding the Infinity Connect clients](#) for more information.

Enabling and disabling use of Infinity Connect clients

Access to conferences from all Infinity Connect clients is enabled by default. If you do not want users to access conferences within your deployment from Infinity Connect clients, you can disable this functionality.

To disable or re-enable this functionality:

1. Go to **Platform > Global Settings**.
2. From within the **Connectivity** section:
 - a. Deselect or select **Enable support for Pexip Infinity Connect and Mobile App**. This controls access from all Infinity Connect clients and third-party clients using the client APIs.
 - b. When **Enable support for Pexip Infinity Connect and Mobile App** is selected, you must also ensure that **Enable WebRTC** and **Enable RTMP** are deselected or selected as appropriate to enable the clients that use those protocols to access conferences.

When access is disabled, users attempting to use Infinity Connect clients to access a conference or make a call are presented with the message **Call Failed: Disabled** (you can customize the clients to change the wording of this message if required).

Comparison of Infinity Connect and other video endpoints

The Infinity Connect suite of clients are developed directly by Pexip and use Pexip's client APIs to integrate with the Pexip Infinity platform. This means that there are some differences in the experience of joining and participating in a Pexip Infinity conference via an Infinity Connect client, when compared with Skype for Business clients and other types of software and hardware endpoints.

The table below summarizes these behavioral differences.

| Feature | Infinity Connect client | Skype for Business and other video clients |
|--|--|--|
| Joining a Host+Guest conference that has a Host PIN but no Guest PIN * | <p>Whether or not a Host has already joined, participants have the option to enter the Host PIN (to join as a Host), or simply select "Join" (to join as a Guest).</p> <p>If they choose to join as a Guest:</p> <ul style="list-style-type: none"> If a Host has not yet joined, they are taken to the "Waiting for Host" screen. <p>While waiting for a Host to join, a keypad option is available on their toolbar which they can use to enter the Host PIN and join as a Host.</p> <ul style="list-style-type: none"> if a Host has already joined, they are taken straight into the conference. | <ul style="list-style-type: none"> If a Host has not already joined, participants are taken to the "Waiting for Host" screen, where they have the opportunity to enter the Host PIN. If a Host has already joined, participants automatically join as a Guest, unless they have included the Host PIN as part of the dial string. |
| Joining a Host+Guest conference that has a Host PIN and Guest PIN * | All clients have the same behavior: participants are asked to enter the conference PIN and if they enter the Host PIN, they join the conference. If they enter the Guest PIN and a Host has already joined then they are taken straight into the conference, otherwise they are taken to the "Waiting for Host" screen. | |
| Conference PINs with a trailing # | When entering PINs, any trailing # is optional. | Participants hear the "please enter the # key" prompts, and must enter the # after the PIN. |
| Joining a VMR via a Virtual Reception | Participants must dial into the Virtual Reception first, and then at the prompt enter the numeric alias of the target Virtual Meeting Room. | <p>Participants using other clients can join a VMR via a Virtual Reception in a single step. They do this by dialing <code><reception_alias>*<destination_alias>@<domain></code>.</p> <p>H.323 devices can also use the dial format <code><reception_alias>#<destination_alias>@<domain></code>.</p> |
| Viewing roster | Participants can view the roster. | The roster is not available. |
| Appearing in the Infinity Connect roster | Other Infinity Connect participants appear in the roster only after they have successfully joined the conference. | <p>Participants using other clients appear in the roster while they are waiting to join the conference, for example while they are being held at the PIN entry screen or waiting for a Host* to join. At this point, they do not have a role assigned.</p> <p> A Host using an Infinity Connect client (including Hosts who have joined in presentation and control-only mode) can let these participants into the conference without them having to enter a PIN.</p> |
| Conference control | Host participants can control the conference (add, mute, and disconnect participants; change a participant's role; lock and unlock the conference). | Participants do not have access to conference control, apart from a limited set of controls available to endpoints that support DTMF. |
| Chat | Participants using Infinity Connect and Skype for Business clients can send and receive chat messages, but other video clients cannot. | |

* At least one Host must join with media (video and/or audio) before Guests are able to join. Alternatively, Infinity Connect users who have joined as a Host in presentation and control-only mode (and who therefore do not act as a trigger for starting the conference) can elect to [Start the meeting](#).

Installing and using Infinity Connect

About the Infinity Connect web app

The Infinity Connect web app is automatically available as part of all Pexip Infinity deployments. It provides a WebRTC interface to Pexip Infinity conferencing services.

The web app is supported in the following browser versions, although we strongly recommend using the latest publicly-released version (i.e. "stable version" or "supported release") of a browser:

- Google Chrome version 61 and later (64-bit only) on Windows, Linux, macOS, iOS*, and Android*
- Mozilla Firefox version 68 and later (but v80 or later is recommended for improved network resilience) on Windows, Linux, macOS, and iOS*
- Microsoft Edge — all chromium-based versions on Windows and iOS*
- Opera version 53 and later on Windows and macOS
- Apple Safari version 11.1 and later on macOS
- Apple Safari on iOS 11.2 and later

* For the best experience on mobile devices, we recommend using the Infinity Connect mobile clients.

i Infinity Connect web app is not supported on devices running on a Windows Phone OS.

Infinity Connect users can share their screen, images and PDFs from any browser.

Accessing a conference or making a call

To access a conference or make a call using the Infinity Connect web app, users enter into the address bar the IP address or domain name of their nearest Conferencing Node (or reverse proxy if, for example, it is being used to host a customized version of the web app), followed by `/webapp/home` (for example, `confnode.example.com/webapp/home`). Users are then presented with the home screen, from where they can check their setup and then select **Call** to enter the alias of the conference or person they want to call.

System administrators and conference organizers can also [provide a preconfigured link](#) to a conference alias.

If your Pexip Infinity deployment is located inside a private network and you want to allow Infinity Connect users who are located outside your network to connect to your deployment, see [Using Infinity Connect from outside your network](#).

Hardware requirements

The performance of the Infinity Connect web app typically depends upon a combination of the choice of browser and which other applications are currently running on the client system.

However, as a minimum we recommend that your client system has:

- 4 GB of RAM
- Intel Core i5 processor or equivalent

About the Infinity Connect desktop client

i The Infinity Connect desktop client is released separately to Pexip Infinity, and may have been updated since this Administrator Guide was released. For the most up-to-date Infinity Connect desktop client user documentation, see [Introduction to Infinity Connect](#).

The Pexip Infinity Connect desktop client is a stand-alone video client that provides access to Pexip Infinity services. It is currently supported on:

- Microsoft Windows 10
- macOS 10.11 and later
- Ubuntu Linux 16.04 and later
- Citrix Cloud

Note that 32-bit operating systems are not supported with the Infinity Connect desktop client.

Hardware requirements

The performance of the Infinity Connect desktop client can depend upon which other applications are currently running on the client system.

However, as a minimum we recommend that your client system has:

- 4 GB of RAM
- Intel Core i5 processor or equivalent

Installing the Infinity Connect desktop client

i No special privileges are required to install the Infinity Connect desktop client, as it is installed in a per-user context.

To install the Infinity Connect desktop client, go to the [Pexip App download page](#) and download and install the appropriate file for your operating system as described below.

Note that 32-bit operating systems are not supported with the Infinity Connect desktop client.

Windows

(Supported on Windows 10.)

Download the `pexip-infinity-connect_<release>_win-x64.msi` file for Windows.

Double-click on the `.msi` file to install the Infinity Connect desktop client and then follow the instructions in the installation wizard. During the installation process the Infinity Connect icon is added to the desktop, and entries are added to the Windows registry to allow links prefixed with `pexip:` and `pexip-provision:` to open automatically in the Infinity Connect desktop client.

macOS

(Supported on macOS 10.11 and later.)

Download the `pexip-infinity-connect_<release>_darwin-x64.dmg` file for macOS.

To install the macOS client, open this file and drag the **Pexip Infinity Connect.app** into the **Applications** folder.

Linux

Download the `pexip-infinity-connect_<release>_linux-x64.tgz` file for Linux.

To install the Linux client:

1. Create a new directory. For example, to install the client for a single user "alice":

```
mkdir /home/alice/pexapp
cd /home/alice/pexapp
```
2. Download the Infinity Connect desktop client `tgz` file to that directory and extract the archive. For example:

```
tar -xzf pexip-infinity-connect_<release>_linux-x64.tgz
```
3. Copy the `.desktop` file to the appropriate location for making the application available for this user as per freedesktop.org-compliant desktop guidelines (see <https://developer.gnome.org/integration-guide/stable/desktop-files.html.en> for more information). For example:

```
cp pexip-infinity-connect_linux-x64/pexip-infinity-connect.desktop /home/alice/.local/share/applications/pexip-infinity-connect.desktop
```
4. Using your preferred text editor, modify the `Exec` line to point to the location of the `pexip-infinity-connect` binary on your system. For example:

```
emacs /home/alice/.local/share/applications/pexip-infinity-connect.desktop
```

and make it look something like this:

```
[Desktop Entry]
Name=Pexip Infinity Connect
Exec=/home/alice/pexapp/pexip-infinity-connect_linux-x64/pexip-infinity-connect
Terminal=false
Type=Application
Icon=application-x-executable
```

Note that if you want to install the application for all users (rather than just a single user), follow the same instructions but instead copy the `.desktop` file into the `/usr/share/applications` directory (you may need root privileges to do this).

Citrix

The Infinity Connect desktop client for Citrix enables users to securely access the Infinity Connect desktop client from any client using the Citrix Workspace App to join VMRs, call through the Pexip Gateway to Microsoft Teams, or to simply place point-to-point calls.

Registering the Infinity Connect desktop client

After the Infinity Connect desktop client has been installed, it can be registered to a Conferencing Node. The administrator can also provision individual users with their registration details and automatically apply those registration settings to their Infinity Connect desktop client.

See [Registering and provisioning the Infinity Connect client](#) for more information.

Accessing a conference or making a call

When users open the desktop client, they are presented with the home screen, from where they can check their setup and then select Call to enter the alias of the conference or person they want to call (for example `meet.alice@vc.example.com`).

System administrators and conference organizers can also [provide a preconfigured link](#) to a conference alias.

About the Infinity Connect mobile clients

 The Infinity Connect mobile clients are released separately to Pexip Infinity, and may have been updated since this Guide was released. For the most up-to-date Infinity Connect mobile client user documentation, see [Introduction to Infinity Connect](#).

The Infinity Connect mobile clients can be used by conference participants to control the conference and view presentations from their own personal Android or iOS device, even when they are using a separate telephone or video endpoint to participate in the conference.

Users also have the ability to join a conference from their Android or iOS device, as either an audio-only or a full audio and video participant, allowing them to participate in a conference from anywhere they have an internet connection.

Prerequisites

Infinity Connect mobile clients require deployments with HTTPS and valid, trusted certificates.

Infinity Connect mobile clients use the Pexip client API, so you must ensure access to this is enabled in your deployment (**Platform > Global Settings > Connectivity > Enable Support For Pexip Infinity Connect And Mobile App**).

Protocols

Infinity Connect mobile clients use the WebRTC protocol, so you must ensure this is enabled in your deployment (**Platform > Global Settings > Connectivity > Enable WebRTC**).

Installing the Infinity Connect mobile client for Android

The Infinity Connect mobile client for Android is available for free from the Google Play store at <https://play.google.com/store/apps/details?id=com.pexip.infinityconnect>. Follow the instructions to download and install the Infinity Connect mobile client on your device.

 If you search for "Pexip" in the Google Play store, you will see two apps. The version labeled **Pexip Infinity Connect** with the  icon is the one you should download for use with Pexip Infinity deployments. You will also see an app called **Pexip (My Meeting Video)**; this is for use by customers of the [Pexip Service](#) and **should not be used** in Pexip Infinity deployments.

The Infinity Connect mobile client for Android requires **Android 7.0** or later.

Installing the Infinity Connect mobile client for iOS

The Infinity Connect mobile client for iOS is available for free from the Apple Store at <https://itunes.apple.com/us/app/pexip/id1195088102>. Follow the instructions to download and install the client on your device.

- i** If you search for "Pexip" in the Apple Store, you will see both the legacy and the latest versions of the app. The version labeled **Pexip Infinity Connect** with the  icon is the latest version and the one you should download. You will also see an app called **Pexip (My Meeting Video)**; this is for use by customers of the [Pexip Service](#) and **should not be used** in Pexip Infinity deployments.

The latest version of the Infinity Connect mobile client for iOS, v1.9, is compatible with any iOS device running **iOS 15.2** or later.

Accessing a conference or making a call

When users open the Infinity Connect mobile client, they are presented with the home screen, from where they can check their setup and then select **Call** to enter the alias of the conference or person they want to call (for example `meet.alice@vc.example.com`).

System administrators and conference organizers can also [provide a preconfigured link](#) to a conference alias.

Infinity Connect client settings

There are various configuration settings available within the Infinity Connect clients. The table below provides information about each of these settings.

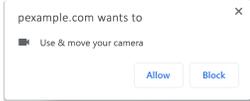
Note that administrators can change, disable or provide default text for many of these settings by [Customizing and branding the Infinity Connect clients](#).

Administrators can also provision individual Infinity Connect desktop client users with their registration details and automatically apply those registration settings to their client. See [Registering and provisioning the Infinity Connect client](#) for more information.

| Setting | Description |
|---|---|
| Home page | |
| Name | <p>The name that appears to other conference participants.</p> <p>You're asked to enter your name the first time you use the client, but you can change your name from the home page by clicking on it.</p> <p>For desktop client users, your name may already have been pre-filled if your administrator has sent you a link that automatically applies your personalized settings to your client, but it can still be overwritten.</p> |
| Settings | |
|  (Camera) | <p>Shows the currently selected camera. Select this option to change the camera to use.</p> <p>When the selected camera is working properly, your self view is shown in the main video window.</p> <p>i If you select <i>None</i> you will join the meeting without a camera, but you can still see everyone else's video. (This option is not available to iOS users.)</p> |
|  (Microphone) | <p>Shows the currently selected microphone. Select this option to change the microphone to use.</p> <p>When the selected microphone is working properly, a green bar appears under the main video window when audio is detected. The length of the bar represents the level of audio volume being picked up by the microphone.</p> <p>i If you select <i>None</i> you will join the meeting without a microphone, but you can still hear everyone else's audio. (This option is not available to iOS users.)</p> |
|  (Speakers) | <p>Shows the currently selected speakers or headset. Select this option to change the speakers to use.</p> <p>To check that the selected speakers are working properly, select the speaker icon from the bottom left of the main video window and then select the speaker to use. A tone will be played from that speaker.</p> |

| Setting | Description |
|--|--|
|  Bandwidth * | <p>The maximum bandwidth for the call, and the bandwidth at which the initial call attempt is made. Note that calls may be temporarily downspeeded due to network conditions.</p> <p>The default is <i>Medium (up to 1264kbps)</i>, but if you are on a cellular connection or slow Wi-Fi connection you may want to reduce this to <i>Very Low (up to 256kbps)</i>.</p> <p>You should also reconnect using a lower bandwidth if you experience slow or low-quality video.</p> |
|  Languages * | <p>(Only applies if additional languages have been enabled by your administrator.)</p> <p>Allows you to select from a drop-down menu the language to use in your Infinity Connect client.</p> <p>i If your browser or device's default language is supported by the Infinity Connect client, that language is used automatically. Alternatively, your administrator may have specified a default language to use.</p> |
|  Registration (Infinity Connect desktop client only) | |
| Registration Host * | <p>The domain, FQDN or IP address of the server to which registration requests are sent. This should be the IP address or FQDN of a local Conferencing Node.</p> <p>For more information, see Setting up DNS records and firewalls for Infinity Connect client connectivity).</p> |
| Alias | <p>The alias that this client will register with. This is the alias that other users should dial when they want to call this client.</p> <p>This alias must match one of the entries on the Management Node under Users & Devices > Device Aliases.</p> |
| Username / Password | <p>The username and password to use when this device registers to Pexip Infinity and is not using Single Sign-On (SSO) services, such as AD FS.</p> <p>The username and password must match those configured for this alias on the Management Node under Users & Devices > Device Aliases.</p> <p>If the client is configured for SSO, you will be asked to sign in to an alternative authentication service.</p> |
| <p>i The registration fields are read-only when the client is successfully registered — you must Unregister if you want to change them. When a client has been configured (provisioned) with SSO registration information, the Username / Password fields are blank and the registration settings can only be modified by resetting the app.</p> | |
|  Advanced settings | |
| Confirm when disconnecting * | <p>When this option is selected, you must confirm each time you wish to disconnect from a meeting. This prevents you from accidentally disconnecting yourself. This is on by default.</p> |

| Setting | Description |
|---|--|
| View incoming presentation in full motion * | <p>This setting determines how presentations from other participants are initially received.</p> <p>Presentations can be received in two formats:</p> <ul style="list-style-type: none"> A higher-bandwidth full motion HD stream (suitable for presentations with a lot of movement). With this option, Pexip Infinity sends the presentation to the Infinity Connect client as a video stream at up to 30 fps, so movement will appear smooth. <ul style="list-style-type: none"> i The actual frame rate used depends on the capabilities of the endpoint that is sending the presentation. Infinity Connect clients can send presentations at up to 30 fps; other clients may send at a higher or lower frame rate. A lower-bandwidth series of still images (suitable when very sharp images are required). With this option, Pexip Infinity periodically takes a snapshot of the presentation and converts it to JPG format, and sends that to the Infinity Connect client at between 0.5 to 1 fps. For this reason, presentations that contain a lot of movement may appear jerky to clients using this option. <p>This setting is on by default: presentations are initially received as full motion video, and you can subsequently elect to view them as still images by selecting the  button at any time during the call. However, when View incoming presentation in full motion is not selected, presentations received by you are always shown as still images by default, and you can then elect to view them as full motion video by selecting the  button.</p> |
| Send anonymous statistics * | <p>When this option is selected, anonymous information about how the client is being used is sent to Pexip. This is on by default.</p> |
| Play ringtone on incoming calls * | <p>(Infinity Connect desktop client only)</p> <p>This is on by default; if you do not want to hear the default ringtone when you are receiving an incoming call, you can de-select this option.</p> |
| Start application in background * | <p>(Infinity Connect desktop client only)</p> <p>The client will always start automatically when the device it is installed on starts. This option allows you to select whether it starts minimized (in the background), or maximized (in the foreground).</p> <p>If you have previously entered your registration details the client will also register on startup. If you are configured for SSO, you may be asked to sign in to your alternative authentication service, such as AD FS.</p> <p>This is off by default.</p> |
| High contrast * | <p>When this option is enabled, there is a higher contrast between foreground and background elements of the user interface, making them more legible. This is off by default.</p> |
| Device pairing | <p>This setting toggles the availability of the option to pair with an alternative device when placing a call.</p> <p>This is on by default for desktop and web app, and is not supported on the mobile clients.</p> |
| Background blur * | <p>This setting controls whether your local background blur is enabled or not. This lets you obfuscate a distracting or sensitive background. You can also control this setting via a toggle button in your self-view window, either from within or before joining a conference.</p> <p>Note that background blur is only available on the desktop client and when using the web app on Chrome browsers. It also incurs a significant local processing overhead which could affect the performance of your device.</p> <p>Background blur is off by default.</p> |

| Setting | Description |
|---|--|
| Enable far-end camera control * | <p>This setting controls whether the currently selected camera can be controlled (if it supports pan/tilt/zoom or zoom-only) by another participant.</p> <p>The web app requires Chrome version 87 or later. You can go to <code>chrome://media-internals/</code> to check if your device's camera supports pan/tilt/zoom. Your browser will also ask for permission to allow your camera to be controlled:</p>  |
| | <p>Far-end camera control (FECC) is off by default.</p> |
| Screen sharing quality | <p>This setting determines the maximum frame rate used when you share your screen with other participants. A lower frame rate results in images with more <i>Sharpness</i> and is best for static presentations; a higher frame rate is less sharp and is best for content where there is more <i>Motion</i>. The default is 2 frames per second; the maximum is 15fps for the desktop client and 30fps for the web app.</p> <p>Note that the actual frame rate at which a presentation is sent depends on the browser, computer, network quality, and nature of the presentation.</p> |
| Import trusted key | <p>(Infinity Connect desktop client only)</p> <p>If customized branding or configuration has been applied to the client, you have to load a trusted key and confirm that you want to apply the customizations before they can take effect. Your administrator needs to supply you with the appropriate key file.</p> |
|  About this app | |
| Reset app | <p>The Reset option clears the app storage and any registration settings.</p> |
| Logs | <p>If you are having issues with your Infinity Connect client, your administrator may ask you to Download logs (web app), Open log folder (desktop client), or Copy to clipboard (mobile clients) to obtain logging information about the last call.</p> |
| <p>* The administrator can provide a first-time default for this option by Customizing and branding the Infinity Connect clients.</p> | |

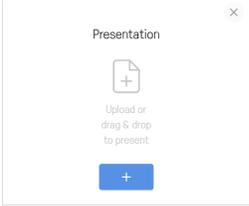
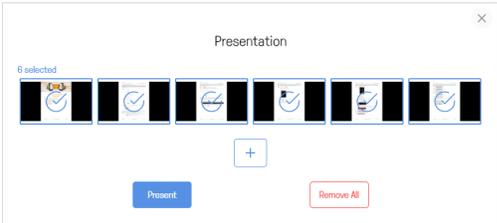
Using Infinity Connect in-call controls

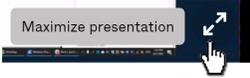
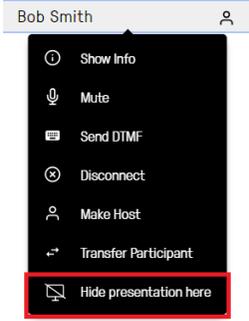
The tables below show the actions that can be performed while a call is in progress. They show the actions available through the client's [buttons, menus and keyboard shortcuts](#), followed by the actions that can be performed using [text-based commands](#).

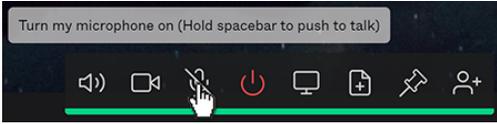
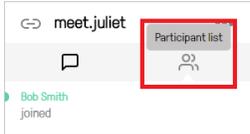
These tables include all features available to the Infinity Connect desktop client, the Infinity Connect web app and the Infinity Connect mobile clients for Android and iOS, although not all features are available to all clients.

Buttons, menus and keyboard shortcuts

| What | How | Keyboard shortcut |
|---|---|-------------------|
| Enter Host PIN (if joined as Guest) | From the toolbar at the bottom of the screen, select Enter Host PIN . | |
|  | | |
| Change your camera, microphone or speakers during a call | <ol style="list-style-type: none"> From the top of the side panel, select Control ● ● ●. Select Select media devices. Select the camera, microphone or speakers/headset, and then choose a new one from the list of available options. | |
|  | | |
| Blur your background | <p>You can select  in the self-view window to blur your local background, or  to remove the blur.</p> <p>Note that background blur is only available on the desktop client and when using the web app on Chrome browsers. It also incurs a significant local processing overhead which could affect the performance of your device.</p> | |
|  | | |
| Pin a minimized version of the client / video window to your screen | <p>Desktop client</p> <p>From the toolbar at the bottom of the screen, select Open minimized view.</p> <p>The Infinity Connect application window will shrink and be pinned on top of all your other application windows, and you can drag it to a suitable location.</p> <p>To return the window to its previous size, select Open maximized view.</p> <p>Web app</p> <p>From the toolbar at the bottom of the screen, select Float video window.</p> <p>The main video window (including thumbnails) shrinks and is pinned on top of all your other application windows. You can drag it to a suitable location.</p> <p>To return to the Chrome tab with the video window resized within it, from the pinned window select Back to tab.</p> <p>To close the pinned video window, from the toolbar select Reset video window.</p> | |
|  | | |

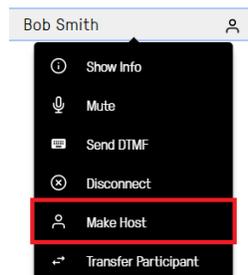
| What | How | Keyboard shortcut |
|---|--|-------------------|
| <p>Share your screen with all other participants</p>  | <p>(Available to Infinity Connect desktop client and web app on the latest desktop browsers.)</p> <ol style="list-style-type: none"> From the toolbar at the bottom of the window, select Share my screen. Select the window, screen or tab you want to share. <p>When you are sharing, the icon changes to blue. To stop sharing, select the Stop presenting button.</p> <p> The best way to share a PowerPoint presentation is to start the Slide Show from within PowerPoint first, and then tab to Infinity Connect, share your screen, and select the Slide Show window.</p> <p>Note that the ability to present into a conference may have been restricted to Hosts only.</p> | |
| <p>Share images or PDFs with all other participants</p>  | <ol style="list-style-type: none"> From the toolbar at the bottom of the screen, select Present files. <p>The Presentation screen appears:</p>  <ol style="list-style-type: none"> Select +, or drag and drop the file(s) you want to share into the Presentation window. You can add multiple files, and they can be a combination of images (JPEG, BMP, PNG or GIF) and PDFs (if supported by your device). Each image and PDF page is converted into an individual slide. By default, every slide is selected for presenting, but you can click on individual slides to select and deselect them:  <ol style="list-style-type: none"> When you have selected all the slides you want to share, select Present. Use the left < and right > on-screen controls, or the arrow keys on your keyboard, to scroll through the slides. You also have the option to  View presentation in separate window. To stop sharing the slides, from the toolbar select Stop presenting. <p>Note that the ability to present into a conference may have been restricted to Hosts only.</p> | |
| <p>View a presentation being shown by another participant</p> | <p>When a participant starts a presentation, you automatically see the content they are sharing as your main image, and the image of the participants reduces to a small thumbnail at the top left corner.</p> <p>You can toggle between viewing the presentation and viewing the participants by clicking on the thumbnail.</p> <p>You can also click and drag the thumbnail to move it.</p> | p |
| <p>View a presentation in a separate window</p>  | <p>Whether you are the presenter or a participant, you can view the current presentation in a separate pop-out window.</p> <p>To do this, from the bottom right of the screen select View presentation in separate window. To close the window, you can select Close separate presentation window.</p> | Shift + P |

| What | How | Keyboard shortcut |
|--|--|-------------------|
| <p>Expand the presentation window when it is displayed in the layout mix</p>  | <p>When receiving presentation content in an Adaptive Composition layout, the presentation stream is shown as part of the layout mix (replacing some of the other video participants), providing the client is receiving video at a medium or higher bandwidth setting (otherwise it is displayed as one large separate stream).</p> <p>You can toggle the presentation content between the "in mix" and "separate" streams via the  maximize and  reset buttons in the bottom-right corner of the presentation.</p>  | e |
| <p>View a presentation at a lower (or higher) refresh rate</p>  | <p>When a participant is showing a presentation, by default you receive it in full motion as HD video. However you may choose to receive it as a series of still images instead which may be more suitable if a very sharp image is required.</p> <p>To do this, from the bottom right of the screen select View normal presentation. To return to the default view, select View full motion presentation.</p> | |
| <p>Stop/start sending presentation to a participant</p> |  <p>(Requires Host privileges)</p> <p>When a participant is sharing a presentation, other participants receive both the presentation and the main video. However, you may want to receive just the main video on a particular endpoint (for example, if you are using a meeting room system for audio and video, but you are already viewing the presentation on your Infinity Connect client, you could stop sending presentation to the meeting room system). To do this, from the Participant list, select the participant and then select Hide presentation here.</p> | |
| <p>Start sending and receiving video</p>  | <p>(For users who have initially joined without audio and video)</p> <p>From the toolbar at the bottom of the window, select Start Video.</p> | |
| <p>Start sending and receiving audio</p>  | <p>(For users who have initially joined without audio and video)</p> <p>From the toolbar at the bottom of the window, select Start audio.</p> | |

| What | How | Keyboard shortcut |
|--|--|-------------------|
| <p>Stop/start sending your video to other participants</p>  | <p>From the toolbar at the bottom of the window, select Turn my camera off or Turn my camera on.</p> <p>Other participants will no longer be able to see you, but you will be able to see them.</p> | c |
| <p>Stop/start sending your audio to other participants</p>  | <p>From the toolbar at the bottom of the window, select Turn my microphone off or Turn my microphone on.</p> <p>Other participants will no longer be able to hear you, but you will be able to hear them.</p> <p>While your microphone is disabled, you can press and hold down the keyboard spacebar to talk.</p>  | m |
| <p>Stop/start viewing the video of yourself</p>  | <p>The video of yourself that is being sent to other participants is shown in a thumbnail at the top right of the screen. To hide this, click on the image. It is replaced by a small Show self view icon; select this to view your image again.</p> | |
| <p>Show or hide the side panel</p>  | <p>To hide or show the side panel (containing the Participant list tab and the Events tab, and the Control menu), select the Hide side panel < and Show side panel > icons. These are at the middle left or bottom of the screen, depending on your device and screen width.</p> | s |
| <p>View a list of other conference participants</p> |  <p>When using Infinity Connect, a list of all other conference participants is shown in the  Participant list tab of the control panel (which is to the left of or at the bottom of the screen, depending on the screen width). You can scroll through this list to view the names of other participants. You can also search for a particular participant using the Filter by name box at the bottom of the list.</p> <p> The /filter command lets you filter the participant list based on certain criteria such as the participants' role.</p> <p>You can show and hide the side panel by clicking on the Hide side panel < and Show side panel > icons.</p> | |

| What | How | Keyboard shortcut | | | | | | | | |
|--|--|-------------------|---|-----|---|----------|---|----------------|---|--|
| View a participant's role and video status | <p>Each person in the Participant list has an icon next to their name, representing their role:</p> <ul style="list-style-type: none">  Hosts, who can control the meeting and other participants  Guests  External Guests, who connected directly to an externally-hosted conference, such as a Microsoft Teams or Skype for Business meeting, or Google Meet. <p>Each participant also has an additional icon displayed if that participant is a streaming/recording participant, is connected as audio-only, is a video-muted Infinity Connect participant, or is inactive, for example, if they are away from the computer (and thus their face cannot be detected in their video stream):</p> <table border="0"> <tr> <td>Alice</td> <td> </td> </tr> <tr> <td>Bob</td> <td> </td> </tr> <tr> <td>Randolph</td> <td></td> </tr> <tr> <td>YouTube Stream</td> <td> </td> </tr> </table> <p>where the indicators represent:</p> <ul style="list-style-type: none">  Muted video or inactive (away)  Connected via audio only  Streaming/recording participant | Alice |   | Bob |   | Randolph |  | YouTube Stream |   | |
| Alice |   | | | | | | | | | |
| Bob |   | | | | | | | | | |
| Randolph |  | | | | | | | | | |
| YouTube Stream |   | | | | | | | | | |

Change a participant's role

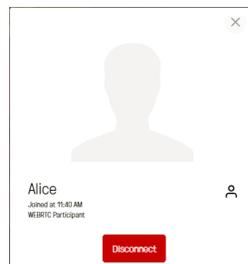


(Requires Host privileges; you cannot change your own role to Guest.)

From the **Participant list**, select the participant and then select **Make Host** or **Make Guest**.

You cannot change the role of **External Guest** participants (those who are connected directly to an externally-hosted conference, such as a Microsoft Teams or Skype for Business meeting, or Google Meet).

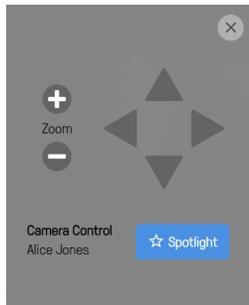
View individual participant's details



From the **Participant list**, select the participant and then select **Show Info**. This brings up an overlay dialog containing details of the participant, including their avatar or image if available (otherwise a placeholder image is shown).

| What | How | Keyboard shortcut |
|------|-----|-------------------|
|------|-----|-------------------|

Control another participant's camera



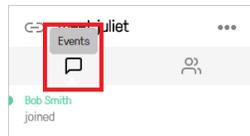
(

Requires Host privileges. This feature must be enabled by an Administrator; not all endpoints can be controlled remotely.)

From the participant list, select the participant whose camera you want to control, and then select **Camera control** (for person-to-person calls, this option is also available via the **Camera control** button on the toolbar).

The **Camera Control** overlay appears. Use the buttons on the overlay, or your keyboard arrow and + or - keys, to pan, tilt and zoom the camera at the far end. For calls in a Virtual Meeting Room or Virtual Auditorium you can also select **Spotlight** to bring the participant into the main video window for as long as the **Camera Control** overlay is open.

View details of events



Shift + S

To see a list of conference events that have occurred during the course of the call (participants joining, leaving, presenting etc.), from the top of the side panel select the **Events** tab:

Send and receive chat messages, and share online videos and images

(Available when chat has been enabled by the administrator)

All events, including chat messages, are shown in the  **Events** tab of the side panel (which is to the left of or at the bottom of the screen, depending on the screen width).

To send a message, type it in the text box at the bottom of the panel:

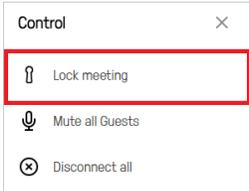
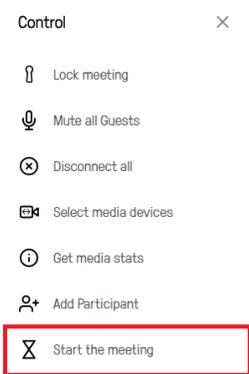


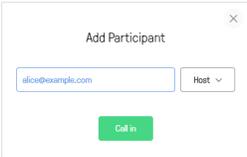
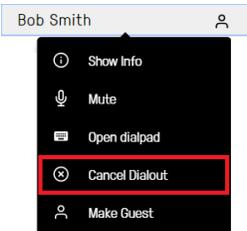
Messages are visible to everyone else in the conference with a chat-capable client (such as Skype for Business or Infinity Connect).

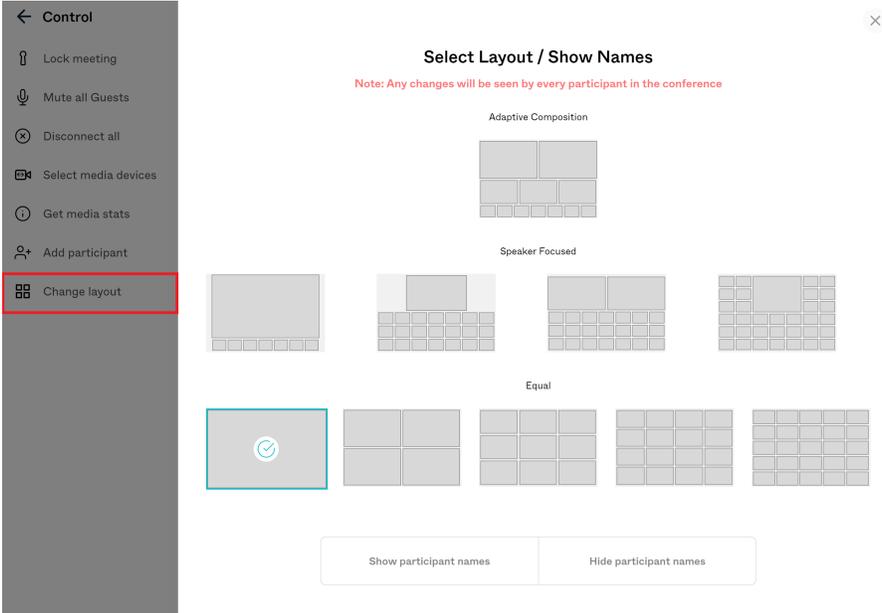
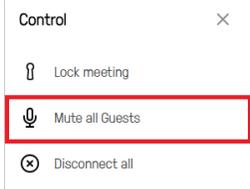
You can also share videos and images by pasting their URL into the text box.

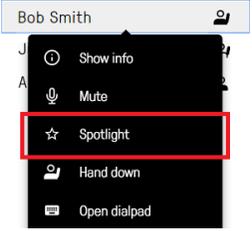
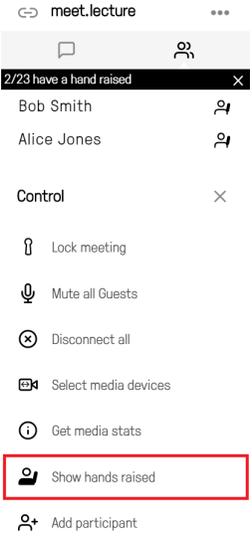
A visual indicator is displayed when a new chat message is received. It is displayed against the **Events** tab if the side panel is open and showing the participant list, or above the button used to show the side panel if the side panel is closed.

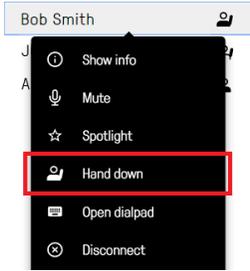
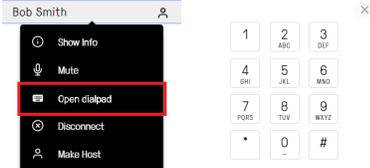
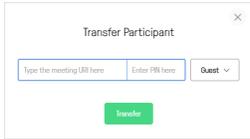


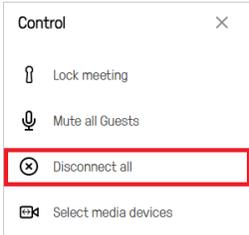
| What | How | Keyboard shortcut |
|---|--|-------------------|
| Prevent/allow others from joining the meeting |  <p>(Requires Host privileges)</p> <p>From the top of the side panel, select Control ● ● ● and then select Lock meeting or Unlock meeting: The impact of locking depends on whether or not the meeting has a Host PIN. For more information, see Locking a conference and allowing participants to join a locked conference.</p> | |
| Allow a participant to join a locked conference |  <p>(Requires Host privileges)</p> <p>Participants who are waiting to join a locked conference are shown in the Participant list with a tick and cross next to their names. To allow these participants to join the conference, select the green tick. If you do not want them to join, select the red cross.</p> | |
| Allow waiting Guests to join a new meeting without a Host |  <p>(Requires Host privileges)</p> <p>If a Guest joins a meeting without a Host, they are kept waiting to join until the first Host joins, at which point all waiting Guests are automatically allowed in to the meeting. However, this only applies if the Host has joined with audio or video; presentation and control-only Hosts do not automatically trigger Guests to join.</p> <p>If you have joined a meeting as a presentation and control-only Host and want Guests to join, from the top of the side panel, select Control ● ● ● and then select Start the meeting.</p> | |

| What | How | Keyboard shortcut |
|--|---|-------------------|
| <p>Add a participant to the conference</p>  |  <p>(Requires Host privileges)</p> <ol style="list-style-type: none">1. From the toolbar at the bottom of the screen, select Add participant.2. At the prompt, enter the address of the person you want to dial.3. Select whether you want the participant to have Host or Guest privileges.4. Select Call in. <p>The call is placed from the conference to the participant and they appear in the participant list with a green line under their name while their endpoint is ringing. If and when the participant answers the call they will join the conference; if they do not answer, or do not accept the call, they will disappear from the participant list.</p> <p>i Automatic routing is used when an Infinity Connect client adds a new participant to a conference. This means that the dialed alias must match an appropriate Call Routing Rule that applies to Outgoing calls from a conference for the call to be placed (using the protocols and call control systems etc. as configured for that rule).</p> | a |
| <p>Cancel a call to a participant</p> |  <p>(Requires Host privileges)</p> <p>Outbound calls are placed from a Virtual Meeting Room to a participant when a Host uses the Add participant option, or if the Virtual Meeting Room has an automatically dialed participant configured.</p> <p>To cancel an outbound call, from the Participant list, select the participant and then select Cancel Dialout.</p> | |

| What | How | Keyboard shortcut |
|--|---|-------------------|
| <p>Change the layout and show/hide participant names</p> | <p>(Requires Host privileges)</p> <p>From the top of the side panel, select Control ● ● ● and then select Change layout.</p> <p>This opens an overlay dialog from where you can dynamically change the layout being used — just select the layout you want to use. You can also use the buttons at the bottom of the overlay to toggle the display of participant names on and off.</p>  | |
| <p>Share a link to the meeting</p> |  <p>If you want to send a link to the meeting to someone so that they can join you, select the Share icon at the top left of the screen and then select Copy meeting link.</p> <p>You can then send this link to other participants who can paste it into their browser to join the meeting.</p> | |
| <p>Mute/unmute another participant</p>  | <p>(Requires Host privileges)</p> <p>From the Participant list, select the participant and then select Mute or Unmute.</p> <p>When muted, a  icon is shown next to the participant's name.</p> | |
| <p>Mute all Guest participants</p> |  <p>(Requires Host privileges)</p> <p>From the top of the side panel, select Control ● ● ● and then select Mute all Guests.</p> | |

| What | How | Keyboard shortcut |
|--|---|-------------------|
| <p>Keep a participant in the main video</p> |  <p>(Requires Host privileges)</p> <p>From the Participant list, select the participant and then select Spotlight.</p> <p>For more information, see Spotlighting a participant.</p> | |
| <p>Indicate that you wish to speak</p>  | <p>(Virtual Auditoriums only by default)</p> <p>From the toolbar at the bottom of the screen, select Raise my hand. The meeting Host is alerted that your hand is raised. If you no longer wish to speak, you can select the button again to Lower my hand.</p> <p>The meeting Host can also lower your hand.</p> | |
| <p>View all participants with raised hands</p> | <p>(Virtual Auditoriums only by default; requires Host privileges)</p>  <p>From the top of the side panel, select Control ● ● ● and then select Show hands raised.</p> <p>Participants are listed in the order that they raised their hand.</p> | |

| What | How | Keyboard shortcut |
|--|--|-------------------|
| Lower a participant's raised hand |  <p>(Virtual Auditoriums only by default; requires Host privileges)</p> <p>From the Participant list, select the participant and then select Hand down.</p> <p>A participant can also lower their own hand.</p> | |
| Send DTMF tones to another participant (when in a VMR) | <p>(Requires Host privileges; you must be joined over audio, or video and audio)</p> <p>From the Participant list, select the participant and then select Open dialpad. This opens a keypad:</p>  <p>This feature is generally used to communicate with external systems (such as audio bridges, automated switchboards, and recording devices) after they have been added to the conference.</p> | |
| Send DTMF tones to the other participant (when in a person-to-person call) |  <p>From the toolbar at the bottom of the window, select Open dialpad. This opens a keypad.</p> | |
| Transfer a participant to another VMR |  <p>(Requires Host privileges)</p> <p>From the Participant list, select the participant and then select Transfer Participant.</p> <p>Enter the alias of the conference you wish to transfer the participant to, the PIN (if applicable) and whether they should join as a Guest or Host, and then select Transfer.</p> <p>You can transfer any participant, including yourself.</p> | |
| Disconnect another participant | <p>(Requires Host privileges)</p> <p>From the participant list, select the participant's name and then select Disconnect.</p> | |

| What | How | Keyboard shortcut |
|---|---|-------------------|
| Disconnect all participants (including yourself) |  <p>(Requires Host privileges)</p> <p>From the top of the side panel, select Control ● ● ● and then select Disconnect all.</p> | |
| Disconnect yourself from the conference | <p>From the toolbar at the bottom of the screen, select Disconnect.</p>  | |
| Mute/unmute the audio coming from the conference | <p>From the toolbar at the bottom of the screen, select Mute/Unmute incoming audio.</p>  | |
| Change the volume of the audio coming from the conference | <p>Desktop client and web app:</p> <p>From the toolbar at the bottom of the screen, use the slider to adjust the volume level (which is indicated by the green bar under the toolbar).</p>  <p>Mobile app:</p> <p>Use your device's volume controls.</p> | |

| What | How | Keyboard shortcut |
|------|-----|-------------------|
|------|-----|-------------------|

View diagnostic information about your call and client

✕

Media Statistics

| Audio | | | |
|------------------------|--------|--------|-------|
| | In | Out | |
| Packets Transmitted | 95293 | 95293 | 95291 |
| Packets Lost | 0 | 0 | 0 |
| Total Percentage Lost | 0.0% | 0.0% | 0.0% |
| Recent Percentage Lost | 0.0% | 0.0% | 0.0% |
| Bitrate | 69kbps | 19kbps | |
| Codec | opus | opus | |

| Video | | | |
|------------------------|----------|-----------|--|
| | In | Out | |
| Packets Transmitted | 92744 | 131950 | |
| Packets Lost | 35 | 0 | |
| Total Percentage Lost | 0.0% | 0.0% | |
| Recent Percentage Lost | 0.0% | 0.0% | |
| Bitrate | 531kbps | 436kbps | |
| Codec | VP9 | VP9 | |
| Resolution | 1280x720 | 1280x720 | |
| Configured Bitrate | N/A | 512.0kbps | |
| Decoder Delay | 5ms | N/A | |

Software versions
 Client version 1.3.1 (chrome v69 on Win32)
 Server version v20 (45159.0.0)

(Available when connected with audio or video)

From the top of the side panel, select **Control** ● ● ● and then select **Get media stats**.

This brings up an overlay dialog that displays statistics such as the codec being used, incoming and outgoing audio and video bitrates, and how many data packets have been lost and received.

It also shows the software version of the client and the Pexip Infinity deployment it is connected to.

Use a text-based interface to filter participants and control the conference

Some tasks can be performed using a command-line-style text input from within the **Filter by name** box at the bottom of the **Participant list**.

Hosts and Guests can filter the list of participants based on criteria such as their role or who is currently speaking. Hosts can also perform other conference control functions such as muting and unmuting participants, spotlighting a participant, and turning the text overlay on and off.

To view a full list of available commands, type **/** into the **Filter by name** box.

Text-based controls

The following actions can be performed by typing the relevant commands into the **Filter by name** box at the bottom of the **Participant list**:

| Command | Description |
|-----------------------------|---|
| Host-only commands | |
| /lock | Lock and unlock the meeting. |
| /unlock | |
| /mute [participant]† | Mute and unmute another participant. |
| /unmute [participant]† | |
| /muteall | Mute and unmute all Guest participants. |
| /unmuteall | |
| /handsdown [participant]* † | Lower a participant's <u>raised hand</u> . |
| /handsdownall* | Lower all participants' <u>raised hands</u> . |
| /disconnect [participant]† | Disconnect a participant. |

| Command | Description | |
|--------------------------------|--|------------------------------------|
| /disconnectall | Disconnect all participants (including yourself). | |
| /spotlight on [participant]† | Put a participant into the main video window. For more information, see Spotlighting a participant . | |
| /spotlight off [participant]† | | |
| /overlay on | Turn text overlay of participant names on and off. | |
| /overlay off | | |
| /layout 1:0 | Change the layout of the main video window and thumbnails. In a Virtual Meeting Room, this affects the view seen by all participants. In a Virtual Auditorium, this affects the view seen by Host participants. | |
| /layout 1:7 | | |
| /layout 1:21 | | |
| /layout 2:21 | | |
| /layout 1:33 | | |
| /layout 2x2 | | |
| /layout 3x3 | | |
| /layout 4x4 | | |
| /layout 5x5 | | |
| /layout AdaptiveComposition | | |
| Host and Guest commands | | |
| /shortcuts | | View a list of keyboard shortcuts. |
| /hand up* | | Raise or lower your hand. |
| /hand down* | | |
| /filter host | Filter the list of participants by the given criteria. | |
| /filter guest | | |
| /filter handraised* | | |
| /filter spotlight | | |
| /filter speaking | | |
| /filter streaming | | |
| /filter external | | |
| /filter waiting | | |
| /filter audio-only | | |
| /filter control-only | | |

* Available in Virtual Auditoriums only.

† When you start entering a participant's name, the participant list is filtered to show only those participants with those characters in their name.

Registering and provisioning the Infinity Connect desktop client

The Infinity Connect desktop client can register to a Pexip Infinity Conferencing Node. This enables it to:

- receive calls (as well as place them)
- use directory services to filter and lookup the contact details (phone book) of other devices or VMRs that are set up on the Pexip Infinity platform, making it easier to call those addresses.

i Registration is optional. You do not need to register your device in order to make calls.

The Infinity Connect desktop client can also be provisioned with branding details, allowing it to use the same branding as used by the web app.

The mobile clients do not support provisioning, registration or branding/customization.

This topic covers the client [authentication options](#), the [DNS requirements](#), how to [provision the clients](#), some [example provisioning email template content](#), and a description of the associated [user experience](#).

Client authentication options

When registering an Infinity Connect client to Pexip Infinity, the alias being registered by the client must match one of the entries on the Management Node under **Users & Devices > Device Aliases**. When configuring a device alias, you can specify whether and how an Infinity Connect client that is attempting to register with that alias should authenticate itself (authentication is optional but recommended):

- **SSO**: the client uses Single Sign-On (SSO) services such as AD FS to authenticate the registration.
- **Non-SSO**: the username and password credentials associated with the device alias are used to authenticate the registration.

For any given alias, we recommend that you enable Infinity Connect registrations for either SSO or non-SSO authentication, not both.

Setting up appropriate DNS records

The Infinity Connect desktop client uses its configured **Registration Host** and performs a DNS SRV lookup on **_pexapp._tcp.<registration host address>** to locate a Conferencing Node to which it can send its registration request.

You must therefore ensure that appropriate DNS records have been set up — for more information, see [Setting up DNS records for mobile and desktop client use](#).

Provisioning the Infinity Connect desktop client with registration and/or branding details

Users can manually enter their registration details (alias, credentials, registration host address) into their Infinity Connect desktop client. However, as an administrator you can simplify this process by provisioning individual users with their registration details and automatically applying those registration settings to their Infinity Connect desktop client.

You can also provision the Infinity Connect desktop client with instructions to use the same app branding that has been uploaded to Pexip Infinity (and which is being used automatically by the web app). Note that the mobile clients do not support provisioning, registration or branding.

You perform these provisioning tasks by supplying each user with a provisioning URI in the format:

`https://<node_address>/api/client/v2/provision?data=<Base64 encoded name-value pairs>&message=<Base64 encoded message>`

where:

- **<node_address>** is the address of a Conferencing Node. You must ensure that when the end-user attempts to provision their client that they are able to reach the specified node.
- **<Base64 encoded name-value pairs>** are the data values used to provision the client, and are described below.
- **<Base64-encoded message>** is the provisioning message that is displayed to the user. The **message** parameter is optional and by default is "Your Pexip App should have opened and asked to be provisioned. You can now close this window."

Base64 encoding is used to ensure that the data does not get modified by email clients. Note that Base64-encoded data is not encrypted.

For example, the provisioning URI might look like this:

`https://px01.vc.example.com/api/client/v2/provision?data=ZzUmVkaXJl...etc...D%3D&message=bkgY3VzdG9tIG1lc3Nh`

This provisioning URI can be inserted into email messages without the risk of the link being disabled (unlike the [alternative pexip-provision://](#) URI scheme). This means users will have a directly clickable link without needing to copy and paste the link into their web browser.

Provisioning name-value pairs

The name-value pairs that can be provisioned in the data query string parameter are described in the following table. If you use Pexip Infinity to bulk provision device aliases and generate emails to each user, you can use the provided template variables and custom Pexip filters to obtain the values for some of the data items and generate the relevant URIs for each user/client.

Each name-value pair must be separated by an &. For example (prior to Base-64 encoding):

`name=Alice®istrationHost=px01.vc.example.com®istrationAlias=alice@example.com®istrationUsername=alice®istrationPassword=password123`

The table shows the common data items, and the additional data items that are used for AD FS SSO authentication:

| Name | Value | Suggested sync template variable |
|----------------------|---|---|
| name | The name of the user as it will appear to other conference participants. | device_username |
| registrationHost | The domain, IP address or FQDN of the Conferencing Node to which the client should register, for example <code>px01.vc.example.com</code> . For more information, see Setting up DNS records for mobile and desktop client use . | There is no suitable variable for this, as it is not a user specific value. |
| registrationAlias | The alias of the device to register to Pexip Infinity. | device_alias |
| registrationUsername | The username associated with the device alias (registrationAlias). This does not apply if you are using SSO services. | device_username |
| registrationPassword | The password associated with the device alias (registrationAlias). This does not apply if you are using SSO services. | device_password |
| brandingURL | A reference to a directory (on an accessible server) that contains customized branding configuration. You typically use this to instruct the desktop client to use the same branding as the web app. Prior to version 1.8 of the desktop client, the branding package could be hosted on a Conferencing Node. From 1.8 this is not allowed and the package must be hosted on a different external server. See Customizing and branding the Infinity Connect clients for more information. | There is no suitable variable for this, as it is not a user specific value. |

Additional data items when using AD FS SSO authentication

| Name | Value | Suggested sync template variable |
|-----------------------------|---|--|
| adfsFederationServiceName † | The Federation Service name e.g. adfs.example.com. | There are no suitable variables for these items, as they are not user specific values. |
| adfsResource † | The Resource Identifier e.g. https://pexipappsso.local. | |
| adfsClientID † | The Client ID e.g. a2a07b42-66d7-41e4-9461-9d343c25b7f3. | |
| adfsRedirectURI | <p>This is the URI you want the user to be redirected back to after they sign into AD FS. It does not correspond with a value configured on the Management Node but it must be one of the redirect URIs you set up when configuring AD FS on your Windows Server. We recommend you use:</p> <p>https://<address>/api/client/v2/oauth2_redirect where <address> is the FQDN of a Conferencing Node or reverse proxy, for example https://px01.vc.example.com/api/client/v2/oauth2_redirect.</p> <p>When the oauth2_redirect page loads it opens the Infinity Connect client to complete the sign-in process. The oauth2_redirect page will remain open but it displays a message which by default is "You have successfully signed in. You can now close this window."</p> <p>You can change this message by including the optional base64-encoded message parameter on the oauth2_redirect page URL. For example, the message "my custom message" is "bXkgY3VzdG9tIG1lc3NhZ2U=" when base64-encoded. You would then specify the adfsRedirectURI as follows: https://confnode.example.com/api/client/v2/oauth2_redirect?message=bXkgY3VzdG9tIG1lc3NhZ2U=</p> | |

† These AD FS related data values should correspond to what you have configured in Pexip Infinity (**Users & Devices > AD FS Authentication Clients**) for the OAuth 2.0 Client.

Notes:

- You do not have to provision all of the common name-value data items — if you supply a subset of the data, the user can manually enter the additional data if required.
- When using AD FS SSO provisioning, all of the AD FS data items must be included in the provisioning data.

Example device email template content

The following example content for a device provisioning email template shows how you can build the relevant URI with base64-encoded provisioning data (using device provisioning variables populated from LDAP) and provide a clickable link for the recipient of the email that will provision their client. The first line in this example defines and sets various variables and the second line incorporates those variables in the paragraph text and link that is displayed to the recipient.

```
{%set provisiondata = "name=" + device_username|capitalize +
"&registrationHost=confnode.example.com&registrationAlias=" + device_alias +
"&registrationUsername=" + device_username + "&registrationPassword=" + device_password
%}
<p>You can open <a href="https://confnode.example.com/api/client/v2/provision?{{pex_url_encode(('data', provisiondata|pex_base64)}}}">this link</a> to automatically configure your client.</p>
```

Remember to substitute **confnode.example.com** with the address of your Conferencing Node.

You can extend the previous example and include the **message** URL parameter (set to 'Provision your app' in this example) in the provisioning link (the `{%set}` statement is identical to the previous example):

```
{%set provisiondata = "name=" + device_username|capitalize +
"&registrationHost=confnode.example.com&registrationAlias=" + device_alias +
"&registrationUsername=" + device_username + "&registrationPassword=" + device_password
%}
```

<p>You can open this link to automatically configure your client.</p>

AD FS SSO examples

This is an example of a provisioning link which can be used to set up Single Sign-On via AD FS:

```
{%set provisiondata = "name=" + device_username|capitalize +
"&registrationHost=confnode.example.com&registrationAlias=" + device_alias +
"&adfsFederationServiceName=adfs.example.com&adfsResource=https://pexipappsso.local&adfs
ClientID=a2a07b42-66d7-41e4-9461-
9d343c25b7f3&adfsRedirectURI=https://confnode.example.com/api/client/v2/oauth2_redirect"
%}
```

<p>Simply open this link to configure your client automatically.</p>

Remember to substitute `confnode.example.com` with the address of your Conferencing Node, and to set the `adfsFederationServiceName`, `adfsResource` and `adfsClientID` variables with the appropriate values for your AD FS service.

This next example shows how to include the "successfully signed in" message URL parameter (set to 'Successfully signed-in message' in this example) in the `oauth2_redirect` link:

```
{%set provisiondata = "name=" + device_username|capitalize +
"&registrationHost=confnode.example.com&registrationAlias=" + device_alias +
"&adfsFederationServiceName=adfs.example.com&adfsResource=https://pexipappsso.local&adfs
ClientID=a2a07b42-66d7-41e4-9461-
9d343c25b7f3&adfsRedirectURI=https://confnode.example.com/api/client/v2/oauth2_
redirect?" + pex_url_encode(('message', 'Successfully signed-in message'|pex_base64)) %}
```

<p>Simply open this link to configure your client automatically.</p>

This final example shows how the "successfully signed in" message (on the `oauth2_redirect` URL) and the "provision your app" message (on the `provision` URL) can be customized:

```
{%set provisiondata = "name=" + device_username|capitalize +
"&registrationHost=confnode.example.com&registrationAlias=" + device_alias +
"&adfsFederationServiceName=adfs.example.com&adfsResource=https://pexipappsso.local&adfs
ClientID=a2a07b42-66d7-41e4-9461-
9d343c25b7f3&adfsRedirectURI=https://confnode.example.com/api/client/v2/oauth2_
redirect?" + pex_url_encode(('message', 'Successfully signed-in message'|pex_base64)) %}
```

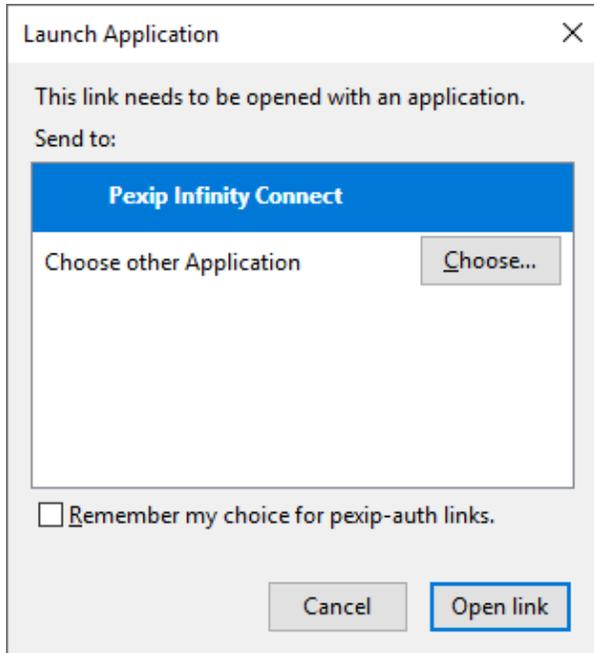
<p>You can open this link to automatically configure your client.</p>

User experience when using the provisioning link

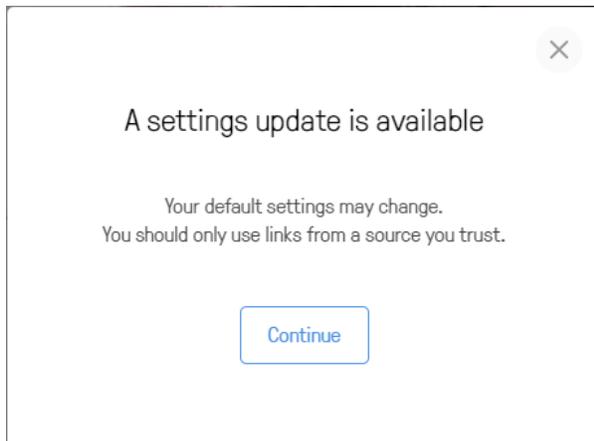
Non-SSO provisioning

When the user clicks on the provisioning link, they are typically asked to confirm or authorize the launch of the Infinity Connect application (the exact nature of the request varies according to the platform and the method of launching the link) and then the

Infinity Connect client will launch and present the user with a confirmation screen:



1. Select **Open Link** to launch Infinity Connect.

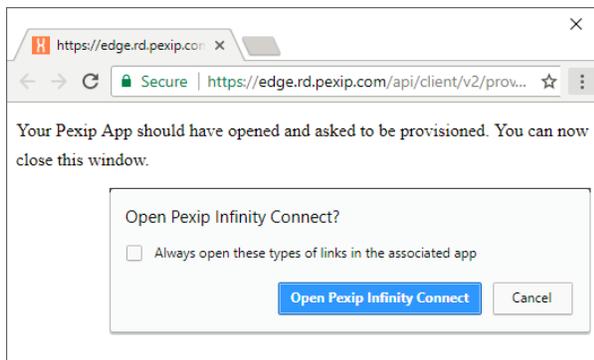


2. Select **Continue** to apply and save the settings contained in the provisioning link.

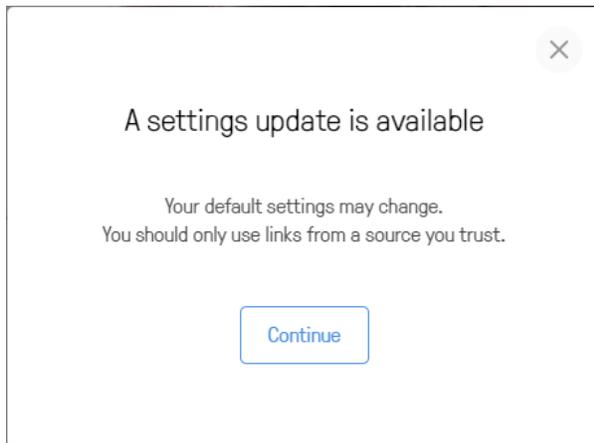
The registration settings in the client are read-only when the client is successfully registered — you must **Unregister** if you want to change them.

AD FS SSO provisioning

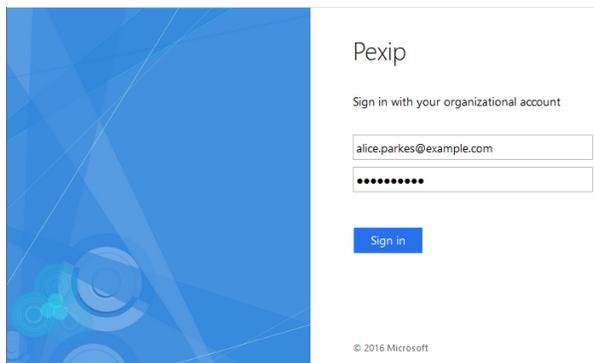
When AD FS SSO provisioning is used, the user is also prompted to sign in to AD FS with their AD credentials. Here are some examples of the screens that are displayed during the provisioning process (the exact nature varies according to the platform, browser and whether the messages have been customized):



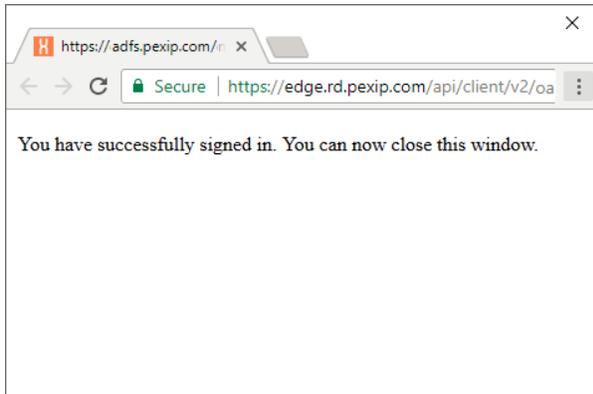
1. Confirm to open the Infinity Connect client.



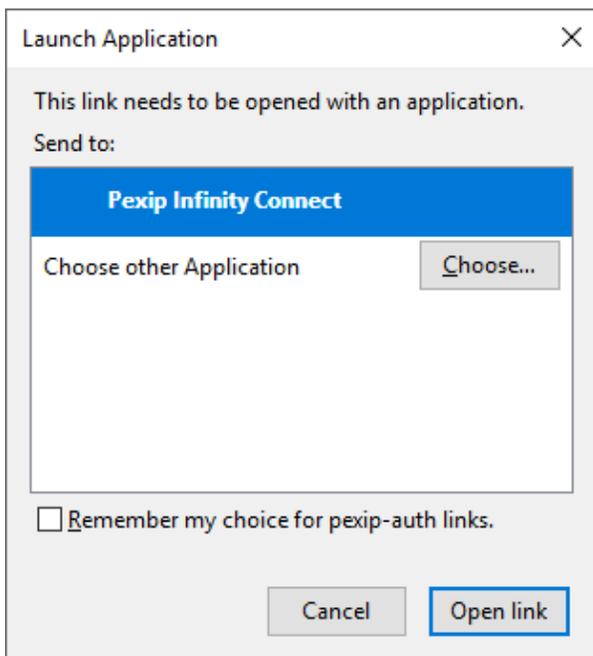
2. Select **Continue** to proceed with provisioning the client.



3. Sign in to AD FS.



4a. AD FS sign-in successful.



4b. Select Open Link to launch Infinity Connect and complete the sign-in process.

When a client has been configured (provisioned) with SSO registration information, the user name / password fields are blank and the registration settings can only be modified by resetting the app.

Alternative pexip-provision:// URI provisioning scheme

When the Infinity Connect desktop client installs, it registers itself to the `pexip-provision://` URI scheme. This provides an alternative provisioning URI that can be used to configure the client with personalized settings for each user. This URI takes the following format:

`pexip-provision://settings/?data=<Base64 encoded name-value pairs>`

where `data` is set to the same set of `name-value pairs` as described above.

- i** We recommend using the `https://<node_address>/api/client/v2/provision` style links instead of the `pexip-provision://` style links, as some mail clients (such as gmail) disable embedded `pexip-provision://` style links and other mail clients (such as Outlook) may present users with a security notice warning that the hyperlink may be unsafe and users must choose to continue in order to launch the application.

The following example content for a device provisioning email template shows how you can build the relevant pexip-provision:// URI with base64-encoded provisioning data (using device provisioning variables populated from LDAP) and provide a clickable link for the recipient of the email that will provision their client.

```
{%set provisiondata = "name=" + device_username|capitalize +
"&registrationHost=px01.vc.example.com&registrationAlias=" + device_alias +
"&registrationUsername=" + device_username + "&registrationPassword=" + device_password
%}

<p>You can open <a href="pexip-provision://settings?data={{provisiondata|pex_base64}}">
this link</a> to automatically configure your client.</p>
```

The generated URI for "this link" will take the form `pexip-provision://settings?data=bmFtZT1...etc...HVhcA==`

Using Infinity Connect to share content

You can use Infinity Connect to share content such as [images and PDFs](#), or [what's on your screen](#), with other participants.

If you are already in the call using another video endpoint, you can use Infinity Connect [just to share content](#) — for example, if you have joined the conference from a meeting room with a dedicated endpoint, and you want to show a presentation from your laptop without worrying about finding and connecting the correct cables.

You can also use the text/chat box in the side panel to share videos and images with other Infinity Connect users — just paste the URL of the content you want to share into the chat box (content may be blocked if you are using a reverse proxy with HTTP Content Security Policy (CSP) enabled).

Note that:

- An administrator can configure individual Virtual Meeting Rooms and Virtual Auditoriums so that Guest participants are not allowed to present into the conference (they can still receive presentation content from other Host participants). By default, Guests are allowed to present content.
- When someone is **sharing their screen**, their content is sent to other participants at 2 fps by default. However, the presenter can change this rate prior to sharing their screen by selecting **Settings > Advanced Settings > Screen sharing quality**. Note that this setting does not influence the frame rate used when **sharing files and images**, which are only updated each time the file or image changes.

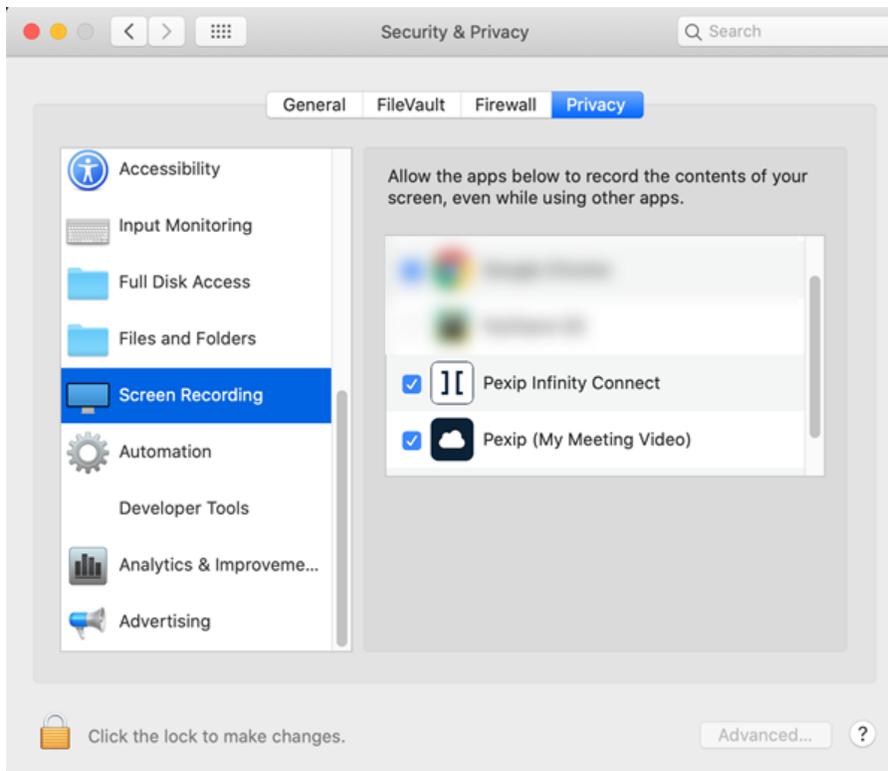
Sharing your screen

Screen sharing is available when using the Infinity Connect desktop client, and the web app on the latest desktop browsers (minimum versions: Chrome v72, Firefox v52, Opera v60, Edge Chromium).

Screen sharing is not supported in Safari on macOS, Safari on iOS/iPadOS, or any other browser on iOS/iPadOS.

macOS permissions

Users of macOS 10.15 and later must explicitly grant permission to individual apps to access the device's screen sharing functionality. This permission must be granted to the Infinity Connect desktop client or to any browsers used to access the Infinity Connect web app, in order for screen sharing to be enabled. This is done via the device's **System Preferences > Security & Privacy > Screen Recording** setting:



Frame rate

You can set the frame rate to use when sharing your screen. A lower frame rate produces *sharper* images and is best for static presentations, whereas a higher frame rate is less sharp and is best for content where there is more *motion*. You must set the frame rate to use before you join the conference via Settings > Advanced Settings > Screen sharing quality.

Infinity Connect web app via Chrome, Edge, or Opera

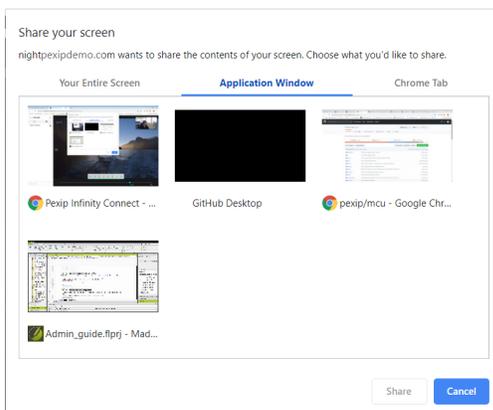
You can choose to share the whole screen, an individual application, or an individual tab. To share your screen:

1. From the toolbar at the bottom of the screen, select Share my screen:



2. From the Your Entire Screen, Application Window, or browser Tab options, select what you want to share.

i Any applications that are currently minimized won't appear on the list.



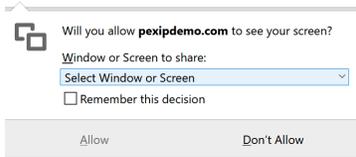
Infinity Connect web app via Firefox

You can choose to share the whole screen, or you can select an individual application window to share. To share your screen:

1. From the toolbar at the bottom of the screen, select **Share my screen**:



2. Select the window or screen you want to share (any applications that are currently minimized won't appear in the list):



Infinity Connect desktop client

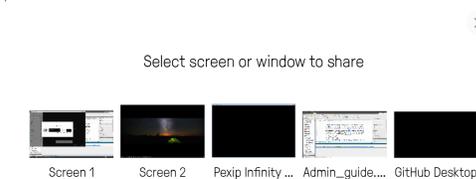
You can choose to share the whole screen, or you can select an individual application window to share. To share your screen:

1. From the toolbar at the bottom of the screen, select **Share my screen**:



2. From the **Your Entire Screen** or **Application Window** options, select what you want to share.

 Any applications that are currently minimized won't appear on the list.



Sharing images and PDFs

When sharing images or PDFs:

- You can share **images** from any Infinity Connect client. Supported image formats are JPEG, BMP, PNG and GIF.
- You can share **PDFs** directly from the Infinity Connect desktop client, web app (except when used on iOS/iPadOS), and mobile client for Android.
- You can't share **PowerPoint** presentations directly via the apps. To share a PowerPoint presentation, either save the presentation as a PDF and share that, or open the presentation as a slide show and then share your screen.

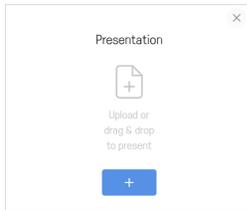
Selecting the images or PDFs to share

To share images or PDFs:

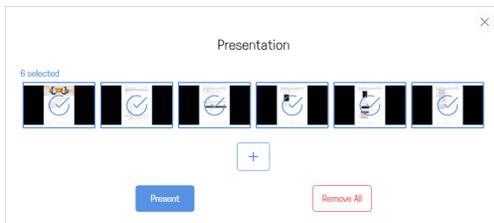
1. From the toolbar at the bottom of the screen, select **Present files**:



The **Presentation** screen appears:



2. Select +, or drag and drop the file(s) you want to share into the **Presentation** window. You can add multiple files, and they can be a combination of images (JPEG, BMP, PNG or GIF) and PDFs (if supported by your device). Each image and PDF page is converted into an individual slide.
3. By default, every slide is selected for presenting, but you can click on individual slides to select and deselect them:



4. When you have selected all the slides you want to share, select **Present**. Use the left < and right > on-screen controls, or the arrow keys on your keyboard, to scroll through the slides. You also have the option to  **View presentation in separate window**.
5. To stop sharing the slides, from the toolbar select **Stop presenting**:



-  Any files you share remain yours — they are not available for other participants to download during or after the conference.

Using Infinity Connect for presentation, chat and conference control only

If you are already in a conference using an endpoint other than Infinity Connect (for example, a dedicated meeting room system), you can still access the additional features available to Infinity Connect users (such as conference control, chat, content sharing and viewing, and viewing the participants list) by using Infinity Connect to join the conference without sending or receiving audio or video — in other words, as a presentation and control-only participant.

To join a conference as a presentation and control-only participant:

1. Open the Infinity Connect client on your computer or mobile device.

2. Select  content .

3. In the box at the top right of the window, enter the address of the meeting you wish to join:



4. Either click on the icon to the right of the box, or press enter.

The client joins the conference as a presentation and control-only participant — it does not send or receive any audio or video from other participants.

You can now [share your screen](#) or [share images and PDFs](#), and view content being shared by other participants. You can also send and receive chat messages, view the participant list, and (if you are a Host) control aspects of the conference such as adding participants, muting participants, disconnecting participants, and locking the conference.

At any point in the call you can also start sending and receiving audio or video from the client. To do this, select **Start video** or **Start audio** from the toolbar at the bottom of the screen:



Locking a conference and allowing participants to join a locked conference

You can lock a conference if you want to prevent any further participants from joining a conference after it has started. A conference can be locked and unlocked by conference participants [using Infinity Connect](#) or [using DTMF-enabled endpoints](#), or by [using the Administrator interface](#).

When a conference is locked, any new participants who attempt to join the conference are held at a waiting screen. They can be [allowed in individually](#) by Infinity Connect participants (Hosts only) already in the conference.

The exact locking behavior depends on whether or not the Virtual Meeting Room or Virtual Auditorium being used has a Host PIN.

If the service **does not have a Host PIN**:

- Participants are able to join the conference until it is locked.
- When the conference is locked:
 - A conference locked indicator  is displayed.
 - Any further participants who attempt to join the conference (including any Automatically Dialed Participants and manually-invited participants who have been given a role of Guest) are held at the **Waiting for the host** screen. However, any ADPs and manually-invited participants with a role of Host will join the conference immediately.
 - All participants who are already in the conference are notified of any participants who are attempting to join the locked conference, and can [allow the waiting participants to join](#). Notifications take the form of an on-screen message and an audio message/alert for each participant attempting to join.
- If the conference is unlocked, any participants who are still waiting will automatically join the conference.

If the service **has a Host PIN**:

- Host and Guest participants are able to join the conference until it is locked.
- When the conference is locked:
 - A conference locked indicator  is displayed to Host participants.
 - New participants who enter the Host PIN will join the conference immediately — locking does not apply to them.
 - Any new Guest participants (including any Automatically Dialed Participants and manually-invited participants who have been given a role of Guest) are held at the **Waiting for the host** screen.
 - All Host participants who are already in the conference are notified of any Guest participants who are attempting to join the locked conference, and can [allow the waiting Guest participants to join](#). Notifications take the form of an on-screen message and an audio message/alert for each participant attempting to join.
- If the conference is unlocked, any Guest participants who are still waiting will automatically join the conference.

All of the on-screen indicators, messages and the **Waiting for the host** screen can be fully customized via the theme associated with your services.

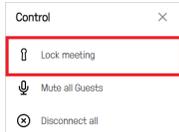
Locking using the Administrator interface

To lock or unlock a conference from the Administrator interface:

1. Log into the Pexip Infinity Administrator interface.
2. Go to **Status > Conferences**.
3. From the **Service name** column, select the conference you want to lock or unlock.
4. At the bottom left of the page, select **Lock conference** or **Unlock conference** as appropriate.

Locking using Infinity Connect

Host participants using Infinity Connect can lock and unlock the conference they are in by going to the side panel, selecting **Control**  and then selecting **Lock meeting** or **Unlock meeting** as appropriate:



 Host participants using Infinity Connect can also use the [commands](#) `/lock` and `/unlock`.

Locking using DTMF

If DTMF controls have been enabled, Host participants using telephones or SIP/H.323 endpoints can lock and unlock the conference using DTMF. The default DTMF entry to do this is `*7` but this may have been customized.

Allowing waiting participants to join a locked conference

When a new participant attempts to join a locked conference, all Host participants (on any endpoint) in the conference are notified that a participant is waiting to join. However, only Host participants who are using Infinity Connect can admit individual participants into the conference.



Participants who are waiting to join a locked conference are shown in the **Participant list** with a tick and cross next to their names. To allow these participants to join the conference, select the green tick. If you do not want them to join, select the red cross.



Note that if the Host has joined as presentation and control-only (and there are no other Host participants), the Host is not offered the telephone icons. However, they can use the **Start the meeting** menu option, which will let in all Guest participants.

If a conference is unlocked, all participants who are still waiting will automatically join the conference.

Rejecting a request to join a locked conference

If a Host (who is using Infinity Connect) does not want a waiting participant to join the conference immediately, they have two options:

- To reject the request completely, the Host participant must click on the red cross icon next to the waiting participant's name. The waiting participant's call will be disconnected.
- To leave the participant at the waiting for Host screen, the Host participant should do nothing. The waiting participant will remain at the waiting screen until:
 - a Host participant chooses to let the waiting participant join the conference, or
 - the conference is unlocked (after which the waiting participant will automatically join the conference), or
 - the participant has been waiting for longer than the [specified waiting time](#) (after which the participant will be disconnected)
 - the conference finishes (after which the waiting participant's call will be disconnected).

Administering Infinity Connect

Customizing and branding the Infinity Connect clients

The branding and styling of the Infinity Connect clients (web app and desktop) can be customized. This changes the look and feel of the Infinity Connect client regardless of which service is being accessed. (However, the theme-based elements of each individual service may also have been customized — a theme changes the look and feel of the actual conference you have joined, or are trying to join.)

Infinity Connect customization can be used to control:

- default settings such as bandwidth, screen sharing frame rate and so on
- the ability to display an image/logo and accompanying welcome text on a landing page, and to use a custom favicon
- language translations and the default language
- the color scheme for buttons, icons and other graphic indicators; elements can be customized individually or a general color scheme can be applied to all similar items.

To customize the web app you typically create and then upload a branding package to the Management Node. That branding package is then automatically applied to all users of the web app. To apply the same customized branding to the desktop clients you need to use Pexip Infinity's provisioning features to instruct those clients to override their built-in branding and use the customized branding instead.

Branding customizations that are applied to the web app via the Management Node will apply to all [web app revisions](#), and will persist over upgrades to subsequent versions of Pexip Infinity software (although you may need to adapt the customization to cater for any new features when upgrading to a new major release).

The instructions in this topic describe how to [create and upload](#), [edit](#) and [remove](#) a branding package, and how to [apply the branding to the desktop clients](#).

Note that the procedures described here apply a generic customization for all Infinity Connect users. If you have specific customization requirements, such as hosting multiple different branding customizations for web app users under different URLs on external web servers or reverse proxies, see [Advanced Infinity Connect customization](#).

Creating and uploading a branding package

You must create a branding package before you can upload it to the Management Node or use it to brand the desktop client. The recommended method to create a branding package for the Infinity Connect clients is to use the Pexip branding portal (<https://brandingportal.pexip.com>).

Creating a branding package via the Pexip branding portal

You can use the Pexip branding portal to customize the Infinity Connect web and desktop clients. This web-based tool guides you through the selection of your image files and colors without having to edit individual CSS files etc, and then generates the customized branding package for you.

To use the Pexip branding portal to generate your branding package for the Infinity Connect clients:

1. Go to the Pexip branding portal (<https://brandingportal.pexip.com>) and sign in.
First time users need to register before they can use the portal.
You can also use the portal to create customizations for the legacy web app if required.
2. Select which version of Pexip Infinity you have installed, so that the relevant branding and customization features can be offered.
3. From here you can choose to create new customizations, or edit an existing customization that you have previously created. Configure your customization as required, selecting the relevant image files, colors and settings:
 - The **App Editor** changes the look and feel of the Infinity Connect clients, including enabling an image/logo on the landing page.
 - The **Customizations** section controls the client's configuration settings, including default options, languages and plugins.
 - The **Splash Screens** section doesn't directly affect the Infinity Connect clients. It is used to customize the Pexip Infinity themes (which are used when you join a VMR or other service either via an Infinity Connect client or other endpoint) and generates a separate ZIP package when built.

- The **Languages** section allows you to set up additional languages for the Infinity Connect clients, or to create a modified version of the default English text strings. When creating a new set of language strings the **Name** is the name you will see within the portal, and the **Label** is the name users will see within the app; the **Locale** enables that language to be used automatically if it matches the browser's default language. If you set up new language option then you must use the **Customizations** section to select the new/modified languages you want to include in your branding package (and deselect the original **English** language strings if required).
4. When you have finished configuring your branding, go to the Dashboard, select the relevant **App Edits** and **Customizations** and then **Build** your customization package. If you have added new languages they are automatically included in your build depending upon which languages are selected in the **Customization**.
This creates and downloads a **branding.zip** file containing your client customizations.
 5. Upload the branding package to your Management Node:
 - a. Go to **Services > Web App Customization**.
 - b. In the **Upload Web App branding** section, select **Choose File** and select the ZIP file containing your customizations.
 - c. Select **Upload branding**.
The branding package will be uploaded. The upload process automatically detects which type of app branding is contained in the ZIP file and processes it accordingly.Wait for the new branding to be replicated out to all Conferencing Nodes (typically after approximately one minute).
- i** This branding package is used to customize the web app by default, but you can also automatically [apply the same branding to the desktop clients](#).

Manually configuring the branding files

Manual configuration is useful if you have plugins or very specific modifications that you want to apply to the branding files. Note that manual configuration requires knowledge of core web-design technologies such as HTML, JavaScript and CSS.

To manually configure the branding files:

1. Download the default web app branding files from the Management Node:
 - a. Go to **Services > Web App Customization**.
 - b. Select **Download** (next to the **Download default branding** label). This downloads a **branding_nextgen_and_legacy_default.zip** file to your local file system.Note that if you have existing branding files uploaded, you can choose to download those instead of the default files. You can also use files that were originally created by the Pexip branding portal — both methods use the same set of configuration files — you can use the branding portal to apply your basic customization requirements and then make further manual amendments to the configuration files if necessary.
2. Unpack the downloaded file and apply your modifications to the relevant files.
3. Repackage your branding files into a single ZIP file (<name>.zip).
 - i** The ZIP file does not have to contain the complete set of branding files. You can upload a subset of the branding files, but you must retain the original file/folder structure in the rebuilt ZIP file. For example, if you have no need to customize the legacy web app files you only need to zip up the **webapp2** folder.
 - i** You must include the **manifest.json** file in the **webapp2** folder.If you are customizing the legacy web app and want to change the **background.jpg** or **logo.png** graphics files, you must also include a **brand.css** file that at least includes the references (**brand-logo** and **brand-background** classes) to those customized images.
4. Upload the branding package to your Management Node:
 - a. Go to **Services > Web App Customization**.
 - b. In the **Upload Web App branding** section, select **Choose File** and select the ZIP file containing your customizations.
 - c. Select **Upload branding**.
The branding package will be uploaded. The upload process automatically detects which type of app branding is contained in the ZIP file and processes it accordingly.Wait for the new branding to be replicated out to all Conferencing Nodes (typically after approximately one minute).

You can now test the branding by dialing in to one of your Pexip Infinity services via the Infinity Connect web app.

Editing an existing branding package

You can modify an existing branding package by either returning to the Pexip branding portal, or manually editing the branding files that were uploaded previously to the Management Node.

Note that when you upload a new branding package to the Management Node all of the previous branding files for that app are deleted and replaced with the new set of files.

Using the branding portal

If you initially created your branding package via the Pexip branding portal, you can return to the portal and change those files:

1. Go to the Pexip branding portal (<https://brandingportal.pexip.com>) and sign in.
2. Make your changes, previewing them if necessary, and then download a new ZIP file.
3. On the Management Node, go to **Services > Web App Customization** and upload your new branding ZIP file.

Wait for the new branding to be replicated out to all Conferencing Nodes (typically after approximately one minute).

Manually changing your existing web app branding on the Management Node

You can manually edit the existing branding files that have been uploaded to the Management Node (even if those files were originally created via the Pexip branding portal):

1. On the Management Node, go to **Services > Web App Customization**.
2. Download the existing branding files:
 - Select the **Download** option next to the **Download default branding** label to download the system default branding files.
 - If customized branding has been uploaded, you can download it by selecting the **Download** option next to the **Download current branding** label.
(Or the **Download** option next to the **Download legacy branding** label for customized legacy clients.)

3. Unpack the downloaded file and apply your modifications to the relevant files.
4. Repackage your modified branding files into a new ZIP file.

If you are also modifying the legacy web app files, you can package the legacy and webapp2 files as two separate ZIP files i.e. one ZIP containing legacy branding and one ZIP containing webapp2 branding, thus matching the ZIP packages you downloaded. You can also combine them into one ZIP package, but it must match the file structure that is produced when downloading the default branding files.

5. Upload the new ZIP file back onto the Management Node (**Services > Web App Customization** then **Choose File** followed by **Upload branding**).

The upload process automatically detects which type of app branding is contained in the ZIP file and processes it accordingly.

Wait for the new branding to be replicated out to all Conferencing Nodes (typically after approximately one minute).

Removing a web app branding package (revert to default branding)

If you want to revert to the default branding for the web app, you need to remove your customized branding from the Management Node. To do this:

1. On the Management Node, go to **Services > Web App Customization**.
2. From the bottom-right corner of the page, select **Remove branding** to remove any branding (or **Remove legacy branding** if customized branding has been uploaded for the legacy clients).

Wait for the customized branding to be removed from all Conferencing Nodes and for the web app to revert to the default branding (typically after approximately one minute).

Applying branding to the desktop clients

Any branding package that is uploaded to the Management Node is only applied to the Infinity Connect web app.

To apply the same customized branding to the desktop clients you need to use Pexip Infinity's provisioning features to instruct those clients to override their built-in branding and use the customized branding instead. This is achieved by specifying the **brandingURL** provisioning parameter when you construct each individual desktop client user's provisioning URI.

- The **brandingURL** parameter must refer to a directory on an accessible server that contains the branding package.
- The branding package must be signed, and the client must upload a trusted (public) key before the branding can be applied.
- The branding package must be presented as a **branding.zip** file and an associated **branding.zip.sig** file.

For example, if **brandingURL** = **pexample.com/foo**, then you need to provide **pexample.com/foo/branding.zip** and **pexample.com/foo/branding.zip.sig**.

After an Infinity Connect client has been provisioned with a **brandingURL** provisioning parameter, every time it launches it checks the contents of the branding files at the brandingURL location to see if the branding has changed (it checks to see if the **brandingID** in the **manifest.json** file has changed). If the branding has been updated, the client fetches and caches the relevant files.

Note that the desktop client's favicon, taskbar/tray icons and app name cannot be updated via branding as these elements are fixed during the installation of the client software.

See [Registering and provisioning the Infinity Connect desktop client](#) for full instructions about how to set up provisioning URIs. Note that the client does not need to be registered in order to use the branding provisioning feature.

Note that as of version 1.8 you cannot apply branding to the mobile clients, and the desktop client branding can no longer be hosted on Conferencing Nodes.

Creating and signing a branding package for the desktop clients

The branding package in the **brandingURL** location must be presented as a **branding.zip** file plus an associated **branding.zip.sig** file that contains the package's signature.

Contents of branding.zip

Typically we recommend that you use a **branding.zip** file produced by the Pexip branding portal as this is a suitable zip file/format and contains all of the relevant content (although you must still sign it yourself).

The **manifest.json** is automatically generated by the Pexip branding portal and includes the **brandingID** timestamp and also indicates which parts of the app are customized.

If you want to create your own **branding.zip** file then it must contain a **webapp2** folder as its root folder and that must then have the following structure/contents:

- **manifest.json** (mandatory)
- **settings.json** (optional)
- **watermark_icon.png** (optional)
- **favicon** files (optional, applies only to the web app)
- **site.webmanifest** (optional)
- **themes** directory containing **styles.css** (both optional)

as shown below:

Name

-  themes
-  favicon.ico
-  manifest.json
-  settings.json
-  android-chrome-192x192.png
-  android-chrome-256x256.png
-  apple-touch-icon.png
-  favicon-16x16.png
-  favicon-32x32.png
-  mstile-150x150.png
-  watermark_icon.png
-  safari-pinned-tab.svg
-  site.webmanifest

Full details of the structure of the `manifest.json` file and the other application files are contained in [Advanced Infinity Connect customization](#).

Signing the branding package

You must use JSON Web Token (JWT) to sign the package. (JWT is an open standard that defines a way for securely transmitting information between parties as a JSON object.)

As part of the process to sign the branding package you need a public/private keypair. You may already have a keypair that you can use for this process, or you can use a third-party tool such as PuTTYgen to generate a keypair. The key must be in RSA format and at least 2048 bits. Alternatively you can log in to your Management Node over SSH and run the following commands to generate a private and public key pair:

```
openssl genrsa -out /dev/shm/privatekey.pem 2048
openssl rsa -in /dev/shm/privatekey.pem -pubout -out /tmp/publickey.pem
```

To sign the branding package and create your `.sig` file:

1. Create your **branding.zip** file.
2. Using a plain text editor, create a shell script file called `mkjwt.sh` containing the following code:

```
#!/bin/sh

set -e

if [ $# -ne 2 ]; then
    echo "Usage: $0 <privatekey.pem> <branding.zip>" >&2
    exit 1
fi

HEADER="eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9"
HASH=$(openssl dgst -sha256 $2 | sed -e 's/^[^ ]* //' )
PAYLOAD=$(echo -n "{\"sha256\": \"${HASH}\"}" | base64 -w0 | sed -e 's/\\+/-/g' -e 's/\\/_/g' -e 's/=//g')
SIG=$(echo -n "${HEADER}.${PAYLOAD}" | openssl dgst -sha256 -sign $1 | base64 -w0 | sed -e 's/\\+/-/g' -e 's/\\/_/g' -e 's/=//g')

echo "${HEADER}.${PAYLOAD}.${SIG}"
```

3. Copy your private key file (named `privatekey.pem`), the `branding.zip` file and the `mkjwt.sh` file into the `/dev/shm` directory on the Management Node using an SCP (Secure Copy) client, for example WinSCP.
4. Connect over ssh into the Management Node as user `admin` with the appropriate password.
5. Run the following commands:


```
cd /dev/shm
chmod 0755 mkjwt.sh
```
6. Run the following command to generate the `.sig` file:


```
./mkjwt.sh privatekey.pem branding.zip >branding.zip.sig
```
7. Run the following command to remove the private key file:


```
rm ./privatekey.pem
```
8. Use the SCP client to copy the generated `branding.zip.sig` file to your local machine.

Using the branding package on the desktop client

The client will not automatically use the customized branding package (as referred to at the provisioned `brandingURL` location).

Each client user must first import a trusted key via **Settings > Advanced settings > Import trusted key** and confirm that they want to apply the branding. The trusted key file they need to import (i.e. that you need to distribute) is the public key file used as part of the key pair used to create the JWT signature.

-  Only distribute the public key. Do not distribute the private key.

Obtaining diagnostic information from Infinity Connect

Users of Infinity Connect clients can obtain information about their client's incoming and outgoing audio and video streams, which may be helpful in diagnosing issues with call quality.

To obtain this information, from the top right of the side panel, select **Control** ●●● and then select **Get media stats**.

Creating preconfigured links to launch conferences via Infinity Connect

You can construct URLs or hyperlinks that may be used to automatically launch the Infinity Connect client and take the user directly into a specific conference. If required it can also pass in any necessary information such as the caller's name or the PIN needed to enter the meeting.

The URLs are in two formats: one that can be used to launch the [web app](#), and one for use with the [desktop and mobile clients](#). The parameters that can be included in the link are the same for both link types (with the exception of [address/domain](#) and [callType](#)).

Security considerations

While embedding information such as participant names and conference PINs into the URL can make it easier for participants to join conferences, note that these parameters are included in the URL in human-readable format. This means that if a user shares the URL — such as in a screen shot of their meeting invitation — and the URL includes the PIN, anyone with access to the URL can deduce the PIN and enter (and control, if it is a Host PIN) the meeting.

As of version 25 of Pexip Infinity, when a user follows a link to join a conference via the Infinity Connect web app, any join parameters, such as a conference PIN, are automatically removed from the URL that is displayed in the browser's address bar.

Links to the web app

To open an instance of the Infinity Connect web app in the user's default browser and take them to the home screen (not into a specific conference), use the following link:

`https://<address>/webapp/home`

where **<address>** is the IP address or domain name of the Conferencing Node (or reverse proxy if, for example, it is being used to host a customized version of the web app).

To provide users with a URL that, when clicked, takes them straight into a specific conference, construct a URL in the format:

```
https://<address>/webapp/#/?conference=<alias>&name=<name>&pin=<PIN>&role=<role>
&muteMicrophone=<muteMicrophone>&muteCamera=<muteCamera>&callType=<callType>
&extension=<extension>&bandwidth=<bandwidth>
```

where:

- **<address>** is the IP address or domain name of the Conferencing Node (or reverse proxy if, for example, it is being used to host a customized version of the web app).
- **<alias>** is one of the aliases for the conference or service the user will join.
- **<name>** is the name of the user who is joining the conference.
- **<PIN>** is either the Host PIN or Guest PIN, if required (note the [Security considerations](#) if these are included).
- **<role>** is **guest** if you want to allow Guests to automatically join a conference that allows Guests but has no Guest PIN. In all other cases, participants are asked to enter a PIN to join the conference (unless there is no Host PIN, or the URL already specifies a **<PIN>**); the PIN determines the participant's role and the **<role>** is ignored. Note that if **role=host**, participants are still prompted to enter the Host PIN to join the conference; this parameter cannot be used to bypass PIN entry requirements.
- **<muteMicrophone>** is **true** to join without sending audio (the user will still receive audio, and send and receive video).
- **<muteCamera>** is **true** to join without sending video (the user will still receive video, and send and receive audio).
- **<callType>** is one of:
 - **none** to join as a [presentation and control-only participant](#), i.e. the user will not send or receive any audio or video. They can still access the conference controls and send and receive presentations.
 - **audioonly** to join as an audio-only participant, i.e. the user will send and receive audio but will not send or receive video.
 - **video** (the default) to join as a full (send and receive) audio and video participant.
- **<extension>** is the Virtual Reception extension, or the Microsoft Skype for Business / Lync Conference ID.
- **<bandwidth>** is the maximum bandwidth for the call, and the bandwidth at which the initial call attempt will be made, in kbps. It can be any number between 256 and 6144.

The URL should always include the **alias** parameter; the remainder of the parameters are optional. If a parameter is not specified in the URL but is required when joining (i.e. **name**, and **PIN** if the conference uses PINs, or **extension** if one is requested), the participant will have to provide the information themselves before they can join the conference.

- i** This URL structure will not work on version 24 or earlier of Pexip Infinity, but any URLs using the previously recommended structure (`https://<address>/webapp/conference/<alias>?<parameters>`) will still work on v25 and later, and the join parameters (but not the alias) will be removed from the browser's address bar.

Examples

Assuming the domain name of your Conferencing Node is **vc.example.com**, and there is a Virtual Meeting Room with the alias **meet.alice**, which has no PIN:

- the basic URL for someone to join the VMR directly would be:
`https://vc.example.com/webapp/#/?conference=meet.alice`
- to set the display name for a participant e.g. "Bob", the URL would be:
`https://vc.example.com/webapp/#/?conference=meet.alice&name=Bob`
(Note that if you shared this same link with many participants, they would all join with their display name set to "Bob".)

If we then gave the same Virtual Meeting Room a Host PIN of **1234**, and allowed Guests to join without a PIN:

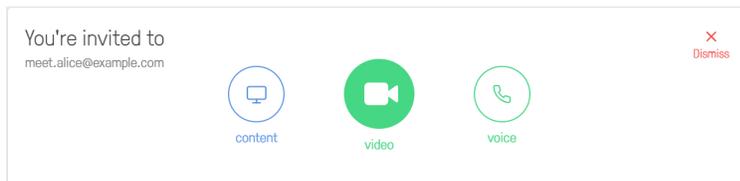
- the URL for Bob to join it directly as a **Host** would be:
`https://vc.example.com/webapp/#/?conference=meet.alice&name=Bob&pin=1234`
- the URL for Bob to join it directly as a **Guest** would be:
`https://vc.example.com/webapp/#/?conference=meet.alice&name=Bob&role=guest`
- the URL for Bob to join it directly as an **audio-only Guest** would be:
`https://vc.example.com/webapp/#/?conference=meet.alice&name=Bob&role=guest&callType=audioonly`

Alternative structure to join with an invitation card

You can use an alternative URL structure in the format:

`https://<address>/webapp/home?conference=<alias>`

In this case the web app will launch with an invitation to join the nominated `<alias>`, and it gives the user an opportunity to modify their settings (such as camera, mic and so on) before joining the conference, and they can select whether they want to join with **video**, **voice**, or **content** and control only.



This can be useful in scenarios where a user has previously set their camera to None, and are unable to modify their device settings if they have been taken directly into a conference.

Links to the desktop and mobile clients

You can create a URL that, when clicked, opens the Infinity Connect client on that device and provides an invitation to join the nominated conference. The same URL can be used for the desktop client and mobile clients for Android and iOS. This URL can be included in web pages, instant messages or emails (but note that some email clients such as Gmail will strip them out for security reasons).

- i** The Infinity Connect desktop or mobile client must already be installed on the device.

The URL is in the format:

`pexip://<alias>?host=<domain>&name=<name>&pin=<PIN>&role=<role>&muteMicrophone=<muteMicrophone>&muteCamera=<muteCamera>&extension=<extension>&bandwidth=<bandwidth>`

where:

- **<alias>** is one of the aliases for the conference or service the user is invited to join.
- **<domain>** is the IP address or domain name of the Conferencing Node (or reverse proxy if, for example, it is being used to host a customized version of the web app) the client should connect to in order to place the call. Note that this is ignored if the client is registered and [Route calls via registrar](#) is enabled.
- **<name>** is the name of the user who is joining the conference.
- **<PIN>** is either the Host PIN or Guest PIN, if required (note the [Security considerations](#) if these are included).
- **<role>** is **guest** if you want to allow Guests to join a conference without having to enter a PIN (providing the conference allows Guests and has no Guest PIN). In all other cases, participants are asked to enter a PIN to join the conference (unless there is no Host PIN, or the URL already specifies a **<PIN>**); the PIN determines the participant's role and the **<role>** is ignored. Note that if **role=host**, participants are still prompted to enter the Host PIN to join the conference; this parameter cannot be used to bypass PIN entry requirements.
- **<muteMicrophone>** is **true** to join without sending audio (the user will still receive audio, and send and receive video).
- **<muteCamera>** is **true** to join without sending video (the user will still receive video, and send and receive audio).
- **<extension>** is the Virtual Reception extension, or the Microsoft Skype for Business / Lync Conference ID.
- **<bandwidth>** is the maximum bandwidth for the call, and the bandwidth at which the initial call attempt will be made, in kbps. It can be any number between 256 and 6144.

The URL must always include `pexip://<alias>`; the remainder of the parameters are optional. If a parameter is not specified in the URL but is required when joining (i.e. **name**, and **PIN** if the conference uses PINs, or **extension** if one is requested), the participant will have to provide the information themselves before they can join the conference.

Example - email footer

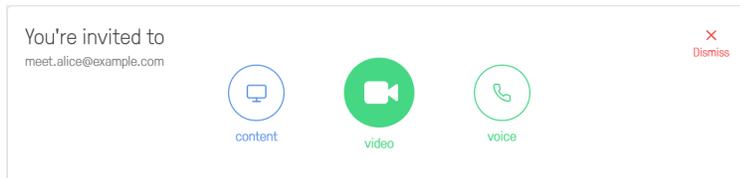
For example, Alice's personal meeting room has the alias `meet.alice@example.com` so she includes the following text in her email footer:

- Video: `meet.alice@example.com`

which displays as:

- Video: [meet.alice@example.com](#)

Now, when someone who has an Infinity Connect client installed on their device clicks on the link in Alice's email, their client will open automatically with an invitation to join `meet.alice@example.com`, and all they need to do is select whether they want to join with **video**, **voice**, or **content** and control only:



Example - Guest PIN

Alice's personal meeting room has a Guest PIN of `1234`. When Alice is chatting with a colleague using an instant messaging client and she wants to move the conversation to video, she sends them the message `pexip://meet.alice@example.com?pin=1234`, which automatically appears as a hyperlink. Her colleague clicks on the link and is invited to join Alice's personal meeting room as a Guest.

Example - always join with microphone muted

If you want the participant to join a meeting with a PIN of `1234`, and you want their microphone to be muted on joining, the URL would be: `pexip://meet.alice@example.com?pin=1234&muteMicrophone=true`

Links to the legacy Infinity Connect clients

For information on creating links to legacy clients, see the [v17 documentation](#).

Setting up DNS records and firewalls for Infinity Connect client connectivity

To ensure that Infinity Connect clients can successfully locate and connect to Pexip Infinity you must set up appropriate DNS records and ensure your firewalls are configured correctly.

DNS records

You must set up DNS records so that the Infinity Connect clients know which host to contact when placing calls or registering to Pexip Infinity.

The host will typically be a public-facing Conferencing Node (for on-premises deployments where your Transcoding Conferencing Nodes are located within a private network we recommend that you deploy public-facing Proxying Edge Nodes).

To enable access from the Infinity Connect desktop clients and Infinity Connect mobile clients, each domain used in aliases in your deployment must either have a DNS SRV record for `_pexapp._tcp.<domain>`, or resolve directly to the IP address of a public-facing Conferencing Node.

The SRV records for `_pexapp._tcp.<domain>` should always:

- point to an FQDN which **must** be valid for the TLS certificate on the target Conferencing Nodes
- reference port 443 on the host.

Note that SRV records are not required for the Infinity Connect web app — the web app clients connect to Conferencing Nodes directly via DNS A-records, so no SRV lookup is required.

Ultimately it is the responsibility of your network administrator to set up SRV records correctly so that the Infinity Connect desktop client and Infinity Connect mobile client know which system to connect to.

You can use the tool at <http://dns.pexip.com> to lookup and check SRV records for a domain.

Firewall configuration

Infinity Connect clients connect to a Conferencing Node, so you must ensure that any firewalls between the two permit the following connections:

- Infinity Connect mobile client > Conferencing Node port 443 TCP
- Infinity Connect (all clients) > Conferencing Node ports 40000–49999 TCP/UDP
- Conferencing Node ports 40000–49999 TCP/UDP > Infinity Connect (all clients)

For more information, see https://docs.pexip.com/admin/port_usage.htm.

Using Infinity Connect from outside your network

In many cases, your Pexip Infinity deployment will be located inside a private network. If this is the case and you want to allow Infinity Connect users who are located outside your network (for example on another organization's network, from their home network, or the public internet) to connect to your deployment, you need to provide a way for those users to access those private nodes.

Since version 16 of Pexip Infinity, we recommend that you deploy Proxying Edge Nodes instead of a reverse proxy and TURN server if you want to allow externally-located clients to communicate with internally-located Conferencing Nodes. A Proxying Edge Node handles all media and signaling connections with an endpoint or external device, but does not host any conferences — instead it forwards the media on to a Transcoding Conferencing Node for processing.

Further information and connectivity examples

Information on how each of the Infinity Connect clients attempts to locate a Conferencing Node when placing a call is described in the following sections. Within each section is an example of the lookup process for that client. The example uses the following records:

Assume that the following `_pexapp._tcp.vc.example.com` DNS SRV records have been created:

```
_pexapp._tcp.vc.example.com. 86400 IN SRV 10 100 443 px01.vc.example.com.  
_pexapp._tcp.vc.example.com. 86400 IN SRV 20 100 443 px02.vc.example.com.
```

These point to the DNS A-records `px01.vc.example.com`, port 443 (HTTPS), with a priority of 10 and a weight of 100, and `px02.vc.example.com`, port 443, with a relatively lower priority of 20 and a weight of 100.

This tells the Infinity Connect desktop and mobile clients to initially send their HTTP requests to host **px01.vc.example.com** (our primary node) on TCP port 443. The clients will also try to use host **px02.vc.example.com** (our fallback node) if they cannot contact px01.

Infinity Connect desktop client

Registering

The Infinity Connect desktop client uses its configured **Registration Host** and performs a DNS SRV lookup on **_pexapp._tcp.<registration host address>** to locate a Conferencing Node to which it can send its registration request.

In all cases, when performing an SRV lookup on **_pexapp._tcp.<registration host address>**:

- If multiple records are returned, the client attempts to contact each host in turn according to the priority and weight of each returned record.
- If the SRV lookup fails (because either the SRV lookup does not return any records, or the client cannot contact any of the hosts (i.e. Conferencing Nodes) on the list that is returned in the SRV lookup), the client performs a DNS A-record lookup for **<registration host address>**. If that A-record lookup is successful, it attempts to connect to port 443 on the IP address returned from the lookup.

Making calls

The way in which Infinity Connect desktop clients decide which Conferencing Node to use when attempting to place a call depends on whether the client is registered, and on the global [Route calls via registrar](#) setting at the time of registration.

When placing a call, the Infinity Connect desktop client attempts to locate a Conferencing Node by doing **one** of the following, in order of precedence:

- If the client is registered to Pexip Infinity and the global [Route via registrar](#) setting is enabled, the client will route all calls directly to the IP address of the Conferencing Node to which it is registered, regardless of the domain being dialed. From there, the call is treated as an incoming call and processed according to the service precedence call routing logic.
- If the client is not registered or [Route calls via registrar](#) is disabled, and the call was placed [via a URL](#) that specifies a host domain, then the client performs an SRV lookup on **_pexapp._tcp.<host domain>**.
- If a **serverAddress** is specified in the client's application settings file (**settings.json**), the client performs an SRV lookup on **_pexapp._tcp.<serverAddress>**. Note that the **serverAddress** is not configured in the default desktop client provided by Pexip, but an address could have been configured during customization and provisioned to the client.
- If a **serverAddress** was not specified, the client performs an SRV lookup on the domain portion of the address that was dialed, i.e. **_pexapp._tcp.<address domain>**.

In all the above cases, when performing an SRV lookup:

- If multiple records are returned, the client attempts to contact each host in turn according to the priority and weight of each returned record.
- If the SRV lookup fails (because either the SRV lookup does not return any records, or the client cannot contact any of the hosts (i.e. Conferencing Nodes) on the list that is returned in the SRV lookup), the client performs a DNS A-record lookup for the domain in the SRV lookup. If that A-record lookup is successful, it attempts to connect to port 443 on the IP address returned from the lookup.
- If the client successfully contacts a host but that Conferencing Node is in maintenance mode, the client will not make any further attempts to contact any other hosts.
- When the client successfully contacts a host, the host will then check to see if the alias that has been dialed exists in its configuration. This means that the alias does not need to include a domain if, for example, the host has been found via a lookup on the **serverAddress**. It also means that the domain in the alias being dialed does not necessarily need to be the same as the domain of the host.

Example

In this example, when a user attempts to place a call to `meet.alice@vc.example.com`, the client does **one** of the following:

- If the client is registered to Pexip Infinity and the global [Route via registrar](#) setting is enabled, the client will route all calls directly to the IP address of the Conferencing Node to which it is registered, regardless of the domain being dialed.

For example, if the client is configured with a Registration Host of `registration.example.com`, then the client will perform an SRV lookup on `_pexapp._tcp.registration.example.com`.

If the SRV lookup fails, or none of the returned hosts in the lookup can be contacted, the client will also attempt to connect directly to that domain, i.e. to `http://registration.example.com:443` (via DNS A-records for `registration.example.com`).

- If the call is being placed via a [preconfigured link](#) that specifies a host domain, then the client will perform an SRV lookup on that domain, and attempt to contact one of the hosts returned in that lookup.

For example, if the URL is `pexip://meet.alice@vc.example.com?host=localserver.example.com` then the client will perform an SRV lookup on `_pexapp._tcp.localserver.example.com`.

If the SRV lookup fails, or none of the returned hosts in the lookup can be contacted, the client will also attempt to connect directly to that domain, i.e. to `http://localserver.example.com:443` (via DNS A-records for `localserver.example.com`).

If that also fails, no further lookups are performed, and the client will report that it could not join the host domain.

- If a `serverAddress` has been configured, the client performs an SRV lookup on that domain, and attempts to contact the host(s) returned in that lookup.

For example, if the `serverAddress` is `localserver.example.com` then the client performs an SRV lookup on `_pexapp._tcp.localserver.example.com`.

If the SRV lookup fails, or none of the returned hosts in the lookup can be contacted, the client also attempts to connect directly to that domain, i.e. to `http://localserver.example.com:443` (via DNS A-records for `localserver.example.com`).

If that also fails, no further lookups are performed, and the client will report that it could not join the host domain.

- In all other cases, the client attempts an SRV lookup on the domain portion of the address that was dialed, i.e. on `_pexapp._tcp.vc.example.com`.

If the SRV lookup succeeds, it returns the records shown above, and the client will attempt to contact `px01.vc.example.com` (the record with the highest priority) on TCP port 443.

If it cannot contact `px01.vc.example.com` it next tries to contact `px02.vc.example.com`.

If it fails to contact either host, the client also attempts to connect directly to the domain, i.e. to `http://vc.example.com:443` (via DNS A-records for `vc.example.com`).

If that also fails, the client will report that it has failed to contact a server.

Infinity Connect mobile client

Making calls

When placing a call, the Infinity Connect mobile client attempts to locate a Conferencing Node as follows:

- If the call was placed [via a URL](#) that specifies a host domain, then the client performs an SRV lookup on `_pexapp._tcp.<host domain>`.
- Otherwise, the client performs an SRV lookup on the domain portion of the address that was dialed, i.e. `_pexapp._tcp.<address domain>`.

In all the above cases, when performing an SRV lookup:

- If multiple records are returned, the client attempts to contact each host in turn according to the priority and weight of each returned record.
- If the SRV lookup fails (because either the SRV lookup does not return any records, or the client cannot contact any of the hosts (i.e. Conferencing Nodes) on the list that is returned in the SRV lookup), the client performs a DNS A-record lookup for the domain in the SRV lookup. If that A-record lookup is successful, it attempts to connect to port 443 on the IP address returned from the lookup.
- If the client successfully contacts a host but that Conferencing Node is in maintenance mode, the client will not make any further attempts to contact any other hosts.

- When the client successfully contacts a host, the host will then check to see if the alias that has been dialed exists in its configuration. This means that the domain in the alias being dialed does not necessarily need to be the same as the domain of the host.

Example

In this example, when a user attempts to place a call to `meet.alice@vc.example.com`, the client does **one** of the following:

- If the call is being placed via a [preconfigured link](#) that specifies a host domain, then the client will perform an SRV lookup on that domain, and attempt to contact one of the hosts returned in that lookup.

For example, if the URL is `pexip://meet.alice@vc.example.com?host=localserver.example.com` then the client will perform an SRV lookup on `_pexapp._tcp.localserver.example.com`.

If the SRV lookup fails, or none of the returned hosts in the lookup can be contacted, the client will also attempt to connect directly to that domain, i.e. to `http://localserver.example.com:443` (via DNS A-records for `localserver.example.com`).

If that also fails, no further lookups are performed, and the client will report that it could not join the host domain.

- In all other cases, the client attempts an SRV lookup on the domain portion of the address that was dialed, i.e. on `_pexapp._tcp.vc.example.com`.

If the SRV lookup succeeds, it returns the records shown above, and the client will attempt to contact `px01.vc.example.com` (the record with the highest priority) on TCP port 443.

If it cannot contact `px01.vc.example.com` it next tries to contact `px02.vc.example.com`.

If it fails to contact either host, the client also attempts to connect directly to the domain, i.e. to `http://vc.example.com:443` (via DNS A-records for `vc.example.com`).

If that also fails, the client will report that it has failed to contact a server.

Switching to the legacy Infinity Connect web app

You can configure Pexip Infinity to default to the legacy version of the Infinity Connect web app.

Switching between current and legacy web app

To switch to using the legacy web app by default for all browsers:

1. Go to **Platform > Global Settings**.
2. In the **Connectivity** section, disable the **Do not default to the legacy Web App** check box.

When this option is disabled, WebRTC-compatible browser users:

- will use the legacy version of the web app.
- who append `/webapp` to the end of the Conferencing Node's address will use the legacy version of the web app.
- who want to use current web app, can do so by appending `/webapp2` to the end of the Conferencing Node's address.

Otherwise (when this option is enabled), WebRTC-compatible browser users who:

- enter just the IP address or FQDN of a Conferencing Node will use the current web app.
- append `/webapp` to the end of the Conferencing Node's address will use the current web app.
- want to use the legacy version of the web app, can do so by appending `/webapp1` to the end of the Conferencing Node's address.

In all cases, RTMP browser users will continue to use the legacy version of the web app.

Comparison of current and legacy Infinity Connect clients

The following table shows the main administrator and user-facing changes in the most recent versions of the Infinity Connect clients when compared to the legacy clients.

| Feature | Change | More information |
|---|---|---|
| Administrator-facing changes | | |
| Consistent branding across Infinity Connect clients | <p>Branding customizations that have been applied to the Infinity Connect web app can also be applied to the Infinity Connect desktop client.</p> <p>The administrator can use Pexip Infinity's provisioning features to instruct the desktop client to use the same branding as the web app.</p> | Customizing and branding the Infinity Connect clients |
| Call routing from registered desktop clients | There is an option to control whether registered desktop clients route their calls via the Conferencing Node to which they are registered, or via DNS. | |
| DNS SRV domain selection | When attempting to locate a Conferencing Node via DNS, the domains used, and the order in which they are selected, has changed. | Setting up DNS records and firewalls for Infinity Connect client connectivity |
| Pre-configured URLs to launch conferences automatically | <p>The format and parameters of pre-configured URLs for the web app, desktop and mobile clients has changed:</p> <ul style="list-style-type: none"> The format for web app links has changed from <code>https://<address>/?conference=<alias>&etc...</code> to <code>https://<address>/webapp/conference/<alias>?etc...</code> <p>However, any existing legacy-style links may still be used and they will be redirected to the new style.</p> <ul style="list-style-type: none"> Parameters that are no longer supported are <code>escalate</code>, <code>join</code>, <code>forceguest</code>, <code>media</code>, and <code>audioonly</code>. They have been replaced with <code>muteMicrophone</code>, <code>muteCamera</code> and <code>callType</code>. As an alternative to <code>join</code>, you can set <code>role</code> to <code>guest</code> if you want to allow Guests to automatically join a conference that has no Guest PIN. Links to the desktop and mobile clients now support additional parameters. <p>If required, web app users can still use the legacy-style web app links and associated parameters by inserting <code>/webapp1</code> after the Conferencing Node address, followed by the legacy parameters.</p> | Creating preconfigured links to launch conferences via Infinity Connect |
| Plugins | The new clients support the use of plugins. | |
| User-facing changes | | |
| Layout of home screen and join workflow | <ul style="list-style-type: none"> The look and feel of the home screen, and the way in which users select devices and enter the address of the person or conference they wish to call, has changed. Users can no longer specify a default domain (which was used when no domain was specified in the address being called). If a presentation and control-only Host joins a conference they must manually start the conference before Guests can join. | |

| Feature | Change | More information |
|------------------------------|---|-------------------------------|
| In-conference controls | <ul style="list-style-type: none"> The side panel to the left of the main video window now contains two tabs: Participant list and Events. All controls have been merged into either the toolbar or the main meeting control menu. All clients let you change the camera, microphone or speakers during a call. Conference events, including any chat messages sent or received, are listed in a separate Events tab on the side panel. A Guest participant now has a keypad available on their toolbar that can be used to enter the Host PIN and thus become a Host. You cannot add a dual streaming participant. Previously, desktop client users could, during a call, change the frame rate being used to send their presentation (although the presentation would still have to be started and stopped for the change to take effect). Now any changes to the frame rate must be made before making the call. | |
| Mobile client behavior | <ul style="list-style-type: none"> The previous iOS client automatically selected an appropriate bandwidth based on whether the connection was WiFi or cellular. Now, all bandwidth selection is manual and done by the end user prior to placing the call. Infinity Connect mobile clients for Android do not support registrations. | |
| Accessibility | A high-contrast option to support WCAG compliance is available. | High contrast |
| Using NFC to join conference | Use of NFC to automatically dial an endpoint into a VMR is not supported. | |
| Automatic language selection | If an administrator has enabled support for a given language and an Infinity Connect user's browser or device uses that language as a default, the client automatically uses that language. | |

Troubleshooting Infinity Connect error messages

The table below lists the specific messages that may be presented to Infinity Connect users, along with their meaning and suggested resolution (where appropriate). To assist administrators with troubleshooting, the associated admin-facing message (which appears in the admin log, and when viewing historical information about a participant) is also given.

For help with general issues that may occur when using Infinity Connect clients within your deployment, see [Troubleshooting the Pexip Infinity platform](#).

| Admin-facing message | User-facing message | Message code | Meaning/resolution |
|---|--|--------------|--|
| Call Failed: Invalid role | The PIN you entered is invalid - please try again. | #pex100 | |
| Call Failed: Invalid PIN | The PIN you entered is invalid - please try again. | #pex101 | The PIN that was entered did not match the Host (or Guest, if configured) PIN. |
| Call failed: Out of proxying resource | Error connecting to the meeting | #pex109 | All Proxying Edge Nodes in the location are out of capacity. |
| Call Failed: System in maintenance mode | The system you are trying to reach is temporarily unavailable. Please try again shortly. | #pex110 | The Conferencing Node is in maintenance mode. Note that if the client encounters a node in maintenance mode while performing an , it will not attempt to contact any other nodes. |

| Admin-facing message | User-facing message | Message code | Meaning/resolution |
|---|--|--------------|--|
| Call Failed: 502 Bad Gateway | There is no connection. Please try again. | #pex111 | |
| Call Failed: 503 Service Unavailable | There is no connection available. | #pex112 | |
| Call Failed: Invalid token | Your connection was lost. Please try again. | #pex113 | |
| Call Failed: Out of resource | The system you are trying to reach is over capacity. | #pex114 | |
| transfer failed | Transfer failed. | #pex115 | A Host participant attempted to transfer another participant from the current meeting to another meeting, but failed. |
| Call Failed: Unexpected Response: 503 | Call failed - please contact your administrator | #pex116 | Pexip Infinity received an Unexpected Response (503) when trying to place the call. If this issue persists, you may wish to send a snapshot to your Pexip authorized support representative. |
| Call failed: <code> | The call failed. Please try again. | #pex117 | Generic failure code. |
| Could not join localhost:8080 | The server cannot be reached. | #pex118 | The host server (obtained either as the result of the DNS lookup, or by using the domain part of the dialed alias) could not be found. |
| Call Failed: Failed to forward request | Call failed: Failed to forward request | #pex119 | |
| Conference host ended the conference with a DTMF command | A Host ended the meeting. | #pex120 | A Host participant ended the call using a DTMF command. |
| Conference terminated by a Host participant | A Host ended the meeting. | #pex121 | An Infinity Connect Host participant has selected "disconnect all", or a client API command was used to terminate the conference. |
| Conference terminated by an administrator | An administrator ended the meeting. | #pex122 | An administrator using the Pexip Infinity Administrator interface has selected "disconnect all", or a management API command was used to end the conference. |
| Disconnected by an administrator | An administrator disconnected you from the meeting. | #pex123 | An administrator using the Pexip Infinity Administrator interface has disconnected this particular participant. |
| Disconnected by another participant | Another participant in the meeting disconnected you. | #pex124 | A Host using an Infinity Connect client has disconnected a specific participant. |
| Conference terminated by another participant | A Host ended the meeting. | #pex125 | An Infinity Connect Host participant has selected "disconnect all", or a client API command was used to terminate the conference. |
| Timeout waiting for conference host to join or permit access to locked conference | The meeting Host has not joined or unlocked the meeting. | #pex126 | The participant timed out because the conference Host either did not join the conference, or did not permit the participant to join a locked conference. |
| | This feature has been disabled. | #pex127 | The setting to Enable support for Pexip Infinity Connect and Mobile App has been disabled by an administrator. |

| Admin-facing message | User-facing message | Message code | Meaning/resolution |
|---|---|--------------|--|
| Call failed: failed to establish media to server. Ensure required firewall ports are permitted. | Call failed: a firewall may be blocking access. | #pex128 | An ICE failure has occurred. |
| Signaling node disconnected | Something went wrong with the meeting. Please try to connect again. | #pex129 | The media node lost connectivity to the signaling node. |
| Media process disconnected | Something went wrong with the meeting. Please try to connect again. | #pex130 | The Conferencing Node hosting the media has encountered an unexpected behavior. |
| Media node disconnected | Something went wrong with the meeting. Please try to connect again. | #pex131 | The signaling node lost connectivity to the media node. |
| Proxied participant disconnected | Something went wrong with the meeting. Please try to connect again. | #pex132 | The proxying node lost connectivity to the transcoding node. |
| No participants can keep conference alive | The meeting has ended. | #pex140 | This was the only remaining participant, and they were an ADP that was not configured to keep the conference alive. |
| All conference hosts departed hosted conference | The meeting ended because the Host(s) left. | #pex141 | There are no Host participants remaining in the conference. |
| Last remaining participant removed from conference after timeout | You were the only participant left in the meeting. | #pex142 | This was the only participant remaining, and they were disconnected after the configured amount of time. |
| Test call finished | The test call has finished. | #pex143 | This was a call to the Test Call Service that was automatically disconnected after the specified time. |
| Call rejected | The person you are trying to call did not answer or could not be reached. | #pex150 | The person being called did not answer or could not be reached. |
| Call disconnected | The other participant has disconnected. | #pex151 | An Infinity Connect client has been disconnected by themselves or another system other than Pexip Infinity. |
| Gateway dial out failed | The call could not be placed. | #pex152 | The alias matched a Call Routing Rule but the call could not be placed. |
| invalid gateway routing rule transform | The call could not be placed. Please contact your administrator. | #pex153 | The alias matched a Call Routing Rule but the resulting alias was not valid. |
| Call Failed: Neither conference nor gateway found | "Cannot connect to <alias>. Check this address and try again. | #pex154 | The alias that was dialed did not match any aliases or Call Routing Rules. |
| Could not join <domain part of dialed alias> | Could not join <domain> | #pex155 | The domain is not part of a Pexip Infinity deployment. This error can occur if an incorrect serverAddress has been specified during customization. It can also occur if a SSL error is preventing a secure connection to the server. |

| Admin-facing message | User-facing message | Message code | Meaning/resolution |
|--|--|--------------|---|
| Participant failed to join conference Reason="No direct route between Edge and Transcoding" | The call could not be placed. | #pex156 | There is an issue with media location policy. This typically occurs if restricted routing for Proxying Edge Nodes is enabled and the proxying node cannot forward the media to the nominated transcoding node. |
| Not Found: The requested URL <address> was not found on this server | Could not join <domain> | #pex157 | Check that the URL is structured correctly. |
| Failed to gather IP addresses. | Call failed: Please disable any privacy extensions on your browser. | #pex170 | The browser cannot find the local IP address. This may be due to ad blockers. An Infinity Connect WebRTC client could not determine its IP address. This may because there are privacy extensions installed. |
| Call Failed: Error: Could not get access to camera/microphone. Have you allowed access? Has any other application locked the camera? | Your camera and/or microphone are not available. Please make sure they are not being actively used by another app. | #pex171 | An Infinity Connect WebRTC participant has not allowed their camera or microphone to be shared, or has no camera or microphone available. |
| Presentation ended | The presentation ended. | #pex180 | |
| Presentation stream remotely disconnected | The presentation stream was disconnected. | #pex181 | |
| Presentation stream unavailable | The presentation stream is unavailable. | #pex182 | |
| Screenshare canceled | The screenshare was canceled. | #pex183 | |
| Screenshare error | Something went wrong with screenshare. Please try again. | #pex184 | |
| Screenshare remotely disconnected | The screenshare was disconnected. | #pex185 | |
| Timer expired awaiting token refresh | Error connecting to the meeting | #pex190 | An Infinity Connect WebRTC client was unable to refresh its token after 2 minutes. This is likely due to network issues. |
| Resource unavailable | Error connecting to the meeting | #pex191 | There was insufficient transcoding or proxying capacity on the Transcoding Conferencing Node or the Proxying Edge Node on which the call landed. |
| Participant exceeded PIN entry retries | Too many PIN entry attempts | #pex192 | The participant exceeded the allowed number of PIN entry attempts (3). |
| Invalid license | Error connecting to the meeting. Please contact your administrator | #pex193 | There is an invalid license, for example a license may have expired. |
| Participant failed to join conference... Reason="Participant limit reached" | This meeting has reached the maximum number of participants. | #pex194 | A user has attempted to join a conference that has exceeded its configured number of participants. |

| Admin-facing message | User-facing message | Message code | Meaning/resolution |
|--------------------------------------|---|--------------|--|
| | Error connecting to the meeting. Please contact your administrator. | #pex195 | All the existing licenses are currently in use. |
| | Error connecting to the meeting. Please reconnect. | #pex196 | The Infinity Connect client's ICE connection failed or was interrupted. Users should attempt to reconnect. |
| ERROR_SSO_AUTHENTICATION | SSO Authentication Failed | #pex200 | Check your username and password and try again. |
| ERROR_SSO_NO_IDENTITY_PROVIDERS | SSO enabled but no Identity Providers configured | #pex201 | SSO setup may not be complete. Contact your administrator. |
| ERROR_SSO_POPUP_FAILED | Unable to open window for SSO authentication. This may have been prevented by a pop-up blocker. | #pex202 | Disable your pop-up-blocker for this website if you can. |
| ERROR_SSO_AUTHENTICATION_MAINTENANCE | SSO Authentication Failed. The system is in Maintenance mode. | #pex203 | Try again later. |
| Failed SAML SSO Request | SSO authentication failed. SSO is not available from this domain. | #pex204 | The domain in the URL (for web app clients) or the domain in the registration address (for desktop clients) is not on the list of allowed Assertion Consumer Service URLs. |

Infinity Connect release notes

For information about the new features and fixed issues the Infinity Connect clients see:

- [Infinity Connect web app release notes](#)
- [Infinity Connect desktop client release notes](#)
- [Infinity Connect mobile client release notes](#)

For release notes for the Pexip Infinity platform, see [Pexip Infinity release notes](#).

Infinity Connect web app release notes

This topic describes the new features and fixed issues in the current and previous supported releases of the Infinity Connect web app:

- [What's new?](#)
- [Fixed issues](#)
- [Known limitations](#)
- [What's new in previous versions](#)
- [Fixed issues in previous versions](#)

What's new?

New in v29 web app

Following are the new features and changes in the Infinity Connect web app in Pexip Infinity version 29:

| Feature | Description | More information |
|---|--|------------------|
| Presentation content defaults to full motion HD | Incoming presentation content is now viewed in full motion HD video by default. The user can switch to the previous default behavior of a series of still images / JPG format if required. | |

Fixed issues

Fixed in v29 web app

There were no significant user-facing fixes in this release.

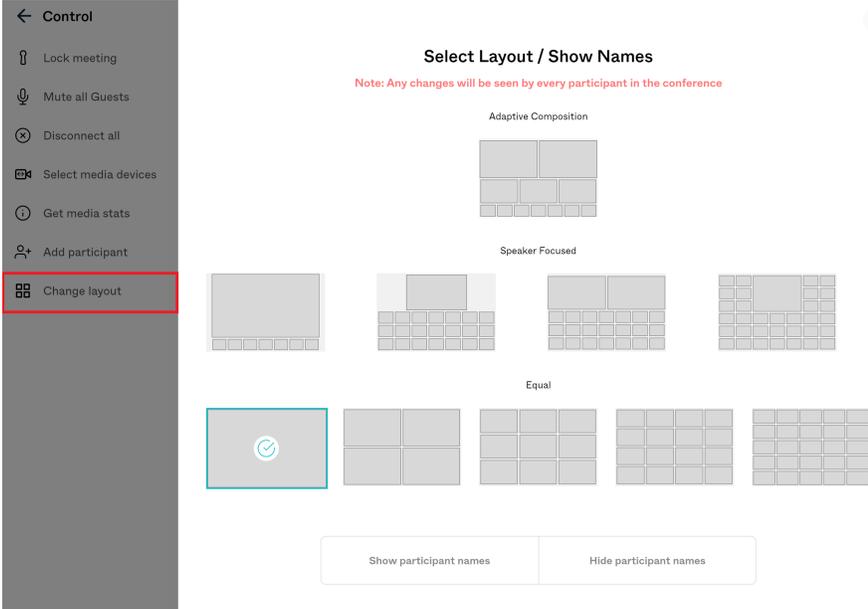
Known limitations

| Ref # | Limitation |
|-------|--|
| 19889 | When using the Infinity Connect web app in a browser on a mobile device in landscape mode, in some cases the video and presentation is cropped. To work around this, we recommend using the Infinity Connect mobile clients on mobile devices. |
| 18119 | Long display names are truncated when there is space available to show the full name. |

What's new in previous versions

New in v28 web app

Following are the new features and changes in the Infinity Connect web app in Pexip Infinity version 28:

| Feature | Description | More information |
|---|---|------------------|
| Change layout during a conference and show/hide participant names | <p>Host participants can use a new Change layout option in the side panel's Control menu. This lets you dynamically change the layout used during a conference to any of the support layout options, and to toggle the display of participant names.</p>  | |
| Chat messages indicator | <p>A visual indicator is displayed when a new chat message is received. It is displayed against the Events tab if the side panel is open and showing the participant list, or above the button used to show the side panel if the side panel is closed.</p>  | |
| Push spacebar to talk | <p>When a participant has muted themselves, they can press and hold down their keyboard spacebar to talk. It does not allow the participant to talk if they have been administratively muted.</p> | |
| Customize the participant list sort order | <p>The participant list can be customized to be sorted alphabetically via a new sortAttendeesAlphabetically application setting (instead of the order that the participants joined).</p> | |

New in v27 web app

Following are the new features and changes in the Infinity Connect web app in Pexip Infinity version 27:

| Feature | Description | More information |
|---|--|------------------|
| New features | | |
| Background blur | Individual participants that are using either a Chrome or Edge browser can now blur their own local background on the image they send to a conference. | |
| Allowing Far End Camera Control (FECC) on your own camera | Individual participants can enable their own local camera for Far End Camera Control (FECC) i.e. they can allow their own camera to be controlled (pan/tilt/zoom) by a remote participant (typically another Infinity Connect user). | |

| Feature | Description | More information |
|--|--|------------------|
| Controlling a remote camera via the keyboard | When controlling a remote camera, as well as using a mouse on the Camera Control overlay, you can now also use your keyboard arrow and + or - keys, to pan, tilt and zoom the camera at the far end. | |
| Receiving a presentation stream as part of the layout mix | When receiving presentation content in an Adaptive Composition layout, the presentation stream is now shown as part of the layout mix (replacing some of the other video participants), providing the client is receiving video at a medium or higher bandwidth setting (otherwise it is displayed as one large separate stream). You can toggle the presentation content between the "in mix" and "separate" streams via the new  maximize and  reset buttons in the bottom-right corner of the presentation. | |
| Support for participant authentication | Support has been added for Pexip Infinity's new participant authentication feature, whereby participants attempting to access an individual Virtual Meeting Room (VMR) or Virtual Auditorium can be required to verify their identity using Single Sign On (SSO) before joining the meeting. | |
| Changes in functionality | | |
| Additional browser support on iOS | The web app on iOS devices is now supported on Chrome, Firefox and Edge browsers, in addition to Safari. | |
| Changes to toolbar icons | Some of the icons used in the toolbar have changed: <ul style="list-style-type: none"> The icons to float and reset the video window have changed from  and  to  and  respectively. The icons to view a presentation in a separate window and close the separate window have changed from  and  to  and  respectively. | |
| The wizardOnFirstRun customization option is no longer supported | The <code>wizardOnFirstRun</code> customization option in the <code>settings.json</code> branding file is no longer supported. | |

New in v26 web app

Following were the new features and changes in the Infinity Connect web app in Pexip Infinity version 26:

| Feature | Description | More information | | | | | | |
|--|--|------------------|---|-----|---|----------|---|--|
| New audio-only and inactive-video indicators in the participant list | Each person in the Participant list now has an additional icon displayed if that participant is connected as audio-only, is a video-muted Infinity Connect participant, or is inactive, for example, if they are away from the computer (and thus their face cannot be detected in their video stream): <table border="0"> <tr> <td>Alice</td> <td> </td> </tr> <tr> <td>Bob</td> <td> </td> </tr> <tr> <td>Randolph</td> <td></td> </tr> </table> where the indicators represent:  Muted video or inactive (away)  Connected via audio only | Alice |   | Bob |   | Randolph |  | |
| Alice |   | | | | | | | |
| Bob |   | | | | | | | |
| Randolph |  | | | | | | | |

| Feature | Description | More information |
|--|--|------------------|
| More bandwidth options in the app settings | <p>There are more bandwidth selection options available in Settings > Bandwidth. You can now choose from <i>Very Low (up to 256kbps)</i>, <i>Low (up to 576kbps)</i>, <i>Medium (up to 1264kbps)</i>, <i>High (up to 2464kbps)</i>, or <i>Very High (up to 6144kbps)</i>.</p> <p>The default is <i>Medium (up to 1264kbps)</i>.</p> | |
| Enable "raise hand" in VMRs | <p>By default the "raise hand" feature is only available in Virtual Auditoriums. There is a new <code>raiseHandInVMR</code> customization option in the <code>settings.json</code> file in a web app branding package that can be used to also enable the feature in Virtual Meeting Rooms.</p> | |

Fixed issues in previous versions

Fixed in v28 web app

| Ref # | Resolution |
|-------|---|
| 22967 | All references to Adobe Flash have now been removed from the Infinity Connect codebase. |

Fixed in v27 web app

| Ref # | Resolution |
|-------|---|
| 26382 | Browser requests for access to camera and mic will no longer time out, improving usability for first-time users. |
| 25929 | When the web app is used on Safari on iOS 15.1 devices, we will force the use of VP8. This is a workaround to an iOS issue which Apple have resolved in iOS 15.2. |

Fixed in v26 web app

| Ref # | Resolution |
|-------|--|
| 24106 | The app now correctly supports different language cultures via branding. For example, it can distinguish between French (fr-FR), French Canadian (fr-CA) and French Belgian (fr-BE). |

Infinity Connect desktop client release notes

This topic describes the new features, fixed issues and known limitations in the current and previous supported releases of the Infinity Connect desktop client:

- [What's new?](#)
- [Fixed issues](#)
- [Known limitations](#)
- [What's new in previous releases](#)
- [Fixed issues in previous releases](#)

What's new?

New in v1.9.1 desktop client

Version 1.9.1 of the Infinity Connect desktop client was released in May 2022. This was the latest version at the time of publishing; to check for updates, see [What's new in Infinity Connect?](#) Below are the new features and changes in v1.9.1:

| Feature | Description | More information |
|---------------------------------|---|------------------|
| Changes in functionality | | |
| Installation file format | The desktop client for Windows is now installed using a .MSI file (rather than the previous .EXE) | |

New in v1.9 desktop client

Version 1.9 of the Infinity Connect desktop client was released in February 2022. This was the latest version at the time of publishing; to check for updates, see [What's new in Infinity Connect?](#) Below are the new features and changes in v1.9:

| Feature | Description | More information |
|---|---|------------------|
| New features | | |
| Background blur | (Desktop client for Windows only) Individual participants can now blur their own local background on the image they send to a conference. | |
| Allowing Far End Camera Control (FECC) on your own camera | Individual participants can enable their own local camera for Far End Camera Control (FECC) i.e. they can allow their own camera to be controlled (pan/tilt/zoom) by a remote participant (typically another Infinity Connect user). | |
| Receiving a presentation stream as part of the layout mix | When receiving presentation content in an Adaptive Composition layout, the presentation stream is now shown as part of the layout mix (replacing some of the other video participants), providing the client is receiving video at a medium or higher bandwidth setting (otherwise it is displayed as one large separate stream). You can toggle the presentation content between the "in mix" and "separate" streams via the new  maximize and  reset buttons in the bottom-right corner of the presentation. | |
| Support for participant authentication | Support has been added for Pexip Infinity's new participant authentication feature, whereby participants attempting to access an individual Virtual Meeting Room (VMR) or Virtual Auditorium can be required to verify their identity using Single Sign On (SSO) before joining the meeting. | |
| Changes in functionality | | |
| Changes to toolbar icons | The icons to view a presentation in a separate window and close the separate window have changed from  and  to  and  respectively. | |
| The <code>wizardOnFirstRun</code> customization option is no longer supported | The <code>wizardOnFirstRun</code> customization option in the <code>settings.json</code> branding file is no longer supported. | |
| iOS version support | The v1.9 Infinity Connect mobile client for iOS requires iOS 15.2 or later. | |
| Automatic speaker detection | (iOS only) Users can no longer manually select which speaker will be used. Instead, if headphones are detected these will be used automatically, otherwise the device's speaker will be used. | |

Fixed issues

Fixed in v1.9.1 desktop client

| Ref # | Resolution |
|-------|--|
| 27867 | Resolved an issue where SSO credentials were not retained after the client was closed and re-opened. |
| 27396 | Improved security of registration password storage. |
| 25848 | Improved security of the macOS desktop client. |

Fixed in v1.9 desktop client

| Ref # | Resolution |
|-------|--|
| 26302 | Resolved an issue in v1.7 and later where the desktop client was unable to register using AD FS. |

Known limitations

| Ref # | Limitation |
|-------|--|
| 28799 | <p>Versions 1.8.x, and 1.9.1 and later of the Infinity Connect desktop client for Windows are installed in a folder under <code>C:\Users\<user>\AppData\Roaming</code> called Pexip Infinity Connect. All other versions (i.e. versions 1.7.x and earlier, and v1.9.0) are installed in the same directory in a folder called pexip-infinity-connect. These folders are where the call history and preferences are stored.</p> <p>This means that after upgrading from a version installed in one folder to a version installed in a different folder, call history and preferences will be lost. To work around this, after installation, copy the contents of the previous folder (i.e. pexip-infinity-connect or Pexip Infinity Connect, as applicable) into the new folder.</p> <p>Note that upgrades between versions that use the same installation folder are not affected.</p> |
| 18210 | The Infinity Connect desktop client may not attempt to re-register if it de-registers while minimized. |
| 18119 | Long display names are truncated when there is space available to show the full name. |
| 11854 | In some cases when sharing Office apps, the client does not capture all portions of the application window. The workaround is to share the entire desktop rather than those specific applications. |

What's new in previous releases

New in v1.8 desktop client

Version 1.8 of the Infinity Connect desktop client was released in June 2021. Below are the new features and changes in v1.8:

| Feature | Description | More information |
|--|--|------------------|
| New audio-only and inactive-video indicators in the participant list | <p>Each person in the Participant list now has an additional icon displayed if that participant is connected as audio-only, is a video-muted Infinity Connect participant, or is inactive, for example, if they are away from the computer (and thus their face cannot be detected in their video stream):</p> <p>Alice  </p> <p>Bob  </p> <p>Randolph </p> <p>where the indicators represent:</p> <p> Muted video or inactive (away)</p> <p> Connected via audio only</p> | |
| Branding and customization | <p>As from 1.8, when branding/customizing the Infinity Connect desktop client:</p> <ul style="list-style-type: none"> When provisioning the client, the brandingURL parameter can no longer refer to a Conferencing Node. Instead it now has to refer to a different server somewhere else (that is hosting the branding package). The branding package must be signed, and the client must upload a trusted (public) key before the branding can be applied. The branding package must be presented as a branding.zip file and an associated branding.zip.sig file. (The branding.zip file produced by the Pexip branding portal is a suitable zip file/format, although you must still sign it yourself.) <p>As from 1.8, the Infinity Connect mobile clients for iOS and Android can no longer be branded/customized.</p> | |

| Feature | Description | More information |
|--|---|------------------|
| Improved certificate validation | The app still detects any invalid/untrusted certificates on launch (and asks for acceptance if it is unknown, as before) but also now detects if the certificate changes in flight. If so it will pop up a dialog and when you close the dialog it goes to the disconnect destination. If you want to allow this new certificate you have to restart the client and it then asks if you want to use the new certificate as per normal behavior. | |
| More bandwidth options in the app settings | There are more bandwidth selection options available in Settings > Bandwidth. You can now choose from <i>Very Low (up to 256kbps)</i> , <i>Low (up to 576kbps)</i> , <i>Medium (up to 1264kbps)</i> , <i>High (up to 2464kbps)</i> , or <i>Very High (up to 6144kbps)</i> . The default is <i>Medium (up to 1264kbps)</i> . | |
| Enable "raise hand" in VMRs (Infinity Connect desktop client only) | By default the "raise hand" feature is only available in Virtual Auditoriums. There is a new <code>raiseHandInVMR</code> customization option in the <code>settings.json</code> file in a web app branding package that can be used to also enable the feature in Virtual Meeting Rooms. | |

New in v1.7 desktop client

There were no significant new features in the v1.7 desktop client.

Fixed issues in previous releases

Fixed in v1.8.6 desktop client

| Ref # | Resolution |
|-------|--|
| 25106 | Resolved an issue where a branding .ZIP file was not correctly loaded. |
| 24356 | Resolved an issue where a bandwidth selection of "Very High" did not always request 1080p from the camera. |

Fixed in 1.8.5 desktop client

There were no significant user-facing fixes in this release.

Fixed in 1.8 desktop client

There were no significant user-facing fixes in this release.

Infinity Connect mobile client release notes

This topic describes the new features, fixed issues and known limitations in the current and previous supported releases of the Infinity Connect mobile clients:

- [What's new?](#)
- [Fixed issues](#)
- [Known limitations](#)
- [What's new in previous releases](#)
- [Fixed issues in previous releases](#)

What's new?

New in v1.9 mobile clients

Version 1.9 of the Infinity Connect mobile clients were released in February 2022. This was the latest version at the time of publishing; to check for updates, see [What's new in Infinity Connect?](#) Below are the new features and changes in v1.9:

| Feature | Description | More information |
|--|---|------------------|
| New features | | |
| Background blur | (Desktop client for Windows only) Individual participants can now blur their own local background on the image they send to a conference. | |
| Allowing Far End Camera Control (FECC) on your own camera | Individual participants can enable their own local camera for Far End Camera Control (FECC) i.e. they can allow their own camera to be controlled (pan/tilt/zoom) by a remote participant (typically another Infinity Connect user). | |
| Receiving a presentation stream as part of the layout mix | When receiving presentation content in an Adaptive Composition layout, the presentation stream is now shown as part of the layout mix (replacing some of the other video participants), providing the client is receiving video at a medium or higher bandwidth setting (otherwise it is displayed as one large separate stream). You can toggle the presentation content between the "in mix" and "separate" streams via the new  maximize and  reset buttons in the bottom-right corner of the presentation. | |
| Support for participant authentication | Support has been added for Pexip Infinity's new participant authentication feature, whereby participants attempting to access an individual Virtual Meeting Room (VMR) or Virtual Auditorium can be required to verify their identity using Single Sign On (SSO) before joining the meeting. | |
| Changes in functionality | | |
| Changes to toolbar icons | The icons to view a presentation in a separate window and close the separate window have changed from  and  to  and  respectively. | |
| The wizardOnFirstRun customization option is no longer supported | The <code>wizardOnFirstRun</code> customization option in the <code>settings.json</code> branding file is no longer supported. | |
| iOS version support | The v1.9 Infinity Connect mobile client for iOS requires iOS 15.2 or later. | |
| Automatic speaker detection | (iOS only) Users can no longer manually select which speaker will be used. Instead, if headphones are detected these will be used automatically, otherwise the device's speaker will be used. | |

Fixed issues

Fixed in v1.9 mobile clients

| Ref # | Resolution |
|-------|---|
| 24684 | Resolved an issue where some iOS devices became unresponsive after escalation from audio-only to video. |

Known limitations

| Ref # | Limitation |
|-------|--|
| 17072 | (Android client only) pexip:// links within the client (for example, links sent via the chat window) are not recognized by the client. |

What's new in previous releases

New in v1.8 mobile clients

Version 1.8 of the Infinity Connect mobile clients were released in June 2021. Below are the new features and changes in v1.8:

| Feature | Description | More information |
|--|--|------------------|
| New audio-only and inactive-video indicators in the participant list | <p>Each person in the Participant list now has an additional icon displayed if that participant is connected as audio-only, is a video-muted Infinity Connect participant, or is inactive, for example, if they are away from the computer (and thus their face cannot be detected in their video stream):</p> <p>Alice  </p> <p>Bob  </p> <p>Randolph </p> <p>where the indicators represent:</p> <p> Muted video or inactive (away)</p> <p> Connected via audio only</p> | |
| Branding and customization | <p>As from 1.8, when branding/customizing the Infinity Connect desktop client:</p> <ul style="list-style-type: none"> When provisioning the client, the brandingURL parameter can no longer refer to a Conferencing Node. Instead it now has to refer to a different server somewhere else (that is hosting the branding package). The branding package must be signed, and the client must upload a trusted (public) key before the branding can be applied. The branding package must be presented as a branding.zip file and an associated branding.zip.sig file. (The branding.zip file produced by the Pexip branding portal is a suitable zip file/format, although you must still sign it yourself.) <p>As from 1.8, the Infinity Connect mobile clients for iOS and Android can no longer be branded/customized.</p> | |
| Improved certificate validation | <p>The app still detects any invalid/untrusted certificates on launch (and asks for acceptance if it is unknown, as before) but also now detects if the certificate changes in flight. If so it will pop up a dialog and when you close the dialog it goes to the disconnect destination. If you want to allow this new certificate you have to restart the client and it then asks if you want to use the new certificate as per normal behavior.</p> | |
| More bandwidth options in the app settings | <p>There are more bandwidth selection options available in Settings > Bandwidth. You can now choose from <i>Very Low (up to 256kbps)</i>, <i>Low (up to 576kbps)</i>, <i>Medium (up to 1264kbps)</i>, <i>High (up to 2464kbps)</i>, or <i>Very High (up to 6144kbps)</i>.</p> <p>The default is <i>Medium (up to 1264kbps)</i>.</p> | |
| Enable "raise hand" in VMRs (Infinity Connect desktop client only) | <p>By default the "raise hand" feature is only available in Virtual Auditoriums. There is a new raiseHandInVMR customization option in the settings.json file in a web app branding package that can be used to also enable the feature in Virtual Meeting Rooms.</p> | |

New in v1.7 mobile clients

There were no significant new features in the v1.7 mobile clients.

Fixed issues in previous releases

Fixed in v1.8.6 mobile clients

There were no significant user-facing fixes in this release.

Fixed in 1.8.5 mobile clients

| Ref # | Resolution |
|-------|---|
| 24569 | (iOS client only) Resolved camera switching issues after escalating from audio/content. |
| 24530 | (iOS client only) Self-view is now hidden when viewing presentation content. |
| 24529 | (iOS client only) Resolved issues with receiving presentation content (not showing or delayed). |
| 24504 | (iOS client only) Vertical images are now displayed with the correct aspect ratio when viewed on a horizontal screen. |
| 24501 | Resolved missing/incorrect Japanese translations. |
| 24459 | Calls are now cleared promptly from Pexip Infinity when a call is canceled mid-join. |
| 24445 | (iOS client only) When the device is in silent mode, an incoming non-Pexip call no longer causes an ongoing Pexip call to drop and crash the app. |
| 24436 | (iOS client only) Resolved issues where switching camera during a call caused other participants to see a frozen image. |
| 24435 | (iOS client only) Resolved issues with being able to drag and move the screen prior to joining a call. |
| 24429 | Resolved Japanese notation issues in language selection options. |
| 24428 | The app no longer switches back to English from another language after it has been closed and restarted. |
| 24427 | (iOS client only) Resolved an issue with an iPhone 8 where switching media devices while on the landing page caused the app to freeze. |
| 24426 | (iOS client only) Resolved an issue where switching media devices caused audio to become robotic. |

Fixed in 1.8 mobile clients

| Ref # | Resolution |
|-------|---|
| 23856 | (iOS client only) Resolved compatibility issues with iOS 14.5. |
| 19883 | (iOS client only) Resolved an issue where users who have been automatically disconnected from a VMR and then rejoin using the "Rejoin now" button do not receive media. |