iMeet Provided by POWWOWNOW | Deployment Guide

Release 4.0

May 23, 2016

Table of Contents

Introduction

The iMeet Deployment Guide is intended for use by IT staff during the planning and execution of an iMeet product deployment. This document covers the options at all points in the deployment of all software and Internet based services related to the product.

It contains the following sections:

- About iMeet – a brief introduction to iMeet, the iMeet Cloud Controls administrative interface, iMeet desktop tools, and user roles.
- Planning worksheets – Two worksheets to assist you planning and discussing your implementation with PGi solutions architects.
- Network considerations – domain whitelisting, required ports, proxy server considerations, and bandwidth estimation metrics.
- System requirements – for using iMeet on the desktop and iMeet mobile apps.
- Deployment considerations – the differences between managed and unmanaged deployments.
- iMeet mobile apps – how to install the iMeet apps for iPad, iPhone, and Android smartphones.
- Support – how to contact the Powwownow support team for assistance from within your meeting, by phone or by email.

Intended audience

This document is intended for IT and network personnel. It is not an end user document.

Version information

Information in this guide is accurate for:

- iMeet 4.1 (meeting rooms)
- iMeet 4.0 desktop app (Mac and Windows)
- iMeet for Android 3.8
- iMeet for iOS 3.8 (includes Apple Watch integration)

What's new in this guide

This version updates the previous version of the *iMeet 3.7 Deployment Guide* released in October 2015. It includes the following product changes and additional implementation details.

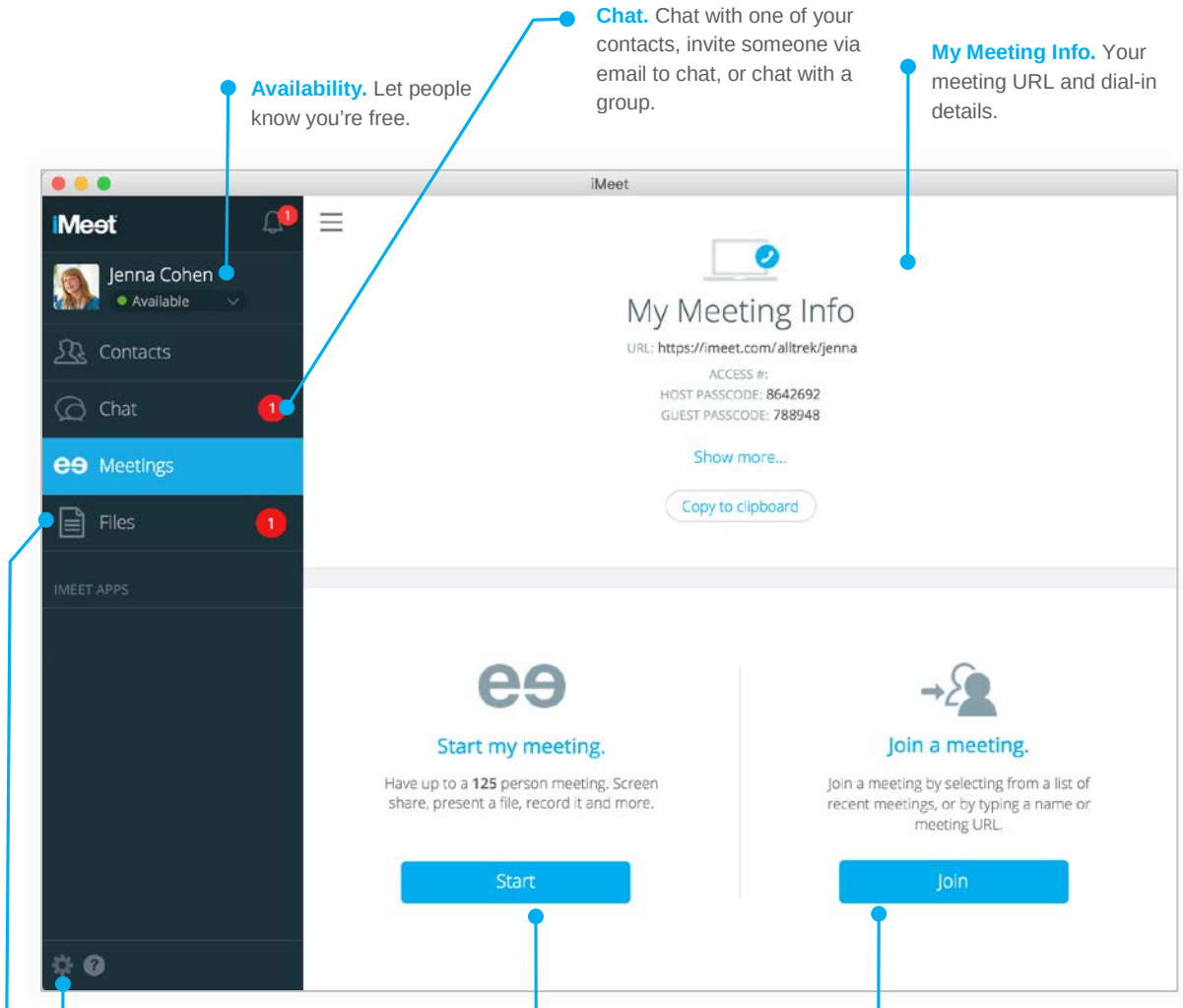
- The iMeet app for Mac and Windows has been redesigned, with a more "open" user interface that is easier to navigate and additional features.
  - The iMeet app is no longer available to unregistered guests. First-time users can easily register from the app.
  - Registered users can add iMeet contacts and join others' iMeet meetings, chat, voice and video call other contacts, and manage a profile (including a profile picture).
- Network considerations have been updated:
  - iMeet Chat requires WebSocket connections (WSS and XMPP protocols) over port 443.
  - Added bandwidth estimates for the new Video Call feature.
- System requirements have been updated:
  - iMeet supports Windows 10 and **REV2** the Microsoft Edge browser.
  - Minimum RAM requirement is 2 GB.
  - Removed the statement about Microsoft Surface support. iMeet, the iMeet app for Windows, and the iMeet Toolbar for Outlook can be used on any Microsoft Surface device that is running a supported version of Windows.
- Installation directories have changed for both Mac and Windows.
  - Mac: the application is located in ~/Applications/iMeet/; the uninstaller is located in ~/iMeet/.
  - Windows: the application and its uninstaller are located in %USERPROFILE\iMeet.

About iMeet

iMeet is a Flash-based browser client used by all participants in the meeting, regardless of role. This is the primary meeting interface for all users. Meeting hosts and guests can host or attend an iMeet meeting from any web browser. For the best meeting experience and to use HD audio over VoIP, they must install the iMeet app for Mac and Windows.

iMeet for Windows and Mac

For meeting hosts and registered users. The iMeet app makes it easy to host or join an online meeting, manage contacts, manage your file cabinet, chat, set availability, and update your profile. When set to launch at startup, the iMeet app monitors a meeting room for visitors.

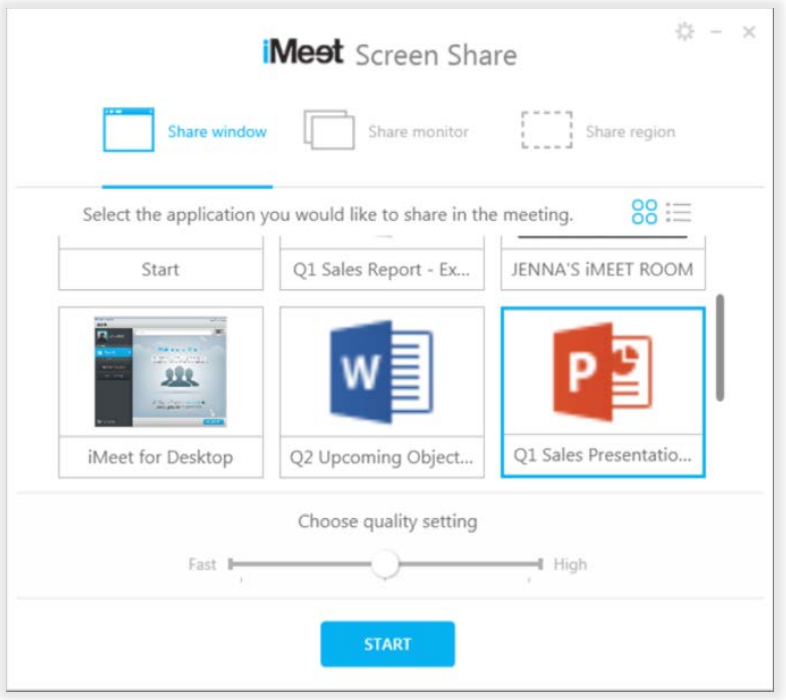


Guests can *register* with iMeet by providing their email address and selecting a password. **Registered users** can add iMeet contacts and join others' iMeet meetings, join recently visited meetings, chat, voice and video call, and manage a profile (including a profile picture).

Screen Share

Screen Share is included when you install the iMeet app. This allows hosts and guests to share an application, a region, or their entire screen with the meeting.

When a host selects SHARE ► SHARE MY SCREEN in the meeting, Screen Share is launched. If Screen Share is not found, iMeet prompts the host to install it.



File Cabinet

Every iMeet room includes a cloud-based file cabinet. Meeting hosts can access and present files and videos right from the room's file cabinet, across any device and pass control to a meeting guest. Hosts can also give guests permission to download files from the FILES tab in the room.

Hosts can upload a file while in iMeet, from the iMeet desktop app, or email files to YourRoomName@iMeetFiles.com.

Storage

Hosts can upload files up to 200 MB each. The total file storage varies by iMeet license; it can be 250 MB, 1 GB, or 25 GB.

Supported file formats

iMeet supports the following file types. Upon upload, the iMeet file cabinet converts them into slide presentations for in-meeting viewing.

Type of Document	File Type	File name Extensions
Image	GIF	.gif
	JPEG	.jpg, .jpeg
	PNG	.png
	TIF/TIFF	.tif, .tiff
	JPEG2000	.jp2
	Windows bitmap	.bmp
CSV	Comma Separated Values	.csv (DOS or UNIX)
Microsoft Office Documents	Microsoft Word	.doc, .docx
	Microsoft Excel (workbooks)	.xls, .xlsx
	Microsoft PowerPoint	.ppt, .pptx
Drawing	Adobe Acrobat PDF	.pdf
	Adobe PostScript	.ps
	Encapsulated PostScript	.eps
Text Documents	Rich Text	.rtf
	ASCII Text	.txt
Open Office v3	Open Office Doc	.odt
Videos	MP4	.mp4
	FLV	.flv

Planning worksheets

This section includes two worksheets to assist in planning your implementation.

Your organization and environment

Please have this information available when discussing your implementation with PGi solutions architects.

Item	Summary
Organizational information	
Executive sponsor(s)	Name(s) and contact information
Organization contacts for rollout	Name(s) and contact information
Rollout plan	All users at once or structured rollout with defined phases? If structured, provide target user groups/regions in order of priority or scheduling. 1. 2. 3. 4.
Target date	
Current conferencing services	Which web conferencing or video conferencing services does your organization currently use? (This will assist with transition planning.)

Item	Summary
Tell us about your environment	
Traffic distribution	Is your network primarily in one country or are your users distributed across multiple countries/regions? Estimate the % of total traffic in each country (for example, 100% US/Canada or 50% US and 50% Germany). 1. 2. 3. 4.
User locations	Will your users host/attend meetings while onsite (on your corporate networks), remotely via VPN, or remotely via home office or third-party networks (Wi-Fi)? Estimate the % of users for each scenario.
Network routing	Describe routing within and between campus/office locations. For example, do you route all European users through a hub in North America?
Proxy servers and security	Describe proxies used or other security policies. Do you use packet inspection?
Video room systems	List any video room systems you would like to integrate with iMeet (Cisco, Polycom, Lifesize, etc.). H.323 or SIP access?

Item	Summary
End user workstations and devices	
Operating systems	Which desktop operating systems do you support? (Mac OS X, Windows 7, 8.1, 10)
Browser support	Which browsers do you support? Are there any restrictions, for example, you may support only Internet Explorer 9 on workstations.
Mobile devices	Mobile devices used (iPad, Android smartphones, iPhone, Blackberry, etc.) Are you a BYOD environment? Does your organization use a mobile device management system like AirWatch? If so, which one?
How do you plan to use iMeet?	
Typical meeting size (participants)	
Webcam streaming	iMeet works with most built-in, laptop webcams and external webcams. Does your organization have a preferred list of webcams (internal, Logitech, Microsoft, Cisco, etc.)?

Item	Summary
Screen sharing	
Video meeting rooms	
Town halls	iMeet can accommodate up to 125 participants in a room. If a primary use is for large-capacity meetings, let us know and we'll work with you to make them go smoothly.

Implementation checklist

This checklist summarizes factors consider when preparing to deploy iMeet and its tools. Click the page number (if available) to go to a detailed description.

☑	Item	Summary	Page
Network setup required to support iMeet			
	Required Domains	Your network must allow communications – or “whitelist” – specific domains and all child subdomains. Allow HTTP and HTTPS protocols over ports 80 and 443 for all required domains.	16
	Proxy Server	Client must be able to connect to all iMeet servers via TCP port 443 either directly or through web proxy. Network administrators may need to be aware of certain considerations since iMeet uses streaming video, audio, webcam, etc.	19
	Bandwidth Requirements	Metrics for estimating usage based on typical meeting activities like Screen Share, file sharing, streaming videos, and sharing webcam.	20
System requirements to support iMeet, iMeet Sales Accelerator, and the meeting tools			
	Operating Systems	Windows 7 through 10 Mac OS X 10.9 or later	21
	Browser Requirements	Microsoft Edge (Windows 10) Internet Explorer 8, 9, 10, or 11 Mozilla Firefox 25 or later Google Chrome 16 or later Apple Safari 6.2 or later (OS X only)	21
	Other	Flash Player 19 or later .NET 4.0.3 required for Screen Share .NET 3.5 required for iMeet toolbar for Outlook	21
	iMeet Mobile Apps	System requirements for iOS (iPhone, iPad), Android, and BlackBerry	22

☑	Item	Summary	Page
Which features and tools will you offer to your users?			
	iMeet app for Mac and Windows	Required for HD audio over VoIP.	5
	iMeet for Android	An app for scheduling, joining, and hosting a meeting from an Android smartphone.	29
	iMeet for BlackBerry	An app for scheduling, joining, and hosting a meeting from a BlackBerry device.	
	iMeet for iOS	An app for scheduling, joining, and hosting a meeting from an iPhone or iPad device.	28
How will you deploy iMeet and iMeet tools (managed and unmanaged deployments)?			
	Unmanaged Deployment	Available for iMeet for Mac and Windows, and all mobile apps. Allow your end users (hosts) to download and install iMeet on their own Mac and Windows machines. Mobile apps are available in the relevant app stores.	25
	Managed Deployment	Available for Windows. Push the iMeet app to your users' Windows machines via the iMeet Installer in "silent" mode. You can choose which components to install: iMeet app (includes Screen Share) and the iMeet toolbar for Outlook.	27

Network considerations

Deployment of any Internet-based service will require consideration of impact to the network. iMeet is built using Adobe Flash and designed to minimize the impact to corporate networks.

The web meetings portion of the iMeet product consists of browser clients used by all participants in the meeting regardless of role. iMeet is designed to work in the vast majority of networking environments. However, there are elements to consider when deploying a solution such as iMeet.

Network traffic

All traffic between the iMeet client and iMeet servers requires outbound access via the TLS protocol on TCP port 443. Generally, this access is required for “imeet.powwownow.com” as well as all hostnames beneath the “imeet.powwownow.com” domain (that is, *.imeet.powwownow.com). Since iMeet was designed to be highly scalable, PWN cannot easily explicitly identify all server names that are used by iMeet. PWN is experienced in working with enterprise IT organizations to find reasonable ways to work with network security issues. Please contact PWN Sales if you anticipate having difficulties with iMeet connectivity due to unusually restrictive network security policies.

In general, iMeet is very firewall friendly and even works well with clients behind most enterprise web proxies. Please note that web proxies can introduce variable latency for streaming media such as iMeet’s VoIP audio, webcam, and video streaming. Networks that restrict RTMPS and/or Port 443 in different way may cause performance problems with the Web Camera. One common issue is that firewalls sometimes are set to down prioritize RTMPS and 443 streams.

Firewall transversal

iMeet encrypts all traffic between client and iMeet servers using TCP port 443. At any time, there may be numerous connections open between the iMeet client and the iMeet servers (e.g. Meeting servers, webcams, software telephone, etc.). Different underlying protocols may be negotiated on TCP port 443; however, these are all fundamentally TLS-encrypted connections. iMeet will prefer a pure TLA-encrypted socket over which iMeet negotiates the RTMP protocol as this is the most efficient means for iMeet to communicate on any network but this type of connection is only available if an encrypted socket connection is allowed by enterprise security infrastructure. Technically, the protocol leveraged by the iMeet client is RTMPS – yet RTMPS is actually a term that denotes a family of TCP network protocols, all of which use TLS encryption. If no enterprise firewall or web proxy has been deployed in an iMeet customer’s environment, such users should be able to enjoy the most optimized client-to-server communications.

If the iMeet client is protected from the public Internet via web proxies or the like – or very specific conditions that are specific to Adobe’s Flash player implementation (such as running iMeet on Google

Chrome on a PC) – iMeet will renegotiate the RTMP protocol over a series of HTTPS requests and responses; this is referred to as RTMPT over TLS but also considered an RTMPS variant. RTMPT over TLS is effectively HTTPS tunneling of the RTMP protocol. Like its pure socket TLS-encrypted counterpart, RTMPT over TLS uses TCP port 443 but instead of an asynchronous socket protocol, the protocol is a series of (synchronous) HTTPS requests / responses which lasts the lifetime of each logical client-to-server connection. Tunneling (i.e. RTMPT over TLS) adds overhead and also delays a server-to-client message until the client has made its next request. Thus while RTMPT over TLS will functionally work even for media streams in environments secured by firewalls, it is not nearly as efficient as the TLS encrypted socket and is also subject to delays due to resource bottlenecks at the enterprise web proxy.

In the case of the non-Flash iPhone implementation, iMeet attempts to negotiate an encrypted socket of a different variety where we pass native messages without an RTMP wrapper; however, this traffic is also negotiated on TCP port 443 and it has no solution that can navigate through web proxies.

If the iMeet client is protected by web proxy and/or enterprise firewall technology that by default blocks HTTPS or any other TLS encrypted connections, a special consideration must be made for iMeet traffic on that enterprise network. PGi is willing and able to work with customer network/security IT departments in order to yield a working solution, but some firewall/ACL exceptions will be necessary; additionally iMeet will put a heavier load on web proxies than typical traffic since the nature of iMeet is streaming media that might otherwise be blocked.

In addition to streaming media traffic, iMeet also uses standard HTTPS connectivity between the client and server for more traditional web requests such as static images assets, document.

Finally, in some cases, iMeet may leverage non-encrypted web traffic (normally on TCP port 80) for third party links that the iMeet user has provided; YouTube, Flickr assets are good examples of such traffic. Standard web proxy and firewall access is expected for this functionality. iMeet does not proxy such traffic between the iMeet client and YouTube or Flickr; these connections are made directly between the client and third party server.

Domain whitelisting

Your network must allow communications to the domains and all child subdomains identified in this section.

- For all whitelisted domains in this section, allow HTTP, HTTPS, RTMP, RTMPE, RTMPS and RTMPT protocols over ports 80 and 443.

  This is required for all meeting tools and mobile apps.
- The softphone requires SIP over ports 5060, 5070 and 10000-65535.
- The chat feature requires WebSocket connections (WSS and XMPP) over port 443.
- For the best user experience, create an additional policy accepting pop-ups from these domains.
- To ensure your network's SSL certificate validation (CRL checks) work, allow traffic over port 80 to cert providers.

iMeet domains

Allow communications to the following domains and all child subdomains. Ensure that these protocols are enabled on the domains and ports listed below: HTTP, HTTPS, RTMP, RTMPE, RTMPS, and RTMPT.

Domain	Ports	Description
*.imeet.powwownow.com	80, 443	iMeet main site
slcsp.imeet.com	5060, 5070 (UDP)	Required for softphone (meeting audio over Internet connection). Traffic flows as RTP over port 4000.
*.pgiconnect.com	80, 443 5060, 5070 (UDP)	Required for softphone (meeting audio over Internet connection). Traffic flows as RTP over port 4000.

Third party domains (iMeet)

Communications must be enabled with the following domains and all sub-domains for iMeet to function properly.

Domain	Ports	Description
*.akamaiedge.net	80, 443	Asset hosting for iMeet
*.akamaihd.com	80, 443	Asset hosting for iMeet
*.akamaitechnologies.com	80, 443	Asset hosting for iMeet
*.amazonaws.com	80, 443	Cloud-based file cabinet
*.evernote.com	80, 443	iMeet Notes integration to Evernote
*.google.com	80, 443	Supporting domain serving content
*.googleapis.com	80, 443	Display fonts
*.speedtest.net	80, 443	iMeet Systems Test page
*.wunderground.com	80, 443	Display weather and time based on user's location
*.ytimg.com	80, 443	YouTube integration

Optional domains (iMeet)

iMeet lets users link to their social media and cloud app accounts. If you would like to offer this to your users, allow communications to the following domains.

Domain	Ports	Description
connect.facebook.net	443	Facebook integration
*.fbcdn.net	80, 443	Facebook integration
*.facebook.com	80, 443	Profile link via cube
Flickr.com	80, 443	Profile link via cube
Linkedin.com	80, 443	Profile link via cube
*.twimg.com	80, 443	Twitter integration (hosted images)
*.twitter.com	80, 443	Profile link via cube

Optional usage tracking domains (iMeet)

The following domains are used for usage tracking and analytics.

Domain	Ports	Description
c.compete.com	80, 443	Analytics
*.eloqua.com	80, 443	Eloqua marketing analytics tracking
*.en25.com	80, 443	Eloqua marketing analytics tracking
*.google-analytics.com	80, 443	Google analytics
*.googletagmanager.com	80, 443	Google analytics
*.hs-analytics.net	80, 443	Analytics
px.spiceworks.com	80, 443	Analytics

Certification authorities

Most organizations' security policies require HTTPS CRL (Certificate Revocation List) validation. Double-check that your network allows communications to port 80 for the following certification authorities:

- *.digicert.com
- *.netsolssl.com

Proxy server considerations

iMeet is designed to be compatible with almost any network environment, including those with a proxy server in place. However, Network Administrator may need to be aware of certain considerations since iMeet uses streaming video, audio, webcam, etc.

Although iMeet is designed to work in proxy environments, the best case scenario for performance is to allow iMeet to bypass the proxy entirely (using the domains listed elsewhere in this guide) or at least not require it to tunnel via HTTPS. In the event, that this is not possible, iMeet negotiates the proxy environment slightly differently depending upon the operating system.

Windows

When Screen Share is initiated on a Windows machine, iMeet runs a discovery process to find the proxy settings. Depending upon how the proxy is configured, this can take up to 30 seconds. iMeet first queries the Internet Explorer settings for the proxy configuration, which could be a proxy address/URL in the IE settings or a PAC file. If the proxy address is set in IE, iMeet honors this. If a PAC file address is returned, iMeet fetches and parses the PAC file and honor the proxy address settings contained in it. If IE configuration settings are not detected, iMeet attempts a WPAD query (DHCP, then DNS). Using both methods is slower, but allows for successful proxy navigation in most environments.

iMeet follows the configuration method recommended by Microsoft. iMeet mainly acts like a web browser for this purpose. Whitelisting domains and allowing streaming through proxy improves the speed.

Mac OS

In the Mac OS, the proxy configuration can be set in system preferences. When Screen Share is initiated, iMeet sends a query to the host machine to see which protocol is set and follow the settings there. In order, iMeet checks 1) auto proxy discovery, 2) automatic proxy configuration, and 3) Secure web proxy (https). A unique aspect of the Mac OS/X is that once the user sets any of these settings the OS does the work. iMeet Screen Share queries for each in the order listed and use the data that resulted from the OS's actions, meaning that it gets either a PAC file URL or an explicit proxy setting.

In either operating system, the customer system should be configured so that the browser knows how proxy is set up. To make the Screen Share launch process faster, iMeet checks for IE configuration, no matter what browser is being used. If no IE configuration is available, iMeet falls back to WPAD. Timing depends upon network speed & complexity (WPAD.dat complexity & rules). Having IE settings available makes Screen Share start up faster.

iMeet runs this proxy detect process when Screen Share is started, and then remembers it for the length of that Screen Share session. In the event that Screen Share is stopped and restarted, iMeet runs the check again.

Registry proxy is not currently supported

There is another proxy method where the Windows system administrator can put proxy info in the machines registry. This method is not suggested by Microsoft and not currently supported by iMeet.

Bandwidth considerations

iMeet is a cloud-based solution and requires a minimum amount of bandwidth in order to run successfully and deliver the best-quality audio and video for web collaboration. iMeet webcam streaming, in particular, is designed to maintain a minimum performance quality rather than hard-cap bandwidth usage.

The approximate bandwidth required to run iMeet with a webcam is 35-55 kbps per user, add in a softphone connection and it goes up to 55-75 kbps per user. Through optimization, iMeet can run between 6 and 15 webcams simultaneously on 125 kbps of dedicated bandwidth (for webcam only).

Approximate bandwidth usage for up and downstream functions are as follows. Total bandwidth required would be 450-500 kbps downstream and 110-200 kbps upstream per user.

Broadcasting (uplink)		**Receiving (downlink)**	
Webcam in normal cube	35 kbps	the iMeet room	225 kbps
Webcam in spotlight cube	55 kbps	Webcams 2- 15	125 kbps
VoIP (Softphone)	32 kbps	VoIP (Softphone)	25 kbps
Screen Sharing	10-15 kbps	Screen Sharing	1 kbps

Video Call bandwidth usage

iMeet users can chat, voice call, and video call any iMeet user (host or registered user) from their contact details. Video calling allows users to communicate one-on-one, outside the meeting room, using iMeet's high-definition audio/video.

Approximate bandwidth usage is 0.5 Mbps upstream and downstream. 2 Mbps available bandwidth is optimal.

System requirements

To install and run the various components of the iMeet system, your computer must meet the following hardware and software requirements.

System Component	iMeet	iMeet Messenger	iMeet Toolbar
Processor	Intel or AMD 1.8Ghz or higher, recommend 2.3Ghz or higher.	Intel or AMD 1.8Ghz or higher, recommend 2.3Ghz or higher.	Intel or AMD 1.8Ghz or higher, recommend 2.3Ghz or higher.
RAM	At least 2GB	At least 2GB	At least 2GB
Operating System	Windows 7 or later Mac OS X 10.9 or later	Windows 7 or later Mac OS X 10.9 or later	Windows 7 or later
Browser	Microsoft Edge (Windows 10) Internet Explorer 8, 9, 10, or 11 Mozilla Firefox 25 or later Google Chrome 16 or later Apple Safari 6.2 or later (OS X only)		
Flash Player	19 or later	19 or later	19 or later
Other	Client must be able to connect to all iMeet servers via TCP port 443 either directly or through web proxy. 3rd party integration might be limited due to local/enterprise security policy restrictions to other sites such as LinkedIn, YouTube, Evernote, Flickr, etc.	For Screen Share: .NET 4.0.3 or later	.NET 3.5 framework Outlook 2007, 2010, and 2013

About Adobe Flash Player

Adobe recommends that all Flash Player users upgrade to the most recent version of the player to take advantage of security updates. Hosts and guests might be prompted to upgrade when starting or joining an iMeet meeting.

System requirements for mobile apps

The following table summarizes system requirements for the iMeet mobile apps. All apps require an active data connection, either through the wireless carrier's 3G/4G/LTE network or via Wi-Fi.

Mobile App	OS Versions	Supported Devices
iMeet for Android	Android platform versions 4.0.3 through 6.0 (Ice Cream Sandwich, Jelly Bean, KitKat, Lollipop, and Marshmallow).	Android smartphones only. Android tablets are not supported.
iMeet for iOS (iPad)	iOS 8 and iOS 9	iPad and iPad Mini, including those with Retina display
iMeet for iOS (iPhone)	iOS 8 and iOS 9	iPhone devices running iOS 8 and iOS 9
iMeet for Apple Watch	iOS 8.2 or later	All Apple Watch devices

Deployment considerations

Meeting hosts – your users – can host or attend an iMeet meeting from any web browser. To be able to Screen Share and use HD audio over their computer mic and speakers, they must install the iMeet app for Windows or Mac.

It includes:

- **iMeet desktop application** – lets Windows and Mac users host or join an online meeting, manage contacts, manage files in the cloud-based file cabinet, chat with contacts, voice and video call their contacts, set availability, and update their profiles. It also monitors the user's iMeet room, alerting the host when someone joins.
- **Screen Share** – launched in the meeting; required if the host wants to share an application or the entire screen with meeting participants.

  Screen Share is downloaded and installed after the user signs in to the desktop app.

Managed v. unmanaged

There are two options for installing iMeet desktop tools: *managed* and *unmanaged*.

In a *managed deployment,* IT administrators push deployments to their users' Windows machines, using the installer's silent mode. This is explained in the section, Managed deployment (Windows), later in this guide.

In an *unmanaged deployment,* a company allows its end users (hosts) to download and install iMeet on their Windows and Mac computers. End users will see the iMeet installer. For unmanaged deployments, companies can either point their users to the installer URL or host the installation file on their own Web page.

Managed deployments (Windows)

The iMeet Windows installer from https://imeet.powwownow.com/tools includes a "silent" mode that can be used for managed deployments.

NOTE: Contact your Sales Engineer for assistance with iMeet installations in a Microsoft SCCM environment.

Installation details

Windows

If Microsoft Outlook is detected, the iMeet Toolbar is installed. %USERPROFILE% represents c:\Users\<username>; %APPDATA% represents c:\Users\<username>\AppData.

```
%USERPROFILE%\iMeet                                    : iMeet and uninstall utilities
%APPDATA%\Local\iMeet                                  : Application cookies and cache
%APPDATA%\Roaming\iMeet                                : Application storage and logs
```

The iMeet app uses Adobe AIR for installation; registry keys are determined by the AIR application.

Mac

On the Mac, files are installed under the user's home folder. **~** represents /Users/<username>.

```
~/Applications/                                        : iMeet and Screen Share apps
~/iMeet/                                               : iMeet uninstall utilities
~/Library/Application Support/iMeet/                   : Application storage and logs
~/Library/Logs/DiagnosticReports/                      : Crash reports
```

Administration privileges

Installation of the iMeet desktop app does not require administrative rights on the PC.

Auto-update

By default, the iMeet app automatically checks for updates – on startup and one time per day when running – to ensure users are on the latest version. Users can dismiss the message and skip the update.

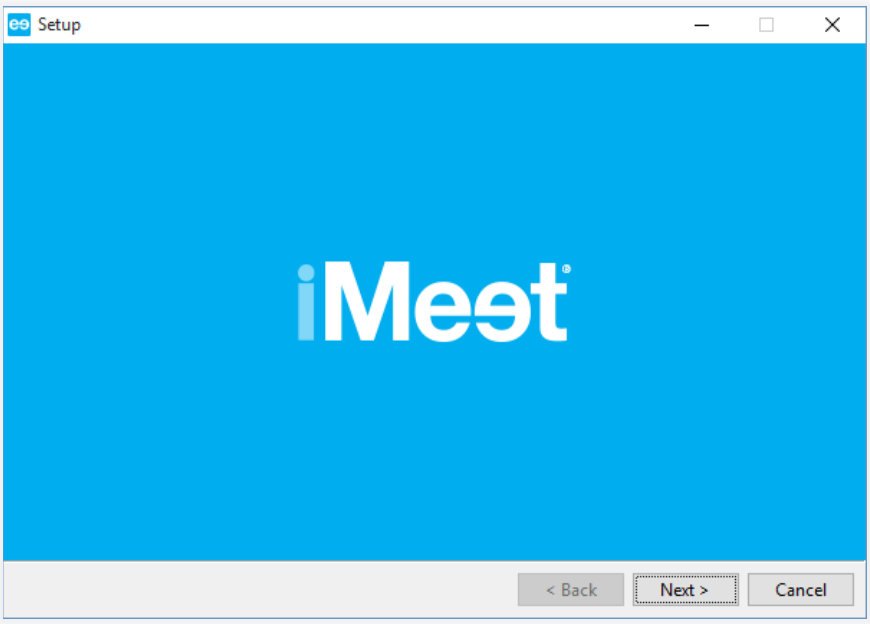
VoIP Audio

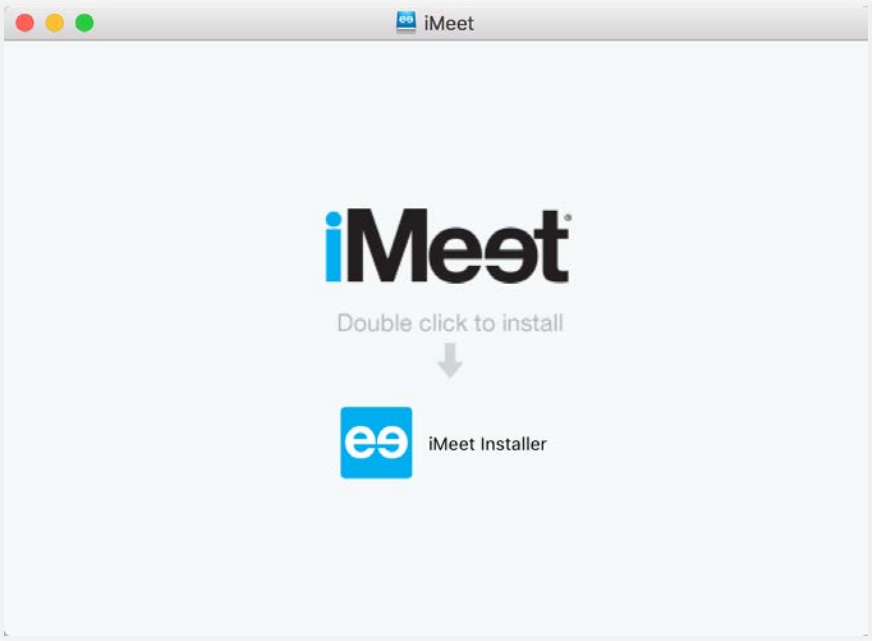
Use the iMeet desktop app to join all meetings and ensure the best audio quality. Select **Use My Computer**, for the best VoIP experience. Headphones are required.

Unmanaged deployment

An *unmanaged deployment* is where a company allows its end users (hosts) to download and install the iMeet toolset on their own Mac and Windows machines.

For an unmanaged deployment, point your users to https://imeet.powwownow.com/tools, where they can download and install iMeet for Mac or Windows.

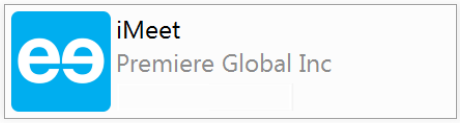




Uninstalling iMeet

Users are able to retain user data on the machine if they expect a reinstall at some point in the future.

Windows users can remove the iMeet tools – Screen Share and the iMeet app– via the Windows Control Panel. In the Uninstall or Change a Program section, find the iMeet entry and click Uninstall.



Mac users can use the uninstaller for the Mac called “uninstall” and it is located in the iMeet folder in the user’s home folder (~/iMeet/uninstall). This is the preferred way to uninstall the Mac app.

Managed deployment (Windows)

Windows installations only.

The Windows installer – iMeet_Tools_Setup.exe – includes iMeet for Windows and the Screen Share application. Download it from https://imeet.powwownow.com/tools and use it for a managed deployment.

NOTE: After iMeet is installed, Screen Share is automatically downloaded and installed in the background.

Installer options

To install in silent mode, use the following command line.

```
iMeet_Tools_Setup.exe –-mode unattended
```

By default, the installer will install iMeet, iMeet Screen Share, and the iMeet Outlook Toolbar on your user's machine without any user interaction ("silent mode").

Uninstaller options

The iMeet uninstaller removes all desktop tools: the iMeet desktop app, Screen Share, and if present, the iMeet Toolbar for Outlook. The uninstaller is located in the directory:

```
%USERPROFILE%\iMeet\
```

To uninstall in silent mode, use the following command line.

```
uninstall.exe --mode unattended
```

By default, the installer removes all iMeet Tools components – the iMeet app, Screen Share, and the iMeet Toolbar.

iMeet mobile apps

iMeet for iOS

The iMeet app for iPhone and iPad (“iMeet iOS”) is available at no charge from the App Store or iTunes store (https://itunes.apple.com/us/app/imeet-mobile/id456757257?mt=8).

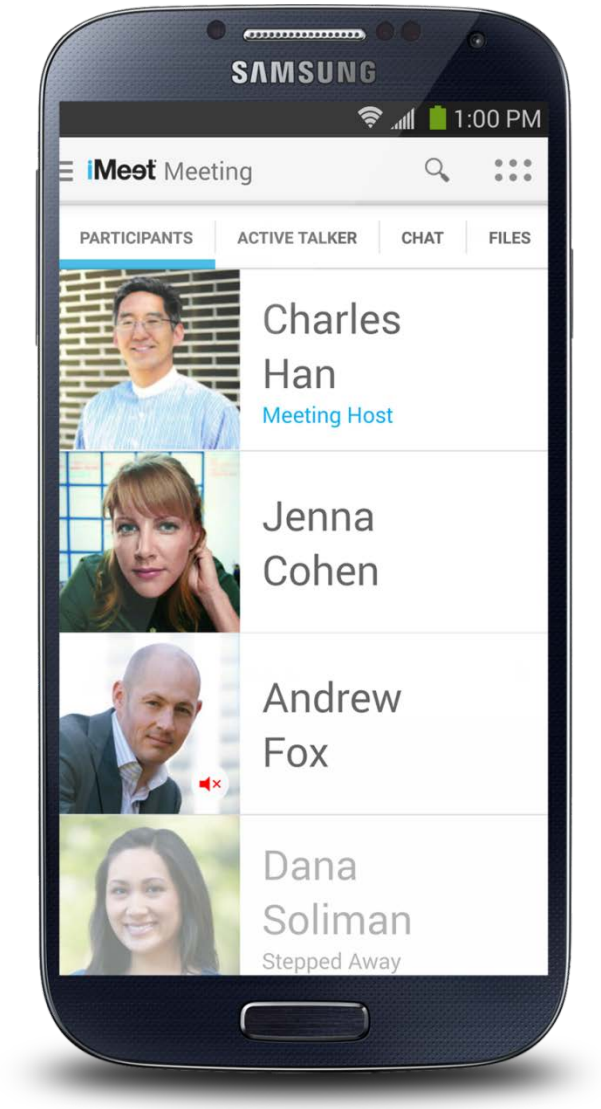
The iMeet app works on all Apple iPhone and iPad devices running iOS 8 and iOS 9, including those with Retina display. Apple Watch integration requires an iPhone device running iOS 8.2 or later.

NOTE: Non-iPad tablet users will be automatically redirected to the tablet site (tablet.imeet.powwownow.com/roomname) when they join an iMeet meeting via a tablet browser.

iMeet for Android

The iMeet app for Android phones (“iMeet Mobile”) is available at no charge from the Google Play store (https://play.google.com/store/apps/details?id=com.imeet&feature=search_result).

The iMeet app supports smartphones running Android platform versions 4.0.3 through 6.0 (Ice Cream Sandwich, Jelly Bean, KitKat, Lollipop, and Marshmallow).

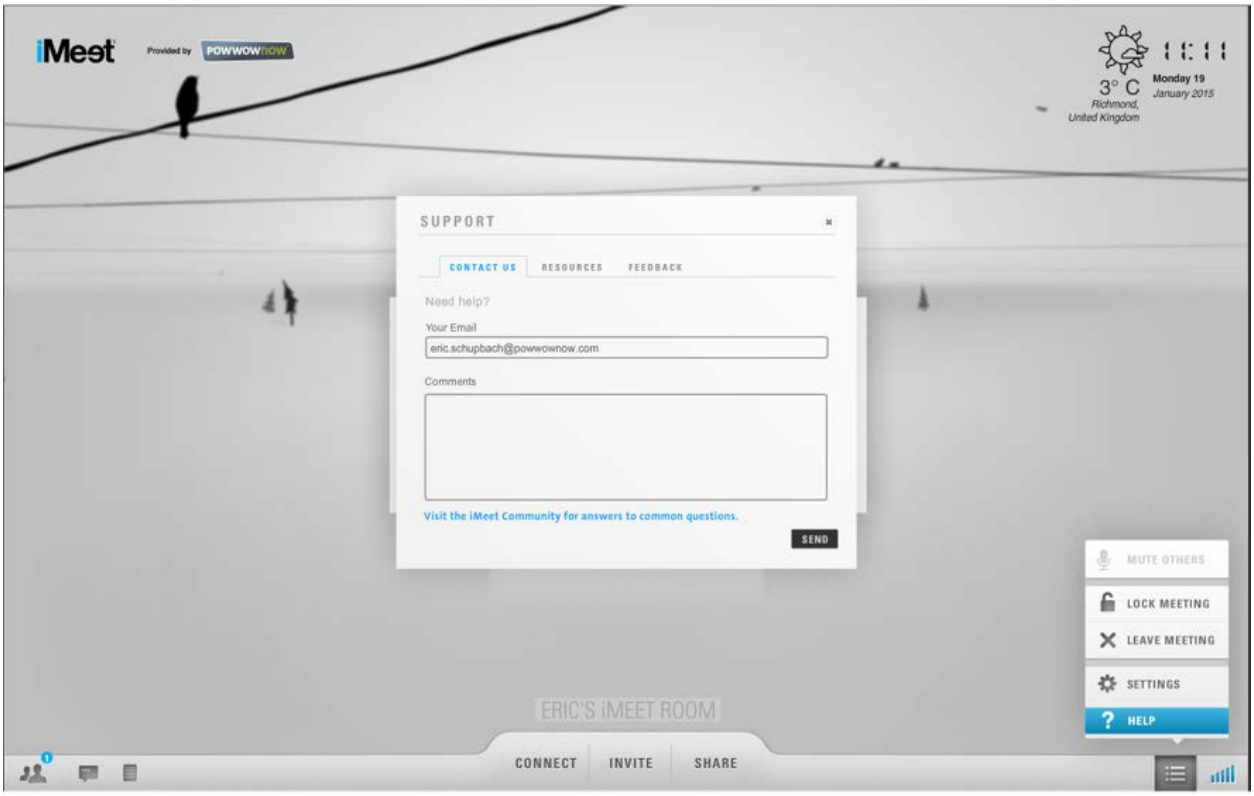


Support

For technical support on iMeet, issues can be reported in-room by selecting HELP on the iMeet controls menu (located in the lower right corner).

Then simply fill in the “Contact Us” form and click the Send button.

Not only does this button send us user’s comments on an issue but it also does a query in the background, sending the Powwownow support team vital technical information about the system on which the meeting is being held.



To contact the customer service team directly please either email or phone us.

iMeet support email address: support@powwownow.com

iMeet support phone number: 0203 398 1919