Infinity Connect
Guide for Administrators

Introduction

About Pexip Infinity and Infinity Connect

Pexip Infinity is a virtualized and distributed multipoint conferencing platform. 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, as well as Virtual Auditoriums, which they can use to hold conferences, share presentations, and chat. Participants can join over audio or video from any location using virtually any type of communications tool (such as Microsoft Lync, a traditional conferencing endpoint, a mobile telephone, or a Pexip Infinity Connect client) for a seamless meeting experience.

Virtual Meeting Rooms and Virtual Auditoriums 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 DTMF tones on their endpoint to select the conference they want to join. The platform also includes the Pexip Distributed Gateway service, allowing end users to place point-to-point calls to other endpoints that use different protocols and media formats.

Infinity Connect clients

The Infinity Connect suite of clients allows conference participants to access any Virtual Meeting Room or Virtual Auditorium within the Pexip Infinity deployment. Infinity Connect users can also control the conference, view presentations, share content, and chat with other conference participants. Infinity Connect can also be used to make outbound point-to-point calls when used in conjunction with the Pexip Distributed Gateway.

All Infinity Connect clients can make outbound calls; the Infinity Connect desktop client and Infinity Connect Mobile client for Android can also register to Pexip Infinity in order to receive incoming calls.

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 and provides voice, video, content sharing and viewing, chat, and conference control.
- The Infinity Connect desktop client is an installable client, supported on Windows, OS X, and Linux. It provides voice, video, content sharing and viewing, chat, and conference control.

- The Infinity Connect Mobile client for Android provides voice, video, content sharing and viewing, chat, and conference control.
- The Infinity Connect Mobile client for iOS provides voice, video, content viewing, image sharing, chat, and conference control.

Infinity Connect guides for end users

We publish a series of quick guides aimed at users of the Infinity Connect desktop client, the Infinity Connect Web App when used in different browsers, and the Infinity Connect Mobile client for iOS and for Android. These guides are available in PDF format from http://docs.pexip.com/admin/download_pdf.htm.

About this guide

This guide covers topics not included in the quick guides, including those that are only relevant to an administrator.

Comparison of Infinity Connect clients

Pexip Infinity Connect is available in three main formats:

- directly from one of the following web browsers (the Infinity Connect Web App):
  - Google Chrome version 43 and later
  - Mozilla Firefox version 38 and later
  - Opera version 23 and later
  - Microsoft Internet Explorer version 10 and later (requires Flash Player 11 and later ActiveX® plug-in, and must not be in Compatibility View)
  - Microsoft Edge version 20.10240 and later
  - Apple Safari version 6 and later (Mac OS X only) (requires Flash Player 11 and later plug-in)
- as an installable desktop application (the Infinity Connect desktop client)
- as an installable application for iOS or Android devices (the Infinity Connect Mobile client).

There are some differences in features available between the different clients and browsers, as shown in the table below:

	Full audio and video mode	**Audio-only mode**	**Presentation and control-only mode** (more info)	**PDF sharing** (more info)	**Image sharing** (more info)	**Screen sharing** (more info)	**View presentations in full motion** (more info)	**Send DTMF to individual participants**	**Chat**	**Register to receive calls** (more info)	**Preconfigured links** (more info)
Desktop client	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web App via Chrome	✓	✓	✓	✓	✓	✓*	✓	✓	✓		✓
Web App via Internet Explorer	✓	✓	✓	✓	✓			✓	✓		✓
Web App via Edge	✓	✓	✓	✓	✓			✓	✓		✓
Web App via Firefox	✓	✓	✓	✓	✓		✓	✓	✓		✓
Web App via Safari	✓	✓	✓	✓	✓			✓	✓		✓
Web App via Opera	✓	✓	✓	✓	✓		✓	✓	✓		✓
Mobile client for Android	✓	✓	✓	✓	✓		✓	✓	✓	✓	
Mobile client for iOS	✓	✓	✓		✓				✓		

* Requires installation of a Chrome extension

Installing and using Infinity Connect

About the Infinity Connect Web App

The Infinity Connect Web App is available as part of all Pexip Infinity deployments. It provides a WebRTC or Flash-based interface to Pexip Infinity services.

The Web App is supported in the following browsers:

- Google Chrome version 43 and later
- Mozilla Firefox version 38 and later
- Opera version 23 and later
- Microsoft Internet Explorer version 10 and later (requires Flash Player 11 and later ActiveX® plug-in, and must not be in Compatibility View)
- Microsoft Edge version 20.10240 and later
- Apple Safari version 6 and later (Mac OS X only) (requires Flash Player 11 and later plug-in)

Infinity Connect users can share images and PDFs from any browser. Additionally, Chrome users can share their screen if they first install a chrome extension. The screen-sharing feature is not available from other browsers but is available from the Infinity Connect desktop client.

To access a conference 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, followed by **/webapp/** (for example, **rp.example.com/webapp/**). Users are then presented with a screen from where they can then 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.

Note that:

- Chrome, Firefox and Opera browsers can connect to privately-addressed "on-premises" nodes via a reverse proxy and route their media through a TURN server (as they use the WebRTC protocol).
- Internet Explorer, Edge, and Safari browsers can connect via a reverse proxy, but they cannot establish audio/video paths to Pexip Infinity via a TURN server (as they use the RTMP protocol). To establish audio/video media connectivity, RTMP clients need a direct TCP connection to a Conferencing Node. The Web App will attempt an encrypted RTMPS connection first. For a secure RTMP connection to be established, the **SIP TLS FQDN** must be configured on the Conferencing Node (via **Platform configuration > Conferencing Nodes**) and it must match the Common Name of its TLS server certificate. If RTMPS fails, it will use an unencrypted connection for media.

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

Installing and managing Chrome extensions

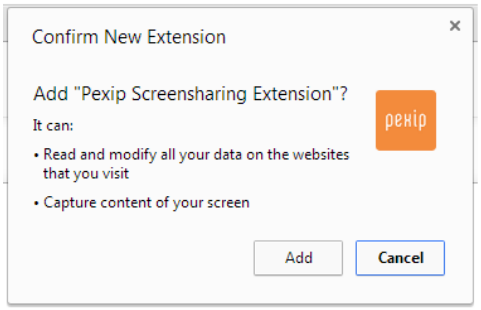
Enabling screen sharing in Chrome

Before you can use Infinity Connect via Google Chrome to share your computer screen with other conference participants, you must install the Pexip Screensharing Extension (screensharing is not currently available from any other browser).

To download the extension:

1. Go to http://www.pexip.com/extension and click on the link provided there.
   This will take you to the Pexip Screensharing Extension on the Chrome web store.
2. Download the extension by clicking on the 

button at the top right of the page.
   The following confirmation will appear:



3. Select **Add**.

You are now ready to share your screen.

Managing the Pexip Screensharing Extension

The Pexip Screensharing Extension maintains a list of all of the domains (or websites) that you have allowed to use the extension.

To remove domains from this list:

1. Go to **chrome://extensions** (type this in to your Chrome browser's address bar).
2. Select **Options** under the **Pexip Screensharing Extension**.
3. Select **X** by any domain you want to remove.

If you subsequently attempt to share your computer screen while participating in a conference hosted at a domain that you have removed, you will once again be asked to allow the **Pexip Screensharing Extension** to share your screen.

About the Infinity Connect desktop client

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 Pexip Infinity.

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 7 and later
- Mac OS X 10.7 and later
- Ubuntu Linux

The Infinity Connect desktop client does not verify TLS certifications and therefore should not be used on untrusted networks.

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

To install the Infinity Connect desktop client, go to **www.pexip.com/software-download** and download and install the appropriate file for your OS:

- Windows: **pexip-infinity-connect_windows-ia32_<release>.msi**. Click on this file to install the Infinity Connect desktop client automatically. During the installation process the Infinity Connect icon will be added to the desktop, and an entry will be added to the Windows registry to allow links prefixed with **pexip:** to open automatically in the Infinity Connect desktop client.
- OS X: **pexip-infinity-connect_osx-ia32_<release>.dmg**. Unzip this file and move it to the **Applications** folder.
- Linux 32-bit: **pexip-infinity-connect_linux-ia32_<release>.tar.gz**. Unzip this file and move it to the desired folder.
- Linux 64-bit: **pexip-infinity-connect_linux-x64_<release>.tar.gz**. Unzip this file and move it to the desired folder.

When users open the desktop client, they are asked to enter the alias of the conference or person they want to call (for example **meet.alice@example.com**).

System administrators and conference organizers can also provide a preconfigured link to a conference alias.

About the Infinity Connect Mobile client for Android

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 client for Android can be used by conference participants to control the conference and view presentations from their own personal device, even when they are using a separate video endpoint to participate in the conference.

In addition, the latest release of the Infinity Connect Mobile client for Android also includes the ability to join a conference over audio-only, or as a full audio and video participant, allowing users to participate in a conference from anywhere they have an internet connection.

Most standard Infinity Connect features are available to Infinity Connect Mobile client users, along with these additional features:

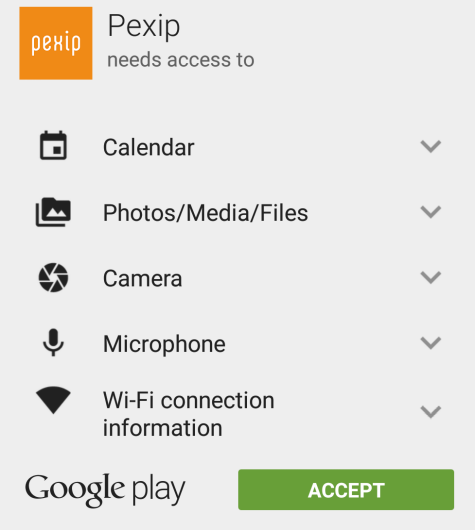
- View the presentation on their personal device.
  - **Video participants** can elect to use their video endpoint just for viewing other participants, while viewing the presentation on their device - essentially providing them with a dual-screen video system.
  - **Audio-only participants** will be able to view the presentation on their personal device, enhancing their conference experience.
- Decide where they want to view the presentation: on their mobile device, on the video endpoint, or both.

Installing the Infinity Connect Mobile client for Android

Version 2.0 of the Infinity Connect Mobile client for Android requires Android 4.0 or later.

It is available for free from the Google Play store at https://play.google.com/store/apps/details?id=com.pexip.android. Follow the instructions to download and install the Infinity Connect Mobile client on your device.

When installing the Infinity Connect Mobile client for Android, it will request permission to access the contacts/calendar on your device:



You must **accept** this request to continue with the installation.

Pexip for SECTOR Network

Special versions of the Infinity Connect Mobile client, called Pexip for SECTOR Network, are also available for iOS and Android. These versions are for use in enterprises that require all mobile apps to work with management solutions based on OpenPeak's ADAM platform, and include additional security features, functionality, and IT management capabilities. For more information, see www.pexip.com/article/news/pexip-app-for-sector-network.

Pexip for SECTOR Network for Android is available for free from the Google Play store at https://play.google.com/store/apps/details?id=com.pexip.android.SEC_APP.

About the Infinity Connect Mobile client for iOS

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 client for iOS can be used by conference participants to control the conference and view presentations from their own personal device, even when they are using a separate video endpoint to participate in the conference.

In addition, Infinity Connect Mobile client for iOS users can join a conference over audio-only, or as a full audio and video participant, allowing them to participate in a conference from anywhere they have an internet connection.

Most standard Infinity Connect features are available to Infinity Connect Mobile client users, along with these additional features:

- View the presentation on their personal device.
  - **Video participants** can elect to use their video endpoint just for viewing other participants, while viewing the presentation on their device - essentially providing them with a dual-screen video system.
  - **Audio-only participants** will be able to view the presentation on their personal device, enhancing their conference experience.
- Decide where they want to view the presentation: on their mobile device, on the video endpoint, or both.
- Zoom in on the presentation on their device, allowing them to see details that would otherwise not be visible from a distance on the screen.

Bandwidth selection

The Infinity Connect Mobile clientfor iOS will automatically select an appropriate bandwidth, as follows:

- wide-CIF for cellular (3G and 4G) connections
- 448p for WiFi connections.

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/id667867771. Follow the instructions to download and install the client on your device.

- **Version 5.0** is compatible with any iOS device running iOS 8.x or later, and Pexip Infinity version 7 or later.
- **Version 1.1** is compatible with any iOS device running iOS 7.x or 8.x, and is optimized for iPhone 5.
- **Version 1.0.3** is available for devices running earlier iOS versions (iOS 5.1 to iOS 6.x).

Pexip for SECTOR Network

Special versions of the Infinity Connect Mobile client, called Pexip for SECTOR Network, are also available for iOS and Android. These versions are for use in enterprises that require all mobile apps to work with management solutions based on OpenPeak's ADAM platform, and include additional security features, functionality, and IT management capabilities. For more information, see www.pexip.com/article/news/pexip-app-for-sector-network.

Pexip for SECTOR Network for iOS will be available for free from the Apple store soon.

Registering your device to receive calls

If you want to be able to receive calls on your Infinity Connect desktop client, Infinity Connect Mobile client for Android, or your SIP or H.323 endpoint, you must first register it with Pexip Infinity using an alias, username, and password provided by your system administrator. These credentials must match a registration entry on Pexip Infinity in order for the registration to be accepted.

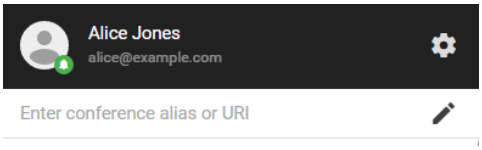
Registration is optional. You do not need to register your device in order to make calls, just to receive them.

Infinity Connect clients

To register your Infinity Connect desktop client or Infinity Connect Mobile client for Android to receive calls (if this is supported in your deployment):

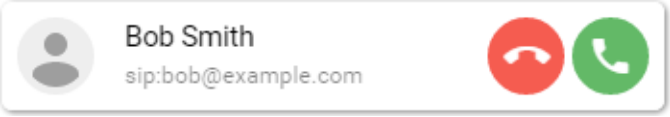
1. Go to the **Settings** screen (from the top right of the Infinity Connect home screen, select **Settings**).
2. In the **Registration** section of the **Settings** screen, enter the **Alias** and **Password** provided to you by your administrator. Be aware that the username and password are case-sensitive, and some devices will default to uppercase for the first character of the user name.
3. Select **Remember password**.
4. Select **Register**.

When you have successfully registered, the button will change to **Unregister**, and when you return to the home screen (by selecting) there will be a green icon next to your name and your registered alias will be shown underneath:



The notification icon for Infinity Connect will also have a green dot on it: . This dot will change to red if you become unregistered: .

Now, when someone calls your endpoint by dialing the **Alias** you have registered with, you will get an incoming call alert at the bottom right of your screen showing the name and address of the person or meeting room who is calling you:



For the Infinity Connect desktop client, you can disable the sound of the incoming call alert by going to **Settings** and selecting a **Ringtone** of ***None***.

Configuring a default domain

If you frequently use Virtual Meeting Rooms and Virtual Auditoriums that have aliases with the same domain, you can configure the Infinity Connect desktop client and Infinity Connect Mobile client so that you only need to enter the initial part of the alias. For example, if you often access Virtual Meeting Rooms with the aliases **meet.alice@example.com**, **meet.bob@example.com** and **meet.sales@example.com**, you could configure the Infinity Connect Mobile client with a **Domain** of **example.com**, so that you only need to enter **meet.alice**, **meet.bob** or **meet.sales** in the URI field in order to join the Virtual Meeting Room.

If you have set up a preconfigured domain, you can still enter Virtual Meeting Room and Virtual Auditorium aliases that use a different domain. Just enter the full URI in the **URI** field - the preconfigured domain will be ignored.

Infinity Connect desktop client and Infinity Connect Mobile client for Android

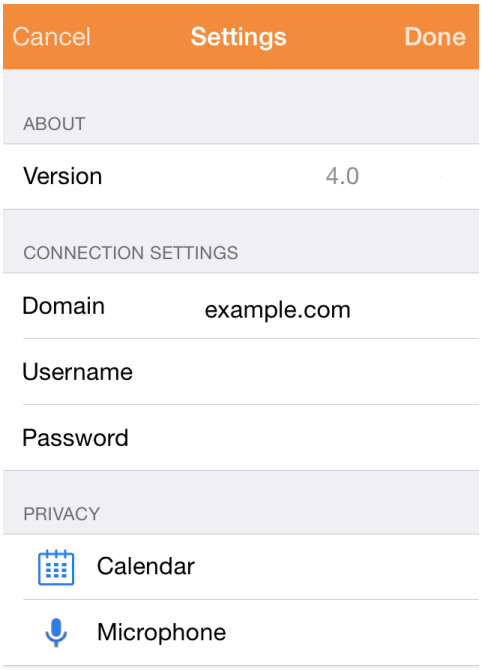
To preconfigure the Infinity Connect Mobile client for Android with a domain:

1. Select **Settings** at the top left of the Infinity Connect window.
2. In the **Connections** section, enter the **Default domain**.

Infinity Connect Mobile client for iOS

To preconfigure the Infinity Connect Mobile client for iOS with a domain:

1. Select **Connection settings**.
2. In the **Domain** field, enter the domain.



3. Select **Done**.

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. What you can share depends on which of the Infinity Connect clients you are using.

If you are already in the call using another video endpoint, you can open and 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.

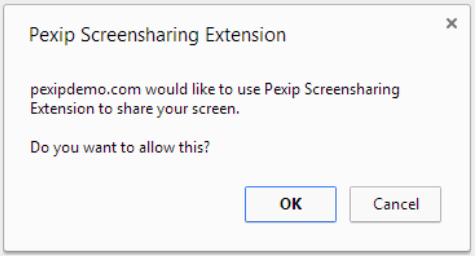
Sharing your screen

Screen sharing is available from:

- the Infinity Connect desktop client
- the Infinity Connect Web App via Chrome (requires the installation of a Chrome extension).

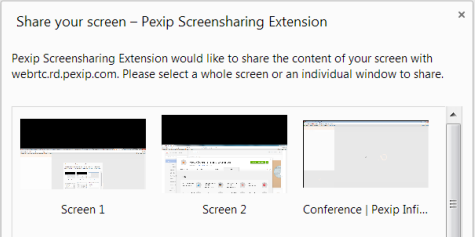
To share your screen:

1. For Chrome users, ensure you have enabled screen sharing.
2. From the toolbar at the bottom of the screen, select **Share screen** .
3. The first time that you use Infinity Connect via Chrome to share your screen from a conference hosted at a particular domain, a confirmation window will appear:



Select **OK** to confirm that you want to share your screen.

4. Select either the entire screen or the individual window you want to share, and then select **Share**.



Sharing images and PDFs

Supported formats and clients

Images

You can share images from any Infinity Connect client. Infinity Connect supports the following image formats:

- JPG
- BMP
- PNG
- GIF

PDFs

You can share PDFs directly from:

- the Infinity Connect desktop client
- the Infinity Connect Web App
- Infinity Connect Mobile client for Android

PowerPoint presentations

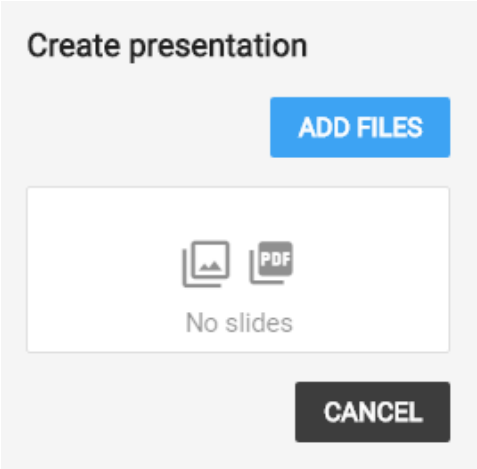
You can't share PowerPoint presentations directly using this method. To share PowerPoint presentations, either

- Save the presentation as a PDF, and share that.
- (If you are using Infinity Connect via the Desktop client or Chrome) From PowerPoint, open the presentation as a slide show, and then share your screen.

How to share images or PDFs

To share images or PDFs:

1. From the toolbar at the bottom of the screen, select **Share images or PDFs** .
   The **Create presentation** screen will appear:



2. Select **Add files**, or drag and drop the file(s) you want to share into the Infinity Connect window. You can add multiple files, and they can be a combination of images and PDFs (if supported by your device). Each image will be converted into an individual slide, as will each page of each PDF.

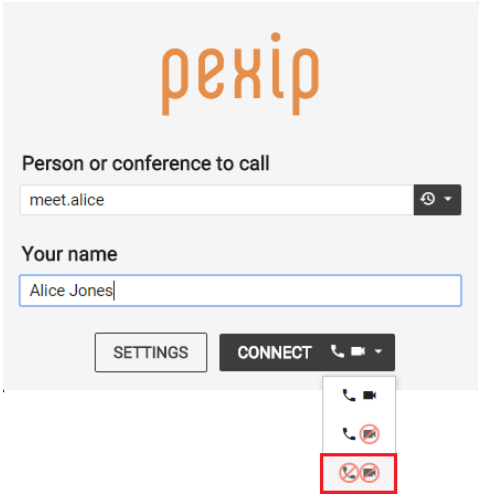
3. Select **Start presenting** and use the left < and right > controls at the top of the screen to scroll through the slides.
4. To stop sharing the slides, from the toolbar select **Stop presenting**.

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

Using Infinity Connect just to share content

If you are in a conference using an endpoint other than Infinity Connect (for example, a dedicated meeting room system) and you want to share content from your computer or mobile device without activating your camera and microphone:

1. Open the Infinity Connect client on your computer or mobile device and enter the details of the Virtual Meeting Room or Virtual Auditorium you are in.
2. From the drop-down options on the **Connect** button, select **Conference control and receive/send presentation only**:

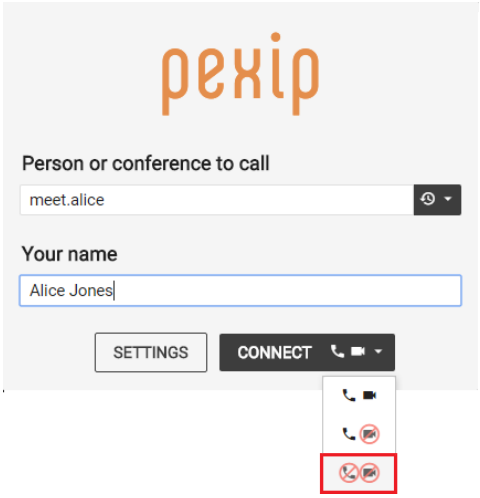


3. From the toolbar, select **Share screen** (Infinity Connect desktop client and Infinity Connect Web App via Chrome only), or **Share images or PDFs**.

Using Infinity Connect for presentation, chat and conference control only

If you are already in a conference using an endpoint other than Infinity Connect, you can still access the additional features available to Infinity Connect users (such as conference control, chat, content sharing, and viewing the roster of participants) by using Infinity Connect to join the conference without activating your camera and microphone.

To do this, from the drop-down options on the **Connect** button, select **Conference control and receive/send presentation only**:



You can now view and share content, 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.

You can also activate your camera and microphone, or just your microphone, at any time after you have joined the conference by selecting either **Join with video** or **Join with audio only**.

Locking a conference and allowing participants to join a locked conference

If you want to prevent any further participants from joining a conference after it has started, you can lock it by either using the Administrator interface or using Infinity Connect. After a conference has been locked, participants who are attempting to join the conference can be allowed in individually by participants already in the conference.

The impact of locking 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 will be able to join the conference until it is locked.
- After the conference has been locked, any further participants who attempt to join the conference (including any Automatically Dialed Participants and manually-invited participants) will be held at the **Waiting for conference host** screen.
- All participants who are already in the conference will be notified of any participants who are attempting to join the locked conference, and will be able to allow the waiting participants to join.
- When 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 will be able to join the conference until it is locked.
- After the conference has been locked, participants who enter the Host PIN will be able to join the conference immediately - locking does not apply to them.
- After the conference has been locked, Guest participants (including any Automatically Dialed Participants and manually-invited participants who have been given a role of Guest) will be held at the **Waiting for conference host screen**.
- All Host participants who are already in the conference will be notified of any Guest participants who are attempting to join the locked conference, and will be able to allow the waiting Guest participants to join.
- When the conference is unlocked, any Guest participants who are still waiting will automatically join the conference.

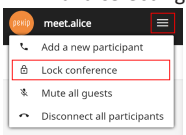
Locking using the Administrator interface

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

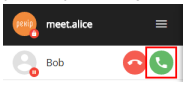
Host participants using Infinity Connect can lock and unlock the conference they are in by clicking on the conference control menu and selecting **Lock conference** or **Unlock conference** as appropriate:



A "locked" icon will appear next to the conference avatar to indicate that the conference is currently locked.

Allowing waiting participants to join a locked conference

When a new participant attempts to join a locked conference, Host participants in the conference who are using Infinity Connect are notified that the participant is waiting to join, and see a red "waiting" icon next to the participant's avatar. To allow the participant to join the locked conference they can click on the green telephone icon next to the participant's name:



In the above example, Bob is waiting to join Alice's locked VMR. Alice is a Host, so can let him join at any time by clicking on the green telephone icon next to Bob's name.

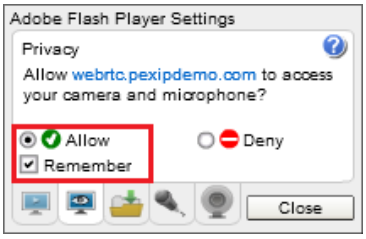
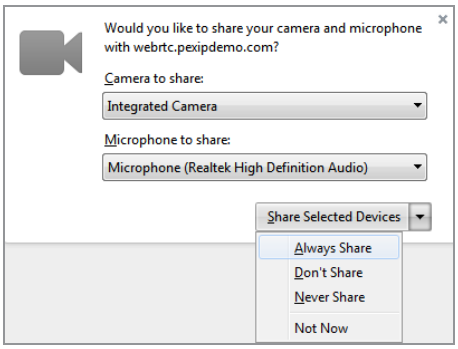
Rejecting a request to join a locked conference

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

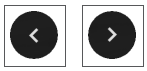
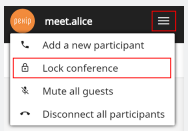
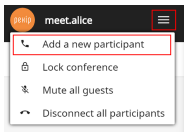
- To reject the request completely, the Host participant must click on the red telephone icon next to the waiting participant's name. The waiting participant's call will be disconnected.
- To leave the participant at the waiting for Host screen, the Host participant should do nothing. The waiting participant 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 conference finishes (after which the waiting participant's call will be disconnected).

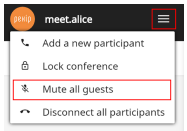
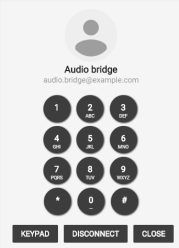
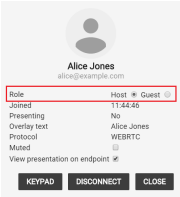
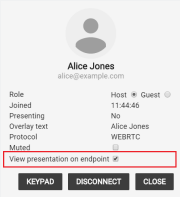
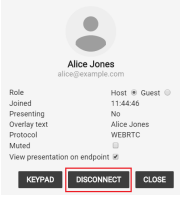
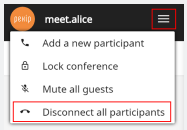
Using Infinity Connect in-call controls

The table below shows the actions that can be performed while a call is in progress. Note that this table includes all features available to the Infinity Connect desktop client, the Mobile client for Android, and the Web App, although not all features are available to all clients. For the features that are available to the Infinity Connect Mobile client for iOS, see the Infinity Connect Mobile client for iOS Quick Guide.

Select the default microphone and camera to use prior to joining over video/audio	**Desktop client and Mobile client for Android** 1. From the home screen, select ⚙. 2. In the **Media** section, select the desired microphone and camera from the drop-down menus. **Web App for Chrome and Opera** 1. From the home page, select **Settings**. 2. In the **Microphone** and **Camera** sections, select the desired devices from the drop-down menus. **Web App for Edge, Internet Explorer and Safari** 1. From the home page, select **Settings**. 2. In the **Microphone** and **Camera** sections, select the desired devices from the drop-down menus. You may need to first enable Adobe Flash by selecting **Allow**, and checking **Remember**:  **Web App for Firefox** 1. From the home page, select **Settings**. 2. In the **Microphone** and **Camera** sections, select the desired devices from the drop-down menus. You may need to first share your camera and microphone:  ⓘ If you always use the same camera and microphone, you may wish to also clear the **Show camera / microphone options when connecting** option in the **Advanced** section of the **Settings** page. Doing so will mean that you won't then have to take the extra step of nominating the camera and microphone to use each time you make a call.

Share your screen with all other participants	(Available to Infinity Connect desktop client and Infinity Connect Web App via Chrome users only) 1. For Chrome users, ensure that you have enabled screen sharing. 2. From the toolbar at the bottom of the window, select **Share screen**. 3. Select the window or screen you want to share. 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.	
Share images or PDFs with all other participants	1. From the toolbar at the bottom of the window, select **Share images or PDFs**. 2. Drag and drop the file(s) you want to share into the Infinity Connect window. You can add multiple files, and they can be a combination of images and PDFs. Each image will be converted into an individual slide, as will each page of each PDF. 3. Select **Start presenting**. The first slide will appear in a presentation thumbnail at the top left of the screen (or in the main video window if you are presentation-only). Use the left < and right > controls to scroll through the slides. You can make the slides appear in your main video window by clicking on the presentation thumbnail. 4. To stop sharing the slides, from the toolbar select **Stop presenting**.	
View a presentation being shown by another participant	When a participant starts a presentation, you will automatically see the content they are sharing as your main image, and the image of the participants will reduce to a small thumbnail at the top left corner. You can toggle between viewing the presentation and viewing the participants by clicking on the thumbnail.	
View a presentation in a separate window	Whether you are the presenter or a participant, you can view the current presentation in a separate pop-out window. To do this, from the bottom right of the screen select **Open presentation in new window**. To close the window, from the bottom right of the screen select **Close**.	
View a presentation at a higher (or lower) refresh rate	When a participant is showing a presentation, by default you receive it as a series of still images. This is suitable for documents and screens being shared, but if the presentation contains a lot of movement it may appear jerky. If this is the case, you can elect to receive the presentation in full motion. To do this, from the bottom right of the screen select **View full motion presentation**. To return to the default view, select **View still image presentation**.	
Start sending and receiving video	(For users who have initially joined without audio and video) From the toolbar at the bottom of the window, select **Connect with audio and video**. Select the camera and microphone you wish to use, and then select **Start**.	
Start sending and receiving audio	(For users who have initially joined without audio and video) From the toolbar at the bottom of the window, select **Connect with audio only**.	
Stop/start sending your video to other participants	From the toolbar at the bottom of the window, select **Disable my camera** or **Enable my camera**.	
Stop/start sending your audio to other participants	From the toolbar at the bottom of the window, select **Mute my microphone** or **Unmute my microphone**.	

View the video image full screen/exit fullscreen	From the toolbar at the bottom of the window, select **Go full screen** or **Exit full screen**.	
Stop/start viewing the video of yourself	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, select the **Hide self view** icon at the top right of the image. It will be replaced by a small **Show self view** icon; select this to view your image again.	
View a list of other conference participants	When using Infinity Connect, a list of all other conference participants will be shown to the left of or at the bottom of the screen. You can scroll through this list, or use the search box at the top of the list, to view other participants. You can show and hide this participant list by clicking on the **Hide side bar <** and **Show side bar >** icons at the bottom right of the list.	
Send and receive chat messages, and share online videos and images	(Available when chat has been enabled by the administrator) At the bottom of the screen there is a **Chat room** area, which shows the messages sent by participants in the conference. To send a message, type it in the bottom window. Messages are visible to everyone else in the conference with a chat-capable client (such as Lync or Infinity Connect). You can also share videos and images by pasting their URL into the chat window.	
Show or hide the roster or chat room	To hide or show the side panel (containing the list of participants and the chat room), select the arrows at the bottom left of the screen. To hide the chat room within the side panel so that only the roster is shown, or to expand it so that only the chat room is shown, select the arrows to the right of the chat room title bar.	 
Prevent/allow others from joining the conference	(Requires Host privileges) From the top left of the screen, select the menu icon and then select **Lock conference** or **Unlock conference**. The impact of locking depends on whether or not the Virtual Meeting Room or Virtual Auditorium being used has a Host PIN. For more information, see Locking a conference and allowing participants to join a locked conference.	
Add a participant to the conference	(Requires Host privileges) 1. At the top left of the screen, select the menu icon and then select **Add a new participant**. 2. At the prompt, enter the address of the person you want to dial. 3. If you want to use a protocol other than **SIP** (the default) select either **H.323** or **Lyc/Skype**. **RTMP** is typically used when connecting to a streaming or recording service. 4. Select whether you want the participant to have **Host** or **Guest** privileges. 5. Select **OK**.	
Mute/unmute another participant	(Requires Host privileges) From the participant list, to the right of the participant's name select **Mute participant** or **Unmute participant**.	

Muting all Guests	(Requires Host privileges) From the top left of the screen, select the menu icon and then select **Mute all guests**.	
Send DTMF tones	(Requires Host privileges; you must be joined over audio, or video and audio) From the participant list, select the participant to whom you want to send DTMF tones, and then select **Keypad**. 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.	
Change the role of a participant	(Requires Host privileges; you cannot change your own role to Guest.) From the participant list, select the participant's name, and then use the radio buttons to select whether their role will be **Host** or **Guest**.	
Stop sending presentation to a participant	(Requires Host privileges) 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 and you are already viewing the presentation on your mobile device). To do this, from the participant list, select the participant's name and then uncheck **View presentation on endpoint**.	
Disconnect another participant	(Requires Host privileges) From the participant list, select the participant's name and then select **Disconnect**.	
Disconnect all participants (including yourself)	(Requires Host privileges) From the top left of the screen, select the menu icon and then select **Disconnect all participants**.	
Disconnect yourself from the conference	From the toolbar at the bottom of the screen, select **Disconnect**.	
View diagnostic information about your call (when connected with audio or video)	From the bottom right of the screen, select **Call statistics**. This brings up an overlay dialog that displays the server version of the host system. Further statistics may also be displayed, if available, such as incoming and outgoing audio and video bitrates, and how many data packets have been lost and received etc.	

Participant icons

The table below shows the different icons or "badges" that can appear on participants' avatars, and their meanings.

	A call is being placed to the participant and they have yet to answer.
	The participant is waiting to join the conference.
	The participant is a streaming or recording device.
	The participant is currently speaking.
	The participant is muted.
	The participant is presenting content.

Administering Infinity Connect

About Infinity Connect client settings

There are various settings available within the Infinity Connect clients. The tables below provide information about each of these settings, and shows which clients use them.

Note that you can change, disable or provide default text for many of these settings by Customizing the Infinity Connect desktop client and Customizing the Infinity Connect Web App.

Desktop client, Android client and Web App

Setting	Description	Desktop client	Android client	Web App
Your name	The name for this user, which will appear to other conference participants. For Desktop client users, this field is automatically pre-filled with the user name of the account used to log in to the device, but it can be overwritten.	✓	✓	✓
Registration alias	The alias that this client will register with. This is the alias that other users will dial when they want to call this client. This alias must match one of the entries on the Management Node under **Service configuration > Device aliases**.	✓	✓	
Registration server address *	The address of the server to which the registration request will be sent. This must be the IP address or FQDN of a local Conferencing Node, or the IP address or FQDN of the reverse proxy. This field is initially hidden from desktop client users unless they expand the section by selecting ⌄. If no server address is entered, Infinity Connect will attempt to register by using the domain returned by an SRV lookup of the domain part of the registration alias as the server address (for more information, see Setting up DNS records for Infinity Connect Mobile client and Infinity Connect desktop client use). If there is no SRV record, it will use the domain part of the registration alias itself as the server address. If this fails, users will be presented with the expanded section where they can enter a different server address.	✓	✓	
Registration user name and password	The username and password to be used by this device when it is registering to Pexip Infinity. The username and password must match those configured for this alias on the Management Node under **Service configuration > Device aliases**. The registration user name is initially hidden from desktop client users unless they expand the section by selecting ⌄. If no user name is entered, Infinity Connect will attempt to register using the local part of the registration alias as the user name. If this fails, users will be presented with the expanded section where they can enter a different user name.	✓	✓	
Connection default domain *	The domain that will be appended to any URIs that are dialed from this client that do not already include a domain.	✓	✓	
Connection server address *	The address of the server to which calls may be sent (see Setting up DNS records for Infinity Connect Mobile client and Infinity Connect desktop client use for a full description of how the client determines and locates the host server). If configured, this must be the IP address or FQDN of a local Conferencing Node, or the IP address or FQDN of the reverse proxy.	✓	✓	

Setting	Description	Desktop client	Android client	Web App
Camera	Allows users to select the camera they wish to use from the drop-down list, and see how their video will appear to other participants.	✓	✓	✓
Microphone	Allows users to select the microphone they wish to use from the drop-down list, and check that it is working properly.	✓	✓	✓
Bandwidth	The maximum bandwidth for the call, and the bandwidth at which the initial call attempt will be made. Note that calls may be temporarily downspeeded due to network conditions.	✓	✓	✓
Show camera / microphone options when connecting *	When this option is selected, users will always be given the opportunity to check and change their microphone and camera prior to joining a call with media. To speed up the joining process, you may wish to clear this option if you always use the same camera and microphone on your device. Selecting the **Don't show me these options again checkbox** when joining a call will automatically clear the **Show camera / microphone options when connecting** checkbox.	✓	✓	✓
Mute microphone when first connecting *	Many videoconference participants mute their microphones unless they are actually speaking, to reduce the level of background noise. This option allows users to join with their microphone muted by default.	✓	✓	✓
Start application in the background	When this option is selected, the client will start automatically when you start your computer. If you have previously entered your registration details and selected **Remember password**, the client will also register on startup, meaning you can receive calls as soon as you log in to your computer.	✓		
Show confirmation dialog when disconnecting *	When this option is selected, users must confirm each time they wish to disconnect from a conference. This prevents users from accidentally disconnecting themselves.	✓	✓	✓
View full motion presentation by default *	This setting determines how presentations from other participants are initially received by this user. Presentations can be received in two formats: • A lower-bandwidth series of **still images** (suitable for documents and screens being shared). With this option, Pexip Infinity periodically takes a snapshot of the presentation and converts it to .jpeg format, and sends that to the Connect client. For this reason, presentations that contain a lot of movement may appear jerky to clients using this option. • A higher-bandwidth **full motion** stream (suitable for presentations with a lot of movement). This option sends the presentation as a video stream, so movement will appear smooth. By default, presentations are initially shown as still images, and users can subsequently elect to view them in full motion by selecting the **HD** button. However, when **View full motion presentation by default** is selected, presentations received by this user will always be shown in full motion by default, and the user can then elect to view it as still images.	✓	✓	✓ †
Send anonymous usage statistics to Pexip *	When this option is selected, anonymous information about how the client is being used is sent to Pexip.	✓	✓	✓
Play ringtone on incoming calls	If users do not want to hear the default ringtone when they are receiving an incoming call, they can clear this checkbox.	✓		

Setting	Description	Desktop client	Android client	Web App
Language *	(Only applies if additional languages have been configured via customization.) Allows users to select from a drop-down menu the language to be used in their Infinity Connect client.	✓		✓

* You can provide a first-time default for this option by Customizing the Infinity Connect desktop client or Customizing the Infinity Connect Web App.

† Not available in Internet Explorer, Edge, or Safari.

Mobile client for iOS

Setting	Description	Path
Name	The name for this user, which will appear to other conference participants. If you don't set a name here, your device's name will be used.	From the Infinity Connect home screen, select **Connection Settings** > **Display Name**.
Domain	The domain that will be appended to any URIs that are dialed from this client that do not already include a domain.	From the Infinity Connect home screen, select **Connection Settings** > **Domain**.
Username Password	The username and password that will be sent by the iOS client in response to an HTTP authentication request. Some connections, such as those to a reverse proxy, may require HTTP authentication.	From the Infinity Connect home screen, select **Connection Settings** > **Username**.

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 bottom right of the Infinity Connect screen, select **Call statistics** ⓘ.

Creating preconfigured links to conferences via Infinity Connect

Links to Infinity Connect Web App

You can provide conference participants with a URL that, when clicked, will open an instance of Infinity Connect in their default browser. You can format the URL with query string parameters so that it pre-fills some or all of the required fields and allows the participant to review these before joining, or you can format the URL so the participant is taken straight into the conference.

The URL is in the format:

https://**<address>**/webapp/?conference=**<alias>**&name=**<name>**&bw=**<bandwidth>**&pin=**<PIN>**&join=**<join>**&role=**<role>**&media=**<media>**&audioonly=**<audioonly>**&escalate=**<escalate>**&extension=**<extension>**

where:

- **<address>** is the IP address or domain name of the Conferencing Node or reverse proxy
- **<alias>** is one of the aliases for the Virtual Meeting Room or Virtual Auditorium the user will join
- **<name>** is the name of the user who is joining the conference
- **<bandwidth>** is the bandwidth in kbps, and can be any number between 256 and 1864
- **<PIN>** is either the Host or Guest PIN, if required
- **<join>** is **1** if you want the participant to automatically join the conference, otherwise it is not present

- **<role>** is either **host** or **guest** and is used when the URL does not contain a PIN (for example, to allow Guests to automatically join a conference that has no Guest PIN). However, if the URL already specifies a **<PIN>**, the PIN will determine the participant's role and the **<role>** will be ignored.
- **<media>** is **1** if you want to start your camera and microphone immediately after joining, or is left empty if you want to join in presentation and control mode.
- **<audioonly>** is **1** if you want to start an audio-only call.
- **<escalate>** is **1** if you want users to be offered the camera and microphone selection options immediately upon joining (only applies when the option to start media immediately has not been activated, i.e. in conjunction with **media=**.
- **<extension>** is the Virtual Reception extension, or the Lync Conference ID.
- **<forceguest>** is **1** if you want to withhold Host-level controls (such as muting all guests) even if the participant joins as a Host.

The URL must always include **https://<address>/webapp/?**; the remainder of the fields are optional, as follows:

- If a field is not specified in the URL but is required when joining (i.e. **alias**, **name**, **PIN** if the conference uses PINs, or **extension** if one is requested), the participant will be required to provide the information themselves before they can join the conference.
- If the **bandwidth** is not specified in the URL and the participant has not previously selected a different value, the default of 576 will be used.

Examples

- If the domain name of your reverse proxy is **conference.example.com**, and there is a Virtual Meeting Room with the alias **meet.alice**, which has no PIN, the URL for Bob to join it directly would be:
  https://conference.example.com/webapp/?conference=meet.alice&name=Bob&join=1
- If we then gave the same Virtual Meeting Room a Host PIN of **1234** but no Guest PIN, the URL for Bob to join it directly as a **Host** would be:
  https://conference.example.com/webapp/?conference=meet.alice&name=Bob&pin=1234&join=1
  and the URL for Bob to join it directly as a **guest** would be:
  https://conference.example.com/webapp/?conference=meet.alice&name=Bob&join=1&role=guest
  and the URL for Bob to join it directly as an audio-only guest would be:
  https://conference.example.com/webapp/?conference=meet.alice&name=Bob&join=1&role=guest&media=1&audioonly=1
- If we wanted Bob to join directly as a guest with audio and video, but allow him to select and check his camera and microphone prior to joining, the URL would be:
  https://conference.example.com/webapp/?conference=meet.alice&name=Bob&join=1&role=guest&media=&escalate=1

Links to Infinity Connect desktop client

You can create a URL that, when clicked, will open an instance of the Infinity Connect desktop client with the conference name pre-filled. This URL can be included in web pages or emails (but note that some email clients such as Gmail will strip them out for security reasons).

This URL is in the format:

pexip:**<alias>**

where:

- **<alias>** is one of the aliases for the Virtual Meeting Room or Virtual Auditorium the user will join.

Example

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 the Infinity Connect desktop client installed clicks on the link in her email, the client will open automatically with **meet.alice@example.com** already entered, and all they need to do is select **Connect**.

Using Infinity Connect from outside your network

In most cases, your Pexip Infinity deployment will be located inside a private network. If this is the case and you wish 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, note that:

- Chrome, Firefox and Opera browsers can connect to privately-addressed "on-premises" nodes via a reverse proxy and route their media through a TURN server (as they use the WebRTC protocol).
- Internet Explorer, Edge, and Safari browsers can connect via a reverse proxy, but they cannot establish audio/video paths to Pexip Infinity via a TURN server (as they use the RTMP protocol). To establish audio/video media connectivity, RTMP clients need a direct TCP connection to a Conferencing Node. The Web App will attempt an encrypted RTMPS connection first. For a secure RTMP connection to be established, the **SIP TLS FQDN** must be configured on the Conferencing Node (via **Platform configuration > Conferencing Nodes**) and it must match the Common Name of its TLS server certificate. If RTMPS fails, it will use an unencrypted connection for media.

This means that Internet Explorer, Edge and Safari users connecting from outside your network will not be able to send or receive media. These users should connect over a VPN, or use another browser.

For more information, see **Pexip Reverse Proxy and TURN Server Deployment Guide**.

Enabling and disabling Infinity Connect clients

If you do not wish to allow participants to use Infinity Connect clients (Infinity Connect desktop client, Infinity Connect Mobile client, and Infinity Connect Web App) to access conferences within your deployment, you can disable this feature.

This feature is enabled by default. To disable or re-enable this feature:

1. Go to **Platform configuration > Global settings**.
2. From within the **Connectivity** section, deselect or select **Enable support for Pexip Infinity Connect and Mobile App**.

When access has been disabled, users attempting to use Infinity Connect clients to access a conference or make a call will be presented with the message **Call Failed: Disabled**. This message is customizable; for more information see Customizing the Infinity Connect Web App.

Setting up DNS records for Infinity Connect Mobile client and Infinity Connect desktop client use

To enable participants to connect to conferences within your deployment using the Infinity Connect desktop client or Infinity Connect Mobile client, you must provide a DNS lookup so that these clients know which host to contact. The host will typically be a reverse proxy (for deployments where Conferencing Nodes are located within a private network), but it can also be a public-facing Conferencing Node.

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

The SRV records for **_pexapp._tcp.<domain>** should always reference port 443 on the host.

More information on the lookup process for the desktop client and mobile client is described below, along with an example.

(Note that the DNS SRV lookup does not apply to participants using the Infinity Connect Web App, because they connect to Conferencing Nodes or the reverse proxy directly, so no 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.

Infinity Connect desktop client

The Infinity Connect desktop client (as of version 2.1 and later) may attempt several DNS lookups for different domains — based on the dialed alias and the client's configuration — until it is able to connect to a reverse proxy or Conferencing Node.

The domains on which the client will perform DNS lookups, and the order in which it will perform those lookups, is as follows:

1. The domain portion, if specified, of the dialed **Conference alias or URI**.
2. The **serverAddress**, if specified, in the client's application settings file (**settings.js**). This address is not configured in the default desktop client provided by Pexip, but an address could have been configured by using the Infinity Connect desktop client toolkit files to customize the client prior to installation.
3. The **Connection server address**, if specified by the user, in the client **Settings** page.
4. The **Registration server address**, if specified by the user, in the client **Settings** page. This address can either have been explicitly specified, or it may have been derived from the domain portion of the user name to be registered.

Note that in many environments, some of these addresses, when used, will often refer to the same domain.

For each domain, the client will first perform an SRV lookup on **_pexapp._tcp.<domain>**. If the SRV lookup fails, or the client fails to contact any of the hosts in the returned SRV records, it will then perform a DNS A-record lookup for that same domain. If that A-record lookup is successful, it will attempt to connect to port 443 on the IP address returned from the lookup. If the client still fails to connect, it will move on to the next domain as specified in the list above. (The only exception is option 1, the dialed **Conference alias or URI**, where the client will perform an SRV lookup only.)

If multiple records are returned by an SRV lookup on **_pexapp._tcp.<domain>**, the client will attempt to contact each host in turn according to the priority of each returned record.

Infinity Connect Mobile client

The Infinity Connect Mobile client will perform a single SRV lookup on **_pexapp._tcp.<domain>**, where **<domain>** is determined as follows:

- **Android client**: uses the **Connection server address** if specified, otherwise it uses the domain portion of the dialed conference address.
- **iOS client**: uses the domain portion of the dialed conference address.

The client currently supports a single SRV record per domain. If multiple SRV records are returned by the SRV lookup on **_pexapp._tcp.<domain>**, the client will attempt to contact the first host in the list, which may or may not be the preferred host. If this attempt fails, no further attempts will be made to contact other hosts on the list.

If the Infinity Connect Mobile client cannot locate the host (i.e. reverse proxy or Conferencing Node) through DNS SRV discovery because either:

- the SRV lookup on **_pexapp._tcp.<domain>** does not return any records, or
- the client cannot contact the first host on the list that is returned in the SRV lookup

it will fall back to performing a DNS A-record lookup for the domain in question. If successful, it will attempt to connect to port 443 on the IP address returned from this A-record lookup.

Example

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

```
_pexapp._tcp.example.com. 86400 IN SRV 10 100 443 proxy1.example.com.
_pexapp._tcp.example.com. 86400 IN SRV 20 100 443 proxy2.example.com.
```

These point to the DNS A-records **proxy1.example.com**, port 443 (HTTPS), with a priority of 10 and a weight of 100, and **proxy2.example.com**, port 443, with a relatively lower priority of 20 and a weight of 100.

- This tells the Infinity Connect desktop client to initially send its HTTP requests to host **proxy1.example.com** (our primary reverse proxy server) on TCP port 443. The desktop client will also try to use host **proxy2.example.com** (our fallback server) if it cannot contact proxy1.
- The Infinity Connect Mobile client will send its HTTP requests either to **proxy1.example.com** or to **proxy2.example.com**, depending on the order of the returned SRV records. If it fails to contact the first host, it will not attempt to contact the second host address.

The connection logic in this example is explained in more detail below for each client. (Note that this section describes the operation of version 2.1 of the Infinity Connect desktop client; earlier versions of the desktop client operate in the same way as the Infinity Connect Mobile client.)

Infinity Connect desktop client

In this example, when a user attempts to access meet.alice@example.com, the Infinity Connect desktop client will attempt an SRV lookup on **_pexapp._tcp.example.com**:

- If the SRV lookup succeeds, it will return the records shown above, and the Infinity Connect desktop client will attempt to contact **proxy1.example.com** (the record with the highest priority) on TCP port 443.

  If it cannot contact **proxy1.example.com** it will next try to contact **proxy2.example.com**.
- If it fails to contact either host, or the SRV lookup fails, and neither a **serverAddress**, **Connection server address** nor a **Registration server address** have been specified, the desktop client will report that it has failed to contact a server.
- If any of the **serverAddress**, **Connection server address** or a **Registration server address** have been specified, and are for a different domain to that of the dialed alias (example.com in this case) the Infinity Connect desktop client will perform SRV lookups on those other domains, and attempt to contact the hosts returned in those lookups. For example, if the **Connection server address** is **localserver.example.com** then it will perform an SRV lookup on **_pexapp._tcp.localserver.example.com**.
- If each subsequent SRV lookup fails, or the returned hosts in those lookups cannot be contacted, the Infinity Connect desktop client will also attempt to connect directly to that domain, for example to **http://localserver.example.com:443** (via DNS A-records for localserver.example.com).

Infinity Connect Mobile client

In this example, when a user attempts to access meet.alice@example.com, the Infinity Connect Mobile client will attempt an SRV lookup on **_pexapp._tcp.example.com**:

- If the SRV lookup succeeds, it will return the records shown above, and the Infinity Connect Mobile client will attempt to contact the first host in the returned list on TCP port 443. Note that the addresses are returned in an arbitrary order and thus the first host may be either **proxy1.example.com** or **proxy2.example.com**.
- If the SRV lookup fails, or it fails to contact the first host on the returned list, the Infinity Connect Mobile client will attempt to connect to **http://example.com:443** (via DNS A-records for example.com).

(Note that for the Android client, this example assumes that a **Connection server address** is not configured on the client. If a connection server address is specified, it would be used instead of the domain portion of the dialed conference address i.e. example.com in this case.)

Using a reverse proxy and TURN server with Infinity Connect

In Pexip Infinity deployments, all Pexip Infinity Connect clients use HTTPS for the call signaling connections towards Conferencing Nodes.

However, with some Pexip deployments, these clients are not able to communicate directly with Pexip Conferencing Nodes, for example in on-prem deployments where the Pexip platform is located on an internal, enterprise LAN network while the clients are located in public networks on the Internet. In these cases it is common to deploy a reverse proxy application in the environment. This is an application which can proxy HTTP and HTTPS traffic from an externally-located client to a web service application located on the internal network — in our case a Pexip Conferencing Node. A reverse proxy can also be referred to as a load balancer.

In addition to providing HTTP/HTTPS connectivity between external Pexip clients and internal Conferencing Nodes, a reverse proxy can also be used for hosting customized Infinity Connect Web App content.

In deployments such as the ones described above, the reverse proxy provides for HTTPS call signaling connectivity between Infinity Connect WebRTC clients (Chrome, Firefox and Opera browsers and the desktop client) and Conferencing Nodes. However, to ensure audio/video/presentation connectivity between the two, a TURN server is also required.

A TURN server is a media relay/proxy which allows peers to exchange UDP or TCP media traffic whenever one or both parties are behind NAT. When Conferencing Nodes are deployed behind NAT, these nodes will instruct the WebRTC client to send its media packets to the TURN server, which will forward (relay) the packets to the Conferencing Nodes. Since this TURN server is normally located outside of the enterprise firewall, the Conferencing Node will constantly send media packets to this TURN server to "punch holes" in the firewall, allowing this TURN server to relay media packets back to the Conferencing Node, as the firewall will classify this as return traffic.

Pexip's Infinity Connect WebRTC clients (the desktop client; Web App for Chrome, Firefox and Opera; and mobile clients for iOS and Android) use ICE (Interactive Connectivity Establishment) to negotiate optimal media paths with Conferencing Nodes. Microsoft Lync clients use a similar ICE mechanism, which means that Pexip can use TURN for all of these client types.

Note that Infinity Connect clients on Internet Explorer, Edge, and Safari browsers use the RTMP protocol, rather than WebRTC. While RTMP clients can connect to Conferencing Nodes via the reverse proxy, they cannot establish audio/video paths to Pexip Infinity via a TURN server. To establish audio/video media connectivity, RTMP clients need a direct TCP connection to a Conferencing Node.

Depending on the network topology, the reverse proxy can be deployed with one or two network interfaces in various configurations:

- Single NIC, public address
- Dual NIC, private and public addresses

In deployments with more than one Conferencing Node, the reverse proxy can load-balance HTTPS traffic between all Conferencing Nodes using a round-robin algorithm. A reverse proxy can also provide an authentication layer between Infinity Connect clients and Conferencing Nodes, for instance through an Active Directory or similar LDAP backend.

For more information about using a reverse proxy, see **Pexip Reverse Proxy and TURN Server Deployment Guide**.