



IP Office Avaya Workplace Client Installation Notes

Release 12.1
Issue 20
February 2025

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Part 1: Workplace Clients	8
Chapter 1: Avaya Workplace Clients and IP Office	9
Operating system support	9
User licensing	10
Avaya Workplace Client Modes	11
Codec support	12
Supporting IPv6 extensions on IP Office	13
Chapter 2: Workplace Ports	15
Avaya Workplace Client Ports	15
Requirements for Avaya Workplace Client and Avaya Cloud Services	16
Requirements for Avaya Workplace Client and Equinox Client Meetings Online	16
Chapter 3: IP Office SIP Configuration for Avaya Workplace Client Support	18
IP Office Messaging Server Configuration	18
User Configuration	19
Creating an Avaya Workplace Client user	19
Avaya Workplace Client Emergency Number Dialing	20
IP Office User Settings for Avaya Workplace Client	21
IP Office Settings Files	22
Avaya Workplace Client NoUser Source Numbers	22
Chapter 4: Workplace Client Installation	24
Windows Workplace Client Installation	24
Windows Workplace Client Installation	24
Windows command line installation	25
Installation using a group policy	27
Installing macOS client software	28
Advanced installation	28
Installing Avaya Workplace Client on an iOS device	29
Installing Avaya Workplace Client on an Android device	29
Chapter 5: Initial Avaya Workplace Client configuration	31
Avaya Workplace Client Email Connection	31
Direct IP Office Avaya Workplace Client connection	32
Calendar Integration	33
Enabling exchange calendar support	33
Selecting the calendar to display	34
Chapter 6: Calendar Integration	35
Enabling exchange calendar support	35
Selecting the calendar to display	36
Chapter 7: Contact Integration	37

Contact Integration.....	37
Exchange Self-Avatar Support.....	37
Chapter 8: Workplace Shared Control Mode.....	39
Enabling shared control mode.....	39
Chapter 9: Simultaneous mode.....	41
Simultaneous Mode Devices.....	41
Simultaneous Mode Notes.....	41
Moving Calls Between Simultaneous Devices.....	42
Chapter 10: Avaya Workplace Client VDI Support.....	43
Virtual client limitations.....	44
Local PC client installation for VDI support.....	44
Installing the local VDI client.....	44
Enabling Chrome desktop mode.....	45
Disabling local notifications.....	45
Virtual desktop client installation for VDI support.....	46
Virtual desktop client installation.....	46
Virtual desktop client login.....	46
Setting the client for the call media.....	47
Chapter 11: Workplace Troubleshooting.....	48
Defaulting an Avaya Workplace Client.....	48
Emailing a bug report.....	49
Setting the Email Address.....	49
Part 2: Avaya Cloud Services.....	50
Chapter 12: Configuring Avaya Cloud Services support.....	51
Avaya Cloud Services support checklist.....	52
Verifying the company domain.....	52
Obtain the domain API Key and Key Secret.....	54
Enter the Avaya Cloud Services settings.....	55
Updating the Avaya Workplace clients.....	56
Chapter 13: Configuring Avaya Cloud Services synchronization.....	57
Avaya Cloud Services synchronization checklist.....	57
IP Office user configuration for Avaya Cloud Services.....	58
Adding the synchronization application.....	58
Enabling Avaya cloud services user synchronization.....	59
Enabling Avaya Cloud Services profile synchronization.....	60
Checking the Avaya Cloud Services Users.....	61
Using Avaya Cloud Services as the IP Office instant messaging server.....	61
Set the Avaya Cloud Services user policy.....	62
Chapter 14: Configuring SSO login support.....	64
SSO/Avaya Cloud authorization checklist.....	64
Enabling Avaya Cloud authorization.....	64
Sync the Avaya Cloud Authorization setting.....	65

Set the Avaya Cloud Services user policy.....	66
Chapter 15: Enabling Apple Push Notifications.....	67
Push notification routing.....	67
Push notification notes.....	69
Checklist for configuring push notification support.....	69
Checking the Avaya Cloud Services timezone.....	70
Adding the push notification application.....	71
Enabling Avaya Push Notification Services.....	71
Synchronizing the enable Apple Push Notifications setting.....	72
Synchronizing the Avaya Cloud Services API settings.....	73
Altering IP Office user and group settings for APNS.....	74
Updating the Avaya Workplace clients.....	74
Chapter 16: Supporting Spaces Calling.....	76
IP Office Components for Spaces Calling.....	77
Spaces Calling Limitations.....	77
Spaces Calling Chrome Extension Schematic.....	77
Spaces Calling Workplace Client Schematic.....	78
Spaces Calling Native Remote Worker.....	79
Spaces Calling Remote Worker Using an ASBCE.....	80
Spaces Calling Licensing.....	81
Checklist for configuring Spaces Calling with IP Office.....	81
Enabling Spaces Calling Support for the Customer Domain.....	82
Spaces Calling Profile Settings.....	83
Setting the Preferred Spaces Calling Clients.....	85
Installing the Spaces Calling Extension.....	86
Blank Calling Extension/Enabling Third-Party Cookies.....	87
Change the Spaces Calling Client.....	87
Getting the Chrome Extension Logs.....	88
Manually Adding a User Phone Number.....	88
Chapter 17: Manually configuring IP Office/Avaya Cloud Services details.....	90
Adding the IP Office system details.....	90
Manually Adding Individual Users.....	92
Manually Importing Multiple Users to Avaya Cloud Services.....	92
Part 3: Further Help.....	94
Chapter 18: The IP Office Settings Files.....	95
Workplace 46xxsettings.txt file settings.....	96
Sample 46xxspecials.txt file.....	98
User Agent spoofing.....	100
Changing the User Agent in Google Chrome.....	100
Changing the User Agent in Safari.....	101
Chapter 19: Additional Help and Documentation.....	102
Additional Manuals and User Guides.....	102

Getting Help..... 102

Finding an Avaya Business Partner..... 103

Additional IP Office resources..... 103

Training..... 104

Part 1: Workplace Clients

Chapter 1: Avaya Workplace Clients and IP Office

Avaya Workplace Client is a unified communications application that works on Windows, Android, macOS and iOS (iPhone and iPad) (see [Operating system support](#) on page 9).

- These notes cover installation of Avaya Workplace Client R3.33 or higher with IP Office R11.1.3 systems. See [Planning for and Administering Avaya Workplace Client for Android, iOS, Mac and Windows](#).
- If planning to support Avaya Workplace Client remote extensions, including IPv6 extensions, see [Deploying Remote IP Office SIP Phones with an ASBCE](#).

Related links

[Operating system support](#) on page 9

[User licensing](#) on page 10

[Avaya Workplace Client Modes](#) on page 11

[Codec support](#) on page 12

[Supporting IPv6 extensions on IP Office](#) on page 13

Operating system support

At the time of the release of IP Office R12.0, Avaya Workplace Client is supported with IP Office R12.0 on the following operation systems.

OS	Support Versions
iOS	iOS 12.x/14.x/16.x. IP Office support is for iPhone and iPad devices only. It does not include other iOS devices such as iPod Touch.
Android	Android 11.x/12.x/13.x.
Windows	Windows 10, Windows 11. Windows support is only on Pro and Enterprise versions.
macOS	macOS 12.x/13.x/14.x

This is based on Avaya Workplace Client v35. For later Avaya Workplace Client releases, refer to the product release notes for details of changes.

Related links

[Avaya Workplace Clients and IP Office](#) on page 9

User licensing

Use of Avaya Workplace Client is subject to the following entitlement requirements.

- **Vantage Phones** - For non-IP Office Subscription systems, these do not apply to Avaya Workplace Client on Vantage V3 devices, where support for the client is enabled by the phone's Avaya IP Endpoint license.
- For descriptions of the 'Basic' and 'Advanced' client feature sets, see [Avaya Workplace Client Modes](#) on page 11.

Subscription Systems

On subscription mode IP Office systems, Avaya Workplace Client is supported for the following users, including Vantage phone users:

User Subscription	Client Features	Operating System
Telephony Plus User	Basic	macOS, Windows
Unified Communications User	Advanced	Android, iOS, macOS, Windows

PLDS Licensed Server Edition/Select Systems

On IP Office Server Edition and IP Office Select systems, Avaya Workplace Client is supported for the following users:

User Profile	System Licenses	User Licenses	Client Features	Operating System
Office Worker User	IP Office Server Edition or IP Office Select	Office Worker	Advanced	macOS, Windows
Power User		Power User		Android, iOS, macOS, Windows

PLDS Licensed IP500 V2 Systems

On IP500 V2 systems running in Essential Edition or Preferred Edition modes, Avaya Workplace Client is supported for the following users

User Profile	System Licenses	User Licenses	Client Features	Operating System
Basic User	Essential Edition	Avaya Softphone License	Basic	macOS, Windows
Mobile User	Essential Edition + Preferred Edition	Mobile Worker + Avaya Softphone License		
Teleworker User		Teleworker	Advanced	Android, iOS, macOS, Windows
Office Worker User		Office Worker		
Power User		Power User		

Related links

[Avaya Workplace Clients and IP Office](#) on page 9

Avaya Workplace Client Modes

The user's Avaya Workplace Client client can operate with either basic or full feature, based on the user's IP Office licenses. See [User licensing](#) on page 10.

Client Features	Description
Basic	<p>This is the basic mode of Avaya Workplace Client support:</p> <ul style="list-style-type: none"> • It only supports Windows and macOS clients. • It only supports basic telephony and local contacts from the host operating system. <p>In this mode, when logged into Avaya Workplace Client, it is the user's sole telephony device:</p> <ul style="list-style-type: none"> • Logging into Avaya Workplace Client logs the user off any other extension. • Logging onto another phone logs them out of Avaya Workplace Client.
Advanced	<p>This is the fully featured mode of Avaya Workplace Client operation.</p> <ul style="list-style-type: none"> • It supports Windows, macOS, Android and iOS clients. • The user can use the client as their sole telephony device or in conjunction with other phones (IP Office simultaneous mode). • A range of additional features, listed below, can be configured.

Feature		Client Features	
		Basic	Advanced
Operating System	Windows, macOS	✓	✓
	Android, iOS	–	✓
Contacts	Local Contacts	✓	✓
	IP Office Directory	–	✓
	Enterprise Directory	–	✓
Presence		–	✓
Instant Messaging		–	✓
IP Office Simultaneous Mode This mode allows a user to use multiple telephony devices at the same time. For example, the user can simultaneously log in on both a physical desk phone and Avaya Workplace Client. See Simultaneous Mode Devices on page 41.		–	✓
Hidden Mode (Agent Mode) This mode is used for users who control their telephone calls through another application but still use the Avaya Workplace Client as the audio connection. See Disabling local notifications on page 45.		–	✓

Avaya Workplace Client Modes

The following Avaya Workplace Client modes are supported by the client **Place and Receive Calls Using...** setting.

Place and Receive Calls Using...	Client Features	
	Basic	Advanced
This Computer In this mode, the client makes and answers calls on the client device, including the call audio and video.	✓	✓
Shared Control (Desk Phone) In this mode, the client is used to make and answer calls on the user's associated IP Office desk phone. See Workplace Shared Control Mode on page 39	–	✓
Other Phone Mode (Telecommuter) In this mode, the user specifies the number of another phone to use as the audio path for their calls. <ul style="list-style-type: none"> • Making a call from the client causes the IP Office to call that other phone and, when answered, then make a call to the number dialed. • Incoming calls to the user are redirected to the other number to be answered on that phone. 	–	✓
Workplace Client (VDI) This mode uses two clients, one installed on the local PC and the other on the user's virtual VDI desktop. The local client is used for call audio whilst the virtual desktop client is used for call control and other features. See Avaya Workplace Client VDI Support on page 43. <ul style="list-style-type: none"> • Power User or Unified Communications User license only. 	–	✓

Related links

[Avaya Workplace Clients and IP Office](#) on page 9

Codec support

The supported audio codecs depend on the type of Avaya Workplace Client and the type of IP Office system.

Codec	Mobile		IP Office	
	iOS, Android	macOS, Windows	IP500 V2	Other
Opus	✓	✓	–	✓ ^[1]

Table continues...

Codec	Mobile		IP Office	
	iOS, Android	macOS, Windows	IP500 V2	Other
G.722	✓	✓	✓	✓
G.711 A-law	✓	✓	✓	✓
G.711 U-Law	✓	✓	✓	✓
G.726	✓	✓	–	–
G.729A	✓	✓	✓	✓
G.729B	✓	–	✓	–

1. Supported from IP Office R11.1 FP2.

Related links

[Avaya Workplace Clients and IP Office](#) on page 9

Supporting IPv6 extensions on IP Office

IP Office can supported J100 and Avaya Workplace Client extensions that use IPv6 using one of the following methods:

- **Remote IPv6 extensions using a dual-stack ASBCE**

This method of connection uses an ASBCE R10.1.2 or higher configured for dual-stack (IPv4/IPv6) and IP Office R11.1.3.1 or higher. It only supports IPv6 for remote J100 and Avaya Workplace Client extensions. See [Deploying Remote IP Office SIP Phones with an ASBCE](#).

- **Remote and local J100 IPv6 extensions**

This method uses a Linux-based IP Office server (R12.1 and higher) configured with IPv6 addresses. That allows connection of both remote and local IPv6 J100 and Avaya Workplace Client extensions. Note: Avaya still only supports remote extensions when connected through a firewall and/or session border controller.

- The IP Office must have an FQDN that DNS resolves to both the IPv4 and IPv6 addresses of the IP Office.
- Within the IP Office configuration, you must use FQDNs where supported by the configuration fields.
- For J100 phones using IPv6, for resilience you must also configure the failover IP Office to use IPv6.
- The IP Office does not support Direct Media for extension connections that use ANAT. However, it will apply RTP relay to reduce the IP Office resource requirements.
- Avaya supports IPv6 on IP Office LAN1. Avaya also supports IPv6 on LAN2 but only when IPv6 is enabled on LAN1 also.

You cannot combine the two methods. For example, you cannot use a dual-stack ASBCE and an IP Office with an IPv6 address.

Related links

[Avaya Workplace Clients and IP Office](#) on page 9

Chapter 2: Workplace Ports

This section covers the ports used by the client and associated applications.

Related links

[Avaya Workplace Client Ports](#) on page 15

[Requirements for Avaya Workplace Client and Avaya Cloud Services](#) on page 16

[Requirements for Avaya Workplace Client and Equinox Client Meetings Online](#) on page 16

Avaya Workplace Client Ports

Firewall requirements inbound to the IP Office system.

Port	Direction	Protocol	Reason
443	In	HTTPS	Secure client configuration/web socket
80	In	HTTP	Client configuration/web socket.
8411	In	HTTP	Client configuration/web socket if Use preferred phone ports enabled on IP Office.
411	In	HTTPS	Secure client configuration/web socket if Use preferred phone ports enabled on IP Office.
5060	In/Out	TCP/UDP	UDP/TCP SIP Signaling. Use of 5060 is deprecated. On Android clients a warning is displayed.
5061	In/Out	TCP/TLS	TLS SIP Signaling
40750-50750	In/Out	UDP-RTP/RTCP	Media for SIP calls and call control.

For the full port matrix, see <https://support.avaya.com/css/secure/documents/101065872>.

Related links

[Workplace Ports](#) on page 15

Requirements for Avaya Workplace Client and Avaya Cloud Services

Avaya Cloud Services endpoints use the following types of traffic:

- HTTPS and WebSocket (WSS) ([WebSocket](#))
- WebRTC ([wiki/WebRTC](#))

TLS traffic is used for both HTTPS and WSS. Any TLS-inspection should support these protocols or have an exception for the listed hosts.

TCP and HTTP tunneling are not supported for Audio and Video.

The following hosts and protocols should be unrestricted for all Avaya Cloud Services features to work as intended. Whitelisting based on IP address is not recommended since they can change dynamically. In addition, HTTP headers such as Authorization should be left intact.

Hosts	Ports	Protocol	Description
*.avayacloud.com	80, 443	HTTPS, WSS	Messages
*.esna.com	80, 443	HTTPS	Mobile authentication
ASN of 15169	5228, 5229, 5230	TCP	Push notification
accounts.google.com	80, 443	HTTPS	SSO
login.microsoftonline.com	80, 443	HTTPS	SSO
login.salesforce.com	80, 443	HTTPS	SSO
*.avaya.com	80, 443	HTTPS	SSO

Related links

[Workplace Ports](#) on page 15

Requirements for Avaya Workplace Client and Equinox Client Meetings Online

Firewall requirements in direction from customer premise to Cloud.

Port	Direction	Protocol	Reason
443, 8443	Out	TCP	Unified Portal, web meet me (WebRTC) signaling.

Table continues...

Port	Direction	Protocol	Reason
35000-40000 (configurable)	Out	UDP	SIP connectivity – media.
3478, 50000-55000 (configurable)	Out	UDP	Web meet me connectivity – media.

Related links

[Workplace Ports](#) on page 15

Chapter 3: IP Office SIP Configuration for Avaya Workplace Client Support

The IP Office system needs to be configured for SIP extension operation. Refer to the [IP Office SIP Telephone Installation Notes](#).

- The system's **SIP Registrar FQDN** should be set and should be resolvable through DNS back to the system.
- For Avaya Cloud Services and external clients, that resolution must be supported externally.

Related links

[IP Office Messaging Server Configuration](#) on page 18

[User Configuration](#) on page 19

[Creating an Avaya Workplace Client user](#) on page 19

[Avaya Workplace Client Emergency Number Dialing](#) on page 20

[IP Office User Settings for Avaya Workplace Client](#) on page 21

[IP Office Settings Files](#) on page 22

[Avaya Workplace Client NoUser Source Numbers](#) on page 22

IP Office Messaging Server Configuration

Avaya Workplace Client clients can perform their initial registration with IP Office either directly or through Avaya Cloud Services. The selected method affects how instant messaging and presence information is provided to clients.

Procedure

1. Using either IP Office Manager or IP Office Web Manager, load the system configuration.
2. Select **System > System**.
3. Locate the **Messaging Server** option and select the required setting:

Setting	Description
one-X Portal	The one-X Portal server is used to support instant messaging between IP Office clients including Avaya Workplace Client. The clients must register directly to the IP Office system by entering the URL for the 46xxsetting.txt file rather than using features such as SSO or an email address.
Avaya Spaces	Workplace client instant messaging and presence is done through Avaya Cloud Services. It does not include non-Avaya Cloud Services users. Clients can register using any of the methods supported through Avaya Cloud Services.

4. Save the configuration change.

Related links

[IP Office SIP Configuration for Avaya Workplace Client Support](#) on page 18

User Configuration

The processes in this document create a new Avaya Workplace Client user who will use Avaya Workplace Client in standalone mode. That is, a user without an associated extension record.



If you want to configure a user who will use both a desk phone and Avaya Workplace Client in simultaneous mode, alter the configuration settings of the existing user. No adjustments to their existing associated extension record are required.

Related links

[IP Office SIP Configuration for Avaya Workplace Client Support](#) on page 18

Creating an Avaya Workplace Client user

Procedure

1. Using either IP Office Manager or IP Office Web Manager, load the system configuration.
2. If using IP Office Manager:
 - a. To edit an existing user, select the existing user record.
 - b. To add a new user, select the system on which the user record should be created and then select  User.
3. If using IP Office Web Manager:
 - a. Select **Call Management > Users**.
 - b. To edit an existing user, click the  pencil icon next to the user.

- c. To add a new user, click **+Add User** and select the system on which the user record should be created.

4. Configure the user settings.

Depending on the license profile selected, the configuration tool may indicate that various other settings must be complete.

5. When creating a new user, after clicking **OK** or **Create**, you are prompted whether to also automatically create a new extension.

If Avaya Workplace Client will be the user's only telephony device, select **None**.

Related links

[IP Office SIP Configuration for Avaya Workplace Client Support](#) on page 18

Avaya Workplace Client Emergency Number Dialing

You must instruct Avaya Workplace Client users on mobile/cellular devices to use the device's native dialer application when connecting from a remote location. Doing otherwise associates the emergency call with the IP Office location rather than the mobile/cellular device user's true location.

Using Cellular Direct Numbers for Emergency Calls

For Avaya Workplace Client users on mobile iOS/Android devices, you can configure a set of "cellular direct numbers" (CDN).

When an Avaya Workplace Client user dials a cellular direct number, the client prompts the user to allow the device's native dialer to make the call using the mobile/cellular public telephone network. The call location information is then determined by the mobile/cellular network provider services.

The SET_CDNL Source Number

For IP Office R11.1 FP2 SP2 and higher, you can use the **NoUser** source number `SET_CDNL=` to add cellular direct number settings to the IP Office system configuration. These settings add CDN commands to the auto-generated `46xxsettings.txt` file.

- `SET_CDNL=DISABLED`

This adds the following string to the auto-generated `46xxsettings.txt` file. This disables cellular direct number operation.

```
- SET CELLULAR_DIRECT_NUMBER_LIST DISABLED
```

- `SET_CDNL="911","9911"`

This adds the following strings to the auto-generated `46xxsettings.txt` file. These enable cellular direct number operation and specify the numbers that will trigger the feature. Enclose each number in " " quotation marks. Separate multiple numbers with commas.

```
- SET CELLULAR_DIRECT_ENABLED 1
  SET CELLULAR_DIRECT_NUMBER_LIST "911","9911"
```

- You can use multiple `SET_CDNL=` source numbers.
- The maximum length of any individual `SET_CDNL=` entry is 63 characters.
- The maximum length of the `SET CELLULAR_DIRECT_NUMBER_LIST` string is 127 characters.

Related links

[IP Office SIP Configuration for Avaya Workplace Client Support](#) on page 18

IP Office User Settings for Avaya Workplace Client

The key settings used for Avaya Workplace Client and functional description.

Function	Description
Password	Enter and confirm the user's password. This password is used for Avaya Workplace Client login.
Extension	Enter an extension number for the user. This value is also used for the Avaya Workplace Client login.
Unique Identity	For Avaya Workplace Client users who will use Avaya Cloud Services, enter their domain email address. They can then use that address to connect their Avaya Workplace Client to the IP Office.
Profile	Avaya Workplace Client is supported for any user profile other than Non-licensed User and Telephony User .
Enable Mobile VoIP client	Select this option to allow the user to use Avaya Workplace Client on Android and iOS devices.
Enable Desktop/ Tablet VoIP client	Select this option to allow the user to use Avaya Workplace Client on macOS and Windows devices.

Related links

[IP Office SIP Configuration for Avaya Workplace Client Support](#) on page 18

IP Office Settings Files

During registration, the Avaya Workplace Client requests a `46xxsettings.txt` file from the IP Office system. This contains a range of settings that control how the client will operate. This is either an `46xxsettings.txt` file auto-generated by the IP Office system when requested or a static file that you have uploaded to the IP Office.

Using the auto-generated file is recommended as its contents automatically change to match the configuration of the IP Office system.

You can change or override the contents of the auto-generated `46xxsettings.txt` file when required:

- **NoUser Source Numbers**

You can add special values to the IP Office system configuration as **NoUser** source numbers. These add additional values to the `46xxsettings.txt` file. See [Avaya Workplace Client NoUser Source Numbers](#) on page 22.

- **46xxspecials.txt File**

For IP Office R11.1.2.4 and higher, the IP Office supports using a `46xxspecials.txt` with Avaya Workplace Client. When present on the IP Office system, after requesting the `46xxsettings.txt` file the client will request the `46xxspecials.txt` file. This allows you to add additional settings whilst still using the auto-generated `46xxspecials.txt` file.

For details of settings file operation, refer to the [IP Office SIP Telephone Installation Notes](#) manual.

Related links

[IP Office SIP Configuration for Avaya Workplace Client Support](#) on page 18

Avaya Workplace Client NoUser Source Numbers

The values in the auto-generated `46xxsettings.txt` settings file are based on settings taken from the IP Office system configuration. However, it may occasionally be necessary to add additional values to the auto-generated file. You can do this by entering the values into the IP Office configuration as **NoUser** source numbers.

- Since these changes are applied to the values in the auto-generated `46xxsettings.txt` file, they are overridden by any setting entered in the `46xxspecials.txt` file if present.
- There are a number of **NoUser** source number settings used for remote extensions. They operate differently in that they change existing values in the auto-generated settings file given

to a phone when the system detects that the phone requesting the file is a remote extension. See the [Deploying Remote IP Office SIP Phones with an ASBCE](#) manual.

Example **NoUser** source numbers for Avaya Workplace Client are:

- EQNX_CONTACT_MATCHING_MIN_DIGITS=N

By default the Avaya Workplace Client performs contact matching on calls using 10-digits. For some locations national numbering is shorter, for example 8 digits in Bahrain. This **NoUser** source numbers adds the command `SET CONTACT_MATCHING_MIN_DIGITS N` to the auto-generated `46xxsettings.txt`, where N is the number of digits to use for contact matching.

- SET_CDNL=DISABLED

This adds the following string to the auto-generated `46xxsettings.txt` file. This disables cellular direct number operation.

```
- SET CELLULAR_DIRECT_NUMBER_LIST DISABLED
```

- SET_CDNL="911", "9911"

This adds the following strings to the auto-generated `46xxsettings.txt` file. These enable cellular direct number operation and specify the numbers that will trigger the feature. Enclose each number in " " quotation marks. Separate multiple numbers with commas.

```
- SET CELLULAR_DIRECT_ENABLED 1
  SET CELLULAR_DIRECT_NUMBER_LIST "911", "9911"
```

- You can use multiple `SET_CDNL=` source numbers.
- The maximum length of any individual `SET_CDNL=` entry is 63 characters.
- The maximum length of the `SET CELLULAR_DIRECT_NUMBER_LIST` string is 127 characters.

Related links

[IP Office SIP Configuration for Avaya Workplace Client Support](#) on page 18

Chapter 4: Workplace Client Installation

This section covers the processes for installation of the workplace client software on individual user devices.

Related links

[Windows Workplace Client Installation](#) on page 24

[Installing macOS client software](#) on page 28

[Installing Avaya Workplace Client on an iOS device](#) on page 29

[Installing Avaya Workplace Client on an Android device](#) on page 29

Windows Workplace Client Installation

Before you begin

- Windows 10, Windows 11
- Microsoft .NET Framework 4.5.2 or a later version.
- Exchange Server/Outlook Integration
 - Exchange Server 2016 and later.
 - Microsoft Outlook add-in for web mail is supported on Exchange Server 2016 and later.
 - Exchange Web Services must be enabled for the Avaya Workplace Client Outlook Add-in. Internet access must also be available because portions of the add-in are hosted on the Internet.

The install package for the Windows Avaya Workplace Client can be downloaded from the IP Office support pages on <http://support.avaya.com>.

Related links

[Workplace Client Installation](#) on page 24

[Windows Workplace Client Installation](#) on page 24

[Windows command line installation](#) on page 25

[Installation using a group policy](#) on page 27

Windows Workplace Client Installation

This process covers simple single user installation without DSCP or IM support.

Procedure

1. Copy the MSI file to a temporary location on the PC.
2. Double-click on the installer.
3. Click **Next**.
4. Accept the terms of the license agreement and click **Next**.
5. Select the type of installation and click **Next**.

The **Custom** option allows you to select not to install the Outlook and web browser options.

6. If necessary change the installation path. Click **Next**.
7. Select the default language and click **Next**.
8. Click **Install**.
9. If prompted by the Windows operating system whether to allow the installation select **Yes**.
10. Click **Finish**.

Next steps

- Proceed to initial configuration. See [Initial Avaya Workplace Client configuration](#) on page 31.

Related links

[Windows Workplace Client Installation](#) on page 24

Windows command line installation

The following command line options can be used to install/uninstall the Windows client. These can be used for individual installations or by network administrators to create group policies for installation (see [Installation using a group policy](#) on page 27).

- The Windows command is `msiexec`. This is then followed by a number of command options and values those options.
- - Several options require the name of the Avaya Workplace Client installation file. Enclose the file name in "" quotation marks. The file name varies depending on the version. For example: `"Avaya Workplace Setup 3.20.1.10.2.msi"`
- Multiple command options can be combined. For example, `msiexec /i "Avaya Workplace Setup 3.20.1.10.2.msi" /qn OP=0` specifies an installation with no display (silent install) and the Outlook plug install disabled.

Command Options

The following are examples of the options and values that can be used with the `msiexec` command for Windows Avaya Workplace Client installation:

Purpose	Command Line Option and Values
Install	<pre>/i "<installer msi file>"</pre> <p>Use the .msi file to perform an installation of the client. For example:</p> <ul style="list-style-type: none"> • <code>msiexec /i "Avaya Workplace Setup.msi"</code>
Silent process	<pre>/qn</pre> <p>Run the command process with no user interface. This option is only supported when executed with administrator privileges.</p> <p>For example, for a silent installation:</p> <ul style="list-style-type: none"> • <code>msiexec /i "Avaya Workplace Setup.msi" /qn</code> •
Automatic configuration	<pre>AUTOCONFIG="<URL of config file>"</pre> <p>Automatically apply the settings from the specified configuration file. This option is not supported for Avaya Cloud Services installations.</p>
Uninstall	<pre>/x "<installer msi file>"</pre> <p>Use the .msi file to run an uninstall of the current client. For example:</p> <ul style="list-style-type: none"> • <code>msiexec /x "Avaya Workplace Setup.msi"</code>
Installer help	<pre>/?</pre> <p>Display general help for the <code>msiexec</code> command. For example:</p> <ul style="list-style-type: none"> • <code>msiexec /?</code>
Log install	<pre>/l<path for install log files></pre> <p>Log the process to log files. The <code>/l</code> option is followed by a number of values that specify what outputs to include in the log.</p> <p>In the example below, the <code>*</code> elements indicates log everything (except verbose log outputs), the <code>v</code> element indicates include verbose log outputs.</p> <ul style="list-style-type: none"> • <code>msiexec /i "Avaya Workplace Setup.msi" /l*v"C:/temp"</code>
Enable IM Provider	<pre>IMPROVIDER=1</pre> <p>Include the IM provider settings in the installation. Installation of the IM provider is disabled by default. For example:</p> <ul style="list-style-type: none"> • <code>msiexec /i "Avaya Workplace Setup.msi" IMPROVIDER=1</code>
Enable DSCP driver installation	<pre>NOQOS=0</pre> <p>Include enabling the DSCP driver in the installation. This is disabled by default. For example:</p> <ul style="list-style-type: none"> • <code>msiexec /i "Avaya Workplace Setup.msi" NOQOS=0</code>

Table continues...

Purpose	Command Line Option and Values
Disable Outlook plug-in install	OP=0 Disable inclusion of the outlook plug-in setup in the installation. For example: <ul style="list-style-type: none"> • <code>msiexec /i "Avaya Workplace Setup.msi" OP=0</code>
Disable browser plug-in	BP=0 Disable inclusion of the browser plug-in in the installation. For example: <ul style="list-style-type: none"> • <code>msiexec /i "Avaya Workplace Setup.msi" BP=0</code>
VDI Install	VDIENV=1 Specify that the installation is one for a virtual desktop. See Avaya Workplace Client VDI Support on page 43. For example: <ul style="list-style-type: none"> • <code>msiexec /i "Avaya Workplace Setup.msi" VDIENV=1</code>

Related links

[Windows Workplace Client Installation](#) on page 24

Installation using a group policy

About this task

Use this procedure to deploy Avaya Workplace Client from a Windows server using a Group Policy. This can be used to automatically install the Avaya Workplace Client when a user logs in on the network.

This process uses the client's command line options. See [Windows command line installation](#) on page 25.

Procedure

1. Open **Group Policy Management** (if necessary use **Start > run > GPMC.MSC**).
2. Navigate to **Default Domain Policy**.
3. Right-click **Default Domain Policy** and click **Edit**.
4. Navigate to **Computer Configuration > Policies > Windows Settings > Scripts**.
5. Place the Avaya Workplace Client installer into the the **Scripts/Startup** folder.

You can open the location by clicking **Show Files**.

6. Add a new script by clicking **Add**.
7. Browse for the Avaya Workplace Client installer.
8. In the **Script Parameters** field, add the command line parameters required.

For example, for a silent installation add the **/qn** parameter and click **OK**

Related links

[Windows Workplace Client Installation](#) on page 24

Installing macOS client software

About this task

The install package for the macOS Avaya Workplace Client can be downloaded from the IP Office support pages on <http://support.avaya.com>.

This process covers simple single user installation. For advanced installation options see [Windows command line installation](#) on page 25.

Procedure

1. Copy the DMG file to a temporary location on the PC.
2. Double-click on the installer.
3. Click **Next**.
4. Accept the terms of the license agreement and click **Next**.
5. If necessary change the installation path. Click **Next**.
6. Select the default language and click **Next**.
7. Click **Install**.
8. If prompted by the macOS operating system whether to allow the installation select **Yes**.
9. Click **Finish**.

Result

- Proceed to initial configuration. See [Initial Avaya Workplace Client configuration](#) on page 31.

Related links

[Workplace Client Installation](#) on page 24

[Advanced installation](#) on page 28

Advanced installation

The following command line options can be used to install/uninstall the macOS client. Note that the silent options only work with administrator privileges.

- Tip: To automatically mount the .dmg file automatically, double-click the file.
- Silent Installation: `/Volumes/Avaya\ Equinox/Install.app/Contents/MacOS/Install -silent`
- Automatic configuration: `/Volumes/Avaya\ Equinox/Install.app/Contents/MacOS/Install -silent -autoconfigURL <URL>` where <URL> is the appropriate path to the settings file.
- Silent Uninstall: `sudo /Volumes/Avaya\ Equinox/Uninstall.app/Contents/MacOS/Uninstall -silent`
- Installation help: `/Volumes/Avaya\ Equinox/Install.app/Contents/MacOS/Install -help`

- Uninstall help: `/Volumes/Avaya\ Equinox/Uninstall.app/Contents/MacOS/Uninstall -help`

Related links

[Installing macOS client software](#) on page 28

Installing Avaya Workplace Client on an iOS device

Procedure

1. Open the App Store and search for Avaya Workplace Client.
2. Select the entry.
3. Select **Install**.
4. After the installation process is complete, select **Open**.
5. Accept the terms of the license agreement and the message to not use Avaya Workplace Client to make emergency calls.

Next steps

- Proceed to initial configuration. See [Initial Avaya Workplace Client configuration](#) on page 31.

Related links


[Workplace Client Installation](#) on page 24

Installing Avaya Workplace Client on an Android device

About this task

The Avaya Workplace Client can be installed from the Google Play Store.

Procedure

1. On the Android device, access the Google Play Store.
2. Search for **Avaya Workplace**.
3. Select **Install**.
4. Once the application is installed, either select **Open** or locate and click the  icon on the desktop.
5. Allow permission for the application to make and manage phone calls.

6. Allow permission for the application to record audio.
 - The remaining permissions are optional (take pictures and record video, access your contacts and access your calendar). However, if not selected then some features of Avaya Workplace Client will not work.
7. Allow the application to restart.
8. When the end user license agreement is displayed, click **Accept**.

Next steps

- Proceed to initial configuration. See [Initial Avaya Workplace Client configuration](#) on page 31.

Related links

[Workplace Client Installation](#) on page 24

Chapter 5: Initial Avaya Workplace Client configuration

The details that the user needs to enter during the initial login vary depending on whether the installation model is using Avaya Cloud Services or not:

Method	Description
Login using Avaya cloud services:	This login uses the user's domain email address as configured in the Avaya cloud services settings. Those settings then connect the client with the IP Office system.
IP Office Direct Login:	This login uses the direct address of the settings file on the IP Office system and then uses the IP Office user's extension number and password.

Related links

[Avaya Workplace Client Email Connection](#) on page 31

[Direct IP Office Avaya Workplace Client connection](#) on page 32

[Calendar Integration](#) on page 33

Avaya Workplace Client Email Connection

About this task

Use this process for installations that use Avaya Cloud Services. In that scenario, Avaya Workplace Client user register with Avaya Cloud Services using their email address. Their email address is set as their **Unique Identity** in the IP Office configuration.

The Avaya Cloud Services configuration for the domain tells the client the address of the IP Office system. This process is common to all the operating systems. If during this initial configuration, the operating system or installed virus checker prompts whether to allow the application, select that option.

Procedure

1. Start the Avaya Workplace Client application.
2. Select **Configure my account**.
3. In **Email**, enter your email address.
4. Click **Next**.

5. If prompted to **Choose your environment**, select the name of the system to which you want to login and click **Next**.
6. The next steps depend on whether the system has been configured for Avaya Cloud Authorization (see [Enabling Avaya Cloud authorization](#) on page 64):
 - If the **Access everything from one account** menu appears:
 - a. Select the type of account you want to use to login and enter the details. Otherwise, enter your email address and click **Get Started**.
 - b. The Avaya Workplace Client login menu appears briefly and then disappears as you are logged in.
 - If the Avaya Workplace Client login menu appears and stays visible:
 - a. Enter your extension number.
 - b. Enter your user password. This is the same password as you use for the user portal (self-administration).
 - c. Click **Sign In**.

Related links

[Initial Avaya Workplace Client configuration](#) on page 31


Direct IP Office Avaya Workplace Client connection

About this task

Use this process for installations where Avaya Cloud Services is not being used. In this scenario, the Avaya Workplace Client user enters the address of the IP Office system's `46xxsettings.txt` file. The user is prompted to register directly with the IP Office system using their extension number and password.

This process is common to all the client operating systems. If during this initial configuration, the operating system or installed virus checker prompts whether to allow the application, select that option.

Procedure

1. Start the Avaya Workplace Client application.
2. Select **Configure my account**.
3. Click on the  settings icon and select **Use web address**.
4. Enter the communication system's FQDN, prefixed with `https://` and followed by `/46xxsettings.txt`
 - It will look something like `https://<serveraddress>/46xxsettings.txt`. Do not use the system's numeric IP address.
5. Click **Next** and wait whilst the application fetches the information it needs from your communication system.

6. The next steps depend on whether the system has been configured for Avaya Cloud Authorization (see [Enabling Avaya Cloud authorization](#) on page 64):
 - If the **Access everything from one account** menu appears:
 - a. Select the type of account you want to use to login and enter the details. Otherwise, enter your email address and click **Get Started**.
 - b. The Avaya Workplace Client login menu appears briefly and then disappears as you are logged in.
 - If the Avaya Workplace Client login menu appears and stays visible:
 - a. Enter your extension number.
 - b. Enter your user password. This is the same password as you use for the user portal (self-administration).
 - c. Click **Sign In**.

Related links

[Initial Avaya Workplace Client configuration](#) on page 31

Calendar Integration

Avaya Workplace Client can display meetings from the user's calendar on its **Top of Mind** and **My Meetings** pages. It can include show meetings from the following sources:

Calendar	Description
Local calendar	On Android and iOS devices, Avaya Workplace Client can display meetings from the device's local calendar.
Exchange server	Copy meetings from the Avaya Workplace Client user's account on an Exchange server.

Related links

[Initial Avaya Workplace Client configuration](#) on page 31

[Enabling exchange calendar support](#) on page 33

[Selecting the calendar to display](#) on page 34

[Enabling exchange calendar support](#) on page 33

[Selecting the calendar to display](#) on page 34




Enabling exchange calendar support

About this task

Before Exchange can be selected as a calendar source, details of the Exchange server and the user's email account on that server need to be entered in the Avaya Workplace Client settings.

Exchange Server 2013 and later versions supported

Procedure

1. Depending on the operating system, click on the settings  icon or click on the  **Menu** icon and then the  settings icon.
2. Select **Services > Exchange Calendar**.
3. Enable **Exchange Calendar**.
4. Enter the Exchange server domain and server address details
5. Go to **Accounts**.
6. In the **Exchange Calendar** section, enter your email account details.
7. Click **Done**.

Result

Following the restart you can select Exchange as your calendar source.


Related links

[Calendar Integration](#) on page 33

[Calendar Integration](#) on page 33

Selecting the calendar to display

Procedure

1. Click on the  **Calendar** icon
2. Click on the **My Meetings** drop down menu.
3. Select the calendars that you want the application to display.
4. Click **My Meetings** again to hide the list of available calendars.

Related links

[Calendar Integration](#) on page 33

[Calendar Integration](#) on page 33

Chapter 6: Calendar Integration

Avaya Workplace Client can display meetings from the user's calendar on its **Top of Mind** and **My Meetings** pages. It can include show meetings from the following sources:

Calendar	Description
Local calendar	On Android and iOS devices, Avaya Workplace Client can display meetings from the device's local calendar.
Exchange server	Copy meetings from the Avaya Workplace Client user's account on an Exchange server.

Related links

[Initial Avaya Workplace Client configuration](#) on page 31

[Enabling exchange calendar support](#) on page 33

[Selecting the calendar to display](#) on page 34

[Enabling exchange calendar support](#) on page 33

[Selecting the calendar to display](#) on page 34




Enabling exchange calendar support

About this task

Before Exchange can be selected as a calendar source, details of the Exchange server and the user's email account on that server need to be entered in the Avaya Workplace Client settings.

Exchange Server 2013 and later versions supported

Procedure

1. Depending on the operating system, click on the settings  icon or click on the  **Menu** icon and then the  settings icon.
2. Select **Services > Exchange Calendar**.
3. Enable **Exchange Calendar**.
4. Enter the Exchange server domain and server address details
5. Go to **Accounts**.
6. In the **Exchange Calendar** section, enter your email account details.

7. Click **Done**.

Result

Following the restart you can select Exchange as your calendar source.


Related links

[Calendar Integration](#) on page 33

[Calendar Integration](#) on page 33

Selecting the calendar to display

Procedure

1. Click on the  **Calendar** icon
2. Click on the **My Meetings** drop down menu.
3. Select the calendars that you want the application to display.
4. Click **My Meetings** again to hide the list of available calendars.

Related links

[Calendar Integration](#) on page 33

[Calendar Integration](#) on page 33

Chapter 7: Contact Integration

This chapter covers processes relating to the display of contacts within Avaya Workplace Client.

- Avaya Workplace Client licensed for basic mode, only support local contacts. See [User licensing](#) on page 10.

Related links

[Contact Integration](#) on page 37




[Exchange Self-Avatar Support](#) on page 37

Contact Integration

About this task

If when you initially logged in to Avaya Workplace Client, you did not configure access to local contacts.

Procedure

1. Depending on the operating system, click on the settings  icon or click on the  **Menu** icon and then the  settings icon.
2. Then:
 - Android: Select **Privacy and safety** > **App permissions** **Contacts** and enable **Contacts** permissions
 - iOS: Select **Privacy** and enable **Contacts**.
 - Windows/macOS: Select **User Preferences** > **Contacts** and enable **Show Local Contacts**.

Related links

[Contact Integration](#) on page 37

Exchange Self-Avatar Support

If not using self-avatar support through Avaya cloud services or SSO login, you can enable self-avatar support using Microsoft Exchange Web Services (EWS).

To configure this, in summary:

1. Add the setting `SELF_AVATAR_ENABLED 1` to be added to the settings file (`46xxsettings.txt` or `46xxspecials.txt`) provided to clients.
2. Configure **Exchange Calendar** support in the Avaya Workplace Client., setting the integration to **Microsoft Modern**. See [Calendar Integration](#) on page 33.

Related links

[Contact Integration](#) on page 37

Chapter 8: Workplace Shared Control Mode

Windows and macOS users can switch their Avaya Workplace Client to shared control mode. In this mode, the client is used to make and answer calls via the user's associated desk phone.

- Supported phones: 1100 Series, 1200 Series, J100 Series (except J129), 9600 Series, DECT R4, digital and analog extensions.
- The Avaya Workplace Client can control the following telephony features on the phone: answer calls, make calls, hold, unhold, ignore, drop, transfer, conference, send DTMF, collect voicemail.
- This feature is not supported for users licensed for 'basic' features only.

When using shared control mode, the following changes apply to the Avaya Workplace Client:

- Mute/unmute is not supported. The clients mute/unmute controls are disabled.
- Video calls are not supported. The video call controls are disabled.
- Conference controls are hidden.
- The user cannot drag multiple contacts in order to create an ad-hoc conference.
- The user cannot add someone to a call.
- Numbers dialed from the client are not processed by the client's dial plan settings.
- Calls ignored on the desk phone (which mutes the phones audible alerting) continue to audible alert on the client.
- Exiting the client/logging in again does not affect existing calls in progress on the desk phone.

Related links

[Enabling shared control mode](#) on page 39

Enabling shared control mode

About this task

Use the following process to switch the desktop client to shared control mode.

- This feature is not supported for users licensed for 'basic' features only.

Procedure

1. Click 

2. Select **Shared Control**.

Related links

[Workplace Shared Control Mode](#) on page 39

Chapter 9: Simultaneous mode

IP Office systems support 'simultaneous' mode operation. In that mode, users can be associated with multiple telephony devices at the same time. They can answer and make calls on any of those devices.

Related links

[Simultaneous Mode Devices](#) on page 41

[Simultaneous Mode Notes](#) on page 41

[Moving Calls Between Simultaneous Devices](#) on page 42

Simultaneous Mode Devices

An IP Office user can be logged in simultaneously on one of each of the following types of telephone devices:

Telephony Client	Notes
A physical desk phone	A physical phone, including a SIP, H.323 or DECT extension. This also includes clients running on a Vantage phone.
A desktop (PC) VoIP client:	<ul style="list-style-type: none">• Avaya Workplace Client for Windows• Avaya Workplace Client for macOS
A mobile VoIP client:	<ul style="list-style-type: none">• Avaya Workplace Client for Android• Avaya Workplace Client for iOS
A WebRTC client:	<ul style="list-style-type: none">• Spaces Calling using the Chrome extension.

Related links

[Simultaneous mode](#) on page 41

Simultaneous Mode Notes

The following notes relate to the operation of simultaneous telephony:

- Incoming calls to the user alert on all their devices and they can choose which device they want to use to answer.

- Whilst the user has a call in progress on one of the devices, any additional incoming call is presented only to that device.
- It is recommended not to mix simultaneous mode operation with features such as mobile twinning, telecommuting and mobile call controls that can lead to multiple duplicate calls. For example, a mobile client's external PSTN numbers as a active mobile twinning destination will cause duplicate alerts for the same call.
- Users can have their desk phone and their softphone applications registered to different servers in an IP Office network.
- Use of simultaneous mode is not supported when also using a non-telephony CTI client to control call handling. In that scenario it is not always possible to predict which telephony client will be used when making/answering a call from the CTI client which can lead to confusion.

Related links

[Simultaneous mode](#) on page 41

Moving Calls Between Simultaneous Devices

The IP Office system supports a number of features to enable users to move calls between their simultaneous devices.

Action	Description
Transfer	Users can transfer calls to their own extension number. That causes the call to alert on their other simultaneous devices.
Steal	For IP Office R11.1.2.4 and higher, a Call Steal shortcode set to with the user's extension number will retrieve a current call from their other simultaneous device.
Workplace Clients	<p>For IP Office R11.1.3 and higher, Avaya Workplace Client users can use their client to move and retrieve calls:</p> <ul style="list-style-type: none"> • Using move, the user can send a call from their Avaya Workplace Client to their other simultaneous devices. • Using retrieve, the user can move a call answered on their simultaneous device to their Avaya Workplace Client. <p>These features are enabled by a <code>SET IPO_CALL_HANDOVER_ENABLED 1</code> line in the <code>46xxsettings.txt</code> file.</p>

Related links

[Simultaneous mode](#) on page 41

Chapter 10: Avaya Workplace Client VDI Support

This section provides notes for deploying Avaya Workplace Client users in a virtual desktop infrastructure (VDI) environment. This is supported in IP Office R11.1 FP2 or higher with Avaya Workplace Client R3.22 or higher.

In basic outline, the solution uses two clients.

- One installed on the user's virtual desktop and used for call control.
- The other installed on the local PC from which the user accesses their virtual desktop. This client is used purely for the call media of calls controlled by the client running on the virtual desktop.
- The user needs to be logged in on both clients at the same time.
- This is supported for **Power User** and **Unified Communications User** user profiles.

	Local PC	Virtual Desktop
Supported VDI environment	VMware and Citrix (XenApps and XenDesktop)	
Operating System	Windows or Chromebook (Android)	Windows
Workplace Client	Workplace for Windows or Workplace for Android	Workplace for Windows
... client role	Call media (audio only)	Call control
... Place and Receive Calls Using Setting	This Computer	Workplace Client
... Notifications	Disabled	Enabled (default)

Related links

[Virtual client limitations](#) on page 44

[Local PC client installation for VDI support](#) on page 44

[Virtual desktop client installation for VDI support](#) on page 46

Virtual client limitations

When using the Avaya Workplace Client client as a virtual desktop client, the following limitations apply:

- Mute/unmute is not supported. The clients mute/unmute controls are disabled.
- Video calls are not supported. The video call controls are disabled.
- Conference controls are hidden.
- The user cannot drag multiple contacts in order to create an ad-hoc conference.
- The user cannot add someone to a call.

Related links

[Avaya Workplace Client VDI Support](#) on page 43

Local PC client installation for VDI support

This section details the processes necessary for installation of the Avaya Workplace Client on the local PC in a VDI setup. This client is then used for the call media (audio) during calls.

- For installation of the client on the virtual desktop, see [Virtual desktop client installation for VDI support](#) on page 46.

Related links

[Avaya Workplace Client VDI Support](#) on page 43

[Installing the local VDI client](#) on page 44

[Enabling Chrome desktop mode](#) on page 45

[Disabling local notifications](#) on page 45

Installing the local VDI client

Procedure

1. The local Avaya Workplace Client is installed and registered using the normal processes for a Windows or Android client installation.
 - **Windows:** See [Windows Workplace Client Installation](#) on page 24.
 - **Chromebook:** See [Installing Avaya Workplace Client on an Android device](#) on page 29.
2. Once installed, the user should be registered as normal. See [Direct IP Office Avaya Workplace Client connection](#) on page 32.
3. Test operation by making calls to and from the client. This tests the media connection between the local client and the IP Office.

Next steps

- Following installation and registration:
 - **Windows:** Go to [Disabling local notifications](#) on page 45.
 - **Chromebook:** Go to [Enabling Chrome desktop mode](#) on page 45 and then [Disabling local notifications](#) on page 45.

Related links

[Local PC client installation for VDI support](#) on page 44



Enabling Chrome desktop mode

When installed on a Chromebook, the Avaya Workplace Client can operation in either of two mode; desktop mode or as a mobility endpoint. When acting as a mobility client it cannot be controlled and used by the Avaya Workplace Client installed on the user's virtual desktop.

About this task

By default, the Avaya Workplace Client is automatically configured to operate in desktop mode. However, that setting should be checked using the process below.

Procedure

1. Click on the  **Menu** icon and then the  settings icon.
2. Select **User Preferences > General**.
3. Check that **Desktop mode** is enabled.

Next steps

- Go to [Disabling local notifications](#) on page 45.




Related links

[Local PC client installation for VDI support](#) on page 44

Disabling local notifications

By default, both the local and the VDI desktop clients will receive and show the same notifications. To prevent this, notifications should be disabled in the local client.

Procedure

1. Depending on the operating system, click on the settings  icon or click on the  **Menu** icon and then the  settings icon.
2. Select **User Preferences**.
3. Depending on the local PC operation system:
 - **Windows:** Select **Display** and enable **Hidden Mode**.
 - **Chromebook:**
 - a. Select **Settings > User Preferences > Notifications > Channel Notification Settings > Incoming calls > Behavior**.

- b. Select the **Make sound** option and minimize the client window to turn off the incoming call notifications.
4. Click **Done**.

Next steps

- Install the user's virtual desktop client. See [Virtual desktop client installation for VDI support](#) on page 46.

Related links

[Local PC client installation for VDI support](#) on page 44

Virtual desktop client installation for VDI support

The Avaya Workplace Client needs to be installed on the Windows VDI desktop using command line instructions.

Related links

[Avaya Workplace Client VDI Support](#) on page 43

[Virtual desktop client installation](#) on page 46

[Virtual desktop client login](#) on page 46

[Setting the client for the call media](#) on page 47

Virtual desktop client installation

Installation of the Avaya Workplace Client on a virtual Windows desktop should not be done using the normal process of double-clicking on the .msi file. Instead it must be done using a command line installation.

The basic command line used command is `msiexec /i "Avaya Workplace Setup.msi" VDIENV=1`. This runs the installation whilst enabling settings for use in a virtual desktop environment. If required, other command options can be included in the command line. See [Windows command line installation](#) on page 25.

The command line can be run either individual on each virtual desktop or using a Windows group policy (see [Installation using a group policy](#) on page 27).

Related links

[Virtual desktop client installation for VDI support](#) on page 46

Virtual desktop client login

Once the client software has been installed, the client needs to register and login directly with the IP Office system. See [Direct IP Office Avaya Workplace Client connection](#) on page 32. Operation in the VDI environment requires the user to be simultaneously logged in on both the local PC client and the virtual desktop client.

Once the virtual desktop client is connected, it needs to be configured to use the local client for its media. See [Setting the client for the call media](#) on page 47.


Related links

[Virtual desktop client installation for VDI support](#) on page 46

Setting the client for the call media

The Avaya Workplace Client installed on the VDI desktop needs to be configured to route its call media to the client installed on the local PC.

Procedure

1. Access the Avaya Workplace Client running on the VDI desktop.
2. Click 
3. Select **Workplace Client**.

Related links

[Virtual desktop client installation for VDI support](#) on page 46

Chapter 11: Workplace Troubleshooting

The following methods can be used to monitor the operation of workplace clients.

Related links

[Defaulting an Avaya Workplace Client](#) on page 48

[Emailing a bug report](#) on page 49




[Setting the Email Address](#) on page 49

Defaulting an Avaya Workplace Client

About this task

You can clear the application settings without having to reinstall the application.

Procedure

1. Depending on the operating system, click on the settings  icon or click on the  **Menu** icon and then the  settings icon.
2. Select **Support**.
3. Click **Reset Application**.
4. Click **Clear**.

The client is restarted.

Next steps

Reconfigure the application

Related links

[Workplace Troubleshooting](#) on page 48




Emailing a bug report

About this task

The Avaya Workplace Client softphone can create an email to which it attaches a zipped copy of its application logs. On Android devices, to use this function, you first need to set an email address

- On a Windows PC, this process can still be used even if the no default email client has been setup. For example, if the user uses browser based email only. After clicking **Report a Problem**, the client archives its logs and places the zip file in the temporary folder:
C:\Users\%USERPROFILE%\AppData\Local\Avaya\Avaya IX Workplace\Temp.
The file name will be similar to the following: Logs_2022-12-19_10-19-36-270.zip.

Procedure

1. Depending on the operating system, click on the settings  icon or click on the  **Menu** icon and then the  settings icon.
2. Select **Support > Report a Problem** (on Android devices, select **Support > Report a Problem > Send Logs**).
3. There is a pause while the application's log files are zipped.
4. On Android devices you may be prompted to select which email application to use.
5. The email application is started with the zipped log files attached.
6. Add any additional information that may assist the support personnel.
7. Complete and send the email.

Related links




[Workplace Troubleshooting](#) on page 48

Setting the Email Address

About this task

This option is only necessary on Android devices. Other Avaya Workplace Client allow manual entry of the address before the email is sent.

Procedure

1. Depending on the operating system, click on the settings  icon or click on the  **Menu** icon and then the  settings icon.
2. Select **Support > Report a Problem > Support Email Address**.
3. Enter the destination email address for support.

Related links

[Workplace Troubleshooting](#) on page 48

Part 2: Avaya Cloud Services

Chapter 12: Configuring Avaya Cloud Services support

This chapter covers the common configuration for IP Office systems to support Avaya Cloud Services. These steps are prerequisites to the configuration for specific features covered in the following chapters.

You can use Avaya Cloud Services to enable and support a range of additional features:

Feature	Description
User Synchronization	The IP Office can share details of users with a Unique Identity (email address) with Avaya Cloud Services. Those users can then: <ul style="list-style-type: none">• Login to and use Avaya Spaces.<ul style="list-style-type: none">- From February 2025, Avaya Spaces for meetings and conferences is no longer available for new customers. It is supported for existing customers until the end of their existing contract.• Register Avaya Workplace Client using their Unique Identity email address.<ul style="list-style-type: none">- Not supported with IPv6.
Workplace SSO login	Using Avaya Cloud Services, you can also configure the IP Office to allow users to login to Avaya Workplace Client using their Google, Office 365, or Salesforce account.
Apple Push Notification	The IP Office can use Apple Push Notification Service (APNS) to send push notifications to Avaya Workplace Client users on iOS devices. If iOS has suspended the client, the user can use controls in the notification to restart the client.
Instant Messaging with Avaya Cloud Services	Support instant messaging between Avaya Cloud Services users, Avaya Workplace Client users and other IP Office clients.
Use Spaces Calling	Spaces calling lets users make and receive IP Office calls through Avaya Cloud Services.
Use Avaya Calling for MS Teams	Make and answer calls within Microsoft Teams. See the Deploying Avaya Calling for MS Teams with IP Office manual.

Related links

- [Avaya Cloud Services support checklist](#) on page 52
- [Verifying the company domain](#) on page 52
- [Obtain the domain API Key and Key Secret](#) on page 54
- [Enter the Avaya Cloud Services settings](#) on page 55
- [Updating the Avaya Workplace clients](#) on page 56

Avaya Cloud Services support checklist

#	Action	Link/Notes	✓
1.	Select an internet time source.	The IP Office system must use an accurate time source to ensure correct certificate validation.	
2.	Configure SIP TLS extension support.	The IP Office must be configured and tested to support SIP TLS.	
3.	Verify the customer domain.	• See Verifying the company domain on page 52.	
4.	Obtain the API key and secret.	• See Obtain the domain API Key and Key Secret on page 54.	
5.	Enter the API key and secret into the IP Office security settings and enable Avaya Cloud Services support.	• See Enter the Avaya Cloud Services settings on page 55.	
6.	Continue with configuration for required Avaya Cloud Services features	<ul style="list-style-type: none"> • Configuring Avaya Cloud Services synchronization on page 57 • Configuring SSO login support on page 64 • Enabling Apple Push Notifications on page 67 • Supporting Spaces Calling on page 76 	

Related links

[Configuring Avaya Cloud Services support](#) on page 51

Verifying the company domain

About this task

The key part of Avaya Cloud Services integration is to associate the customer's domain address with their Avaya Cloud Services account. This process requires:

- The customer domain. For example: `example.com`
- Access to the DNS server settings for the domain.

! Important:

- Following the end-of-sale of Avaya Spaces, it is not possible to add a new company. Customers needing to add a new company for other Avaya Cloud Services should raise a support request with Avaya support.

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. If not already done so, click on your name top-right and select **Add Company**. Otherwise, click on **Manage Companies** and then either:
 - Click on the existing company name.
 - Click **Add New Company** to add another company.
3. Select the **Domains** tab.
4. Select **Add Domain**.
5. Enter the domain address and click **OK**.
6. Click on the **Verify** button shown next to the domain name. The menu displays a verification code.

Verify Domain

example.com

To confirm that you are in fact the owner of this domain, please follow the steps below:

1. Access the DNS record section of your domain's host
2. Add a new TXT entry with your verification code
3. Add @ to the host field (if required)
4. Once DNS changes have propagated click the Verify button below

Note: DNS changes should take only minutes to take effect but could take up to 72 hours

5. Leave the TXT entry in the DNS record as it may be checked periodically to maintain verification status

Detailed instructions can be found [HERE](#).

Your verification code is:
ZA=j1/luvcWpsxtvl9PCuy/dEnOM3LQDoYcPIU7XmBuJpQ=

Verify

- Copy the verification code and add it as a `TXT` record to the DNS entries on the domain's DNS server. For example:



Name	Type	TTL	Information
dns.example.com.	A	86400	192.168.0.6
example.com.	NS	86400	dns.example.com.
example.com.	TXT	86400	"ZA=j1/luvcWpstxtvI9PCuy/dE..
ldap.example.com.	A	86400	192.168.0.6
mail.example.com.	A	86400	192.168.0.6
mail.example.com.	MX	86400	1 192.168.0.6.

- If the DNS record requires a **Name** value, enter @.

- After saving the DNS entry, in Avaya Cloud Services, click **Verify**.

Next steps

- Go to [Obtain the domain API Key and Key Secret](#) on page 54.

Related links

[Configuring Avaya Cloud Services support](#) on page 51

Obtain the domain API Key and Key Secret

Connections between the IP Office and Avaya Cloud Services require a domain API key and secret. You must obtain these from Avaya Cloud Services and enter them into the IP Office security settings.

Before you begin

- Verify the customer domain. See [Verifying the company domain](#) on page 52.

Procedure

- Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
- Click on **Manage Companies** and click on the existing company name.
- Select the **API** tab.
 - If there is an existing key with its **Role** set to `IPOFFICE` key:
 - Click **View/Edit** and use the menu controls to either download the values as a CSV file, or to copy and paste the values to a temporary document on your PC.
 - If there is no existing key with its **Role** set to `IPOFFICE` key:
 - Click **Add API key+**. Set the role to **IPOFFICE** and click **Add API key**.
 - Click **View/Edit** and use the menu controls to either download the values as a CSV file, or to copy and paste the values to a temporary document on your PC.

Next steps

- [Enter the Avaya Cloud Services settings](#) on page 55.

Related links

[Configuring Avaya Cloud Services support](#) on page 51

Enter the Avaya Cloud Services settings



This process sets the base settings for the IP Office servers that should connect to Avaya Cloud Services.

- If supporting multi-site network, you must do this configuration on each server configured as a SIP registrar.
- Includes the secondary server to support users registered to the primary server during resilience.

Before you begin

- Obtain the API key and secret (see [Obtain the domain API Key and Key Secret](#) on page 54).

Procedure

1. Login to the IP Office using IP Office Web Manager to edit the configuration settings. Using IP Office Web Manager provides access to additional controls to ease configuration.
2. Select **Security > Security Settings**.
 - If configuring servers in a multi-site network, click on the  icon next to the required server.
3. Select **System**.
4. In the **AVAYA SPACES KEYS** section, enter the **Avaya Spaces API Key** and **Avaya Spaces Key Secret** values.
5. Click **Update**.
6. Select **System Settings > System**.
 - If configuring servers in a multi-site network, click on the  icon next to the required server.
7. Select **Avaya Cloud Services**.
8. Enter a name for **Profile Name**.
 - If using a single IP Office server for client connections, this value is for information only.
 - If using several IP Office servers, users see this value when registering their Avaya Workplace Client and use it to select the required IP Office.
9. Select **Enable Avaya Cloud Account**.

10. Check the **Account URL** matches the appropriate value below:
 - IP500 V2 = `accounts-ipo.avayacloud.com`
 - Linux-based Server = `accounts.avayacloud.com`
11. Enter the **Company Domain** verified with Avaya Cloud Services.
12. Click **Update**.
13. Select the **Solution** tab.

Next steps



- Repeat the process for any other servers configured as SIP registrars in the network.
- Configure the required Avaya Cloud Services feature:
 - [Configuring Avaya Cloud Services synchronization](#) on page 57
 - [Configuring SSO login support](#) on page 64
 - [Enabling Apple Push Notifications](#) on page 67
 - [Supporting Spaces Calling](#) on page 76

Related links

[Configuring Avaya Cloud Services support](#) on page 51

Updating the Avaya Workplace clients

Enabling **Enable Avaya Cloud Account** changes the contents of the auto-generated `46xxsettings.txt` file provided by the IP Office system.

- To apply the new settings to existing Avaya Workplace Client applications:
 - By default, the clients regularly update using the `SETTINGS_CHECK_INTERVAL` setting. The IP Office auto-generated `46xxsettings.txt` file uses the default of 1 day.
 - Otherwise, to force an update:
 - **For desktop clients:** Click the  icon and select **Support**. Then click **Check for Updates**.
 - **For mobile clients:** Click the  icon and select **Exit**. Then restart the application.

Settings file change details

Enabling **Enable Avaya Cloud Account** makes the following change to the auto-generated `46xxsettings.txt` file:

- The `SET ENABLE_AVAYA_CLOUD_ACCOUNT 0` string changes to `SET ENABLE_AVAYA_CLOUD_ACCOUNT 1`.

Related links

[Configuring Avaya Cloud Services support](#) on page 51

Chapter 13: Configuring Avaya Cloud Services synchronization

The IP Office can share details of users with a **Unique Identity** (email address) with Avaya Cloud Services. Those users can then:

- Login to and use Avaya Spaces.
 - From February 2025, Avaya Spaces for meetings and conferences is no longer available for new customers. It is supported for existing customers until the end of their existing contract.
- Register Avaya Workplace Client using their **Unique Identity** email address.
 - Not supported with IPv6.

Related links

[Avaya Cloud Services synchronization checklist](#) on page 57

[IP Office user configuration for Avaya Cloud Services](#) on page 58

[Adding the synchronization application](#) on page 58

[Enabling Avaya cloud services user synchronization](#) on page 59

[Enabling Avaya Cloud Services profile synchronization](#) on page 60

[Checking the Avaya Cloud Services Users](#) on page 61

[Using Avaya Cloud Services as the IP Office instant messaging server](#) on page 61

[Set the Avaya Cloud Services user policy](#) on page 62

Avaya Cloud Services synchronization checklist

#	Action	Link/Notes	✓
1.	Configure Avaya Cloud Services support.	• See Configuring Avaya Cloud Services support on page 51.	
2.	Configure the IP Office users.	• See IP Office user configuration for Avaya Cloud Services on page 58.	
3.	Add the cloud services application.	• See Adding the synchronization application on page 58.	

Table continues...

#	Action	Link/Notes	✓
4.	Enable automatic user synchronization.	• See Enabling Avaya cloud services user synchronization on page 59.	
5.	Enable automatic IP Office profile creation.	• See Enabling Avaya Cloud Services profile synchronization on page 60.	
5.	Check the synchronization operation.	• See Checking the Avaya Cloud Services Users on page 61.	

Related links

[Configuring Avaya Cloud Services synchronization](#) on page 57

IP Office user configuration for Avaya Cloud Services

You must complete the following IP Office user configuration before enabling user synchronization.

Before you begin

- See [Avaya Cloud Services synchronization checklist](#) on page 57.

Procedure

The user configuration must include the user's **Unique Identity** email address. This is used as follows:

- Automatic synchronization includes users with a **Unique Identity**.
- Avaya cloud services sends the user a welcome email.
- The user can use the email address for their initial Avaya Workplace Client registration.

Next steps

- See [Adding the synchronization application](#) on page 58.

Related links

[Configuring Avaya Cloud Services synchronization](#) on page 57

Adding the synchronization application

Before you begin

- See [IP Office user configuration for Avaya Cloud Services](#) on page 58.

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.

2. Click on **Manage Companies** and click on the existing company name.
3. Select the **Apps** tab.
4. Click **Configure New App+**.
5. From the **Product** drop-down, select **Equinox Cloud Client**.
6. The IP Office automatically adds the JSON settings after you have completed configuration.
7. Click **Save**,

Next steps

- See [Enabling Avaya cloud services user synchronization](#) on page 59.

Related links

[Configuring Avaya Cloud Services synchronization](#) on page 57


Enabling Avaya cloud services user synchronization

This process enables automatic synchronization of IP Office users with a **Unique Identity** with users in Avaya Cloud Services.

Before you begin

- See [Adding the synchronization application](#) on page 58.

Procedure

1. Login to the IP Office using IP Office Web Manager to edit the configuration settings. Using IP Office Web Manager provides access to additional controls to ease configuration.
2. Select **System Settings > System**.
 - If configuring servers in a multi-site network, click on the  icon next to the required server.
3. Select **Avaya Cloud Services**.
4. To perform a manual check of the connection to Avaya Cloud Services:
 - a. Select **Manual user sync**.
 - b. Click **Refresh**.
 - c. Return to the menu. After a few minutes, the **Synchronization status** shows if the synchronization was successful.
5. If the synchronization was successful, select **Enable user sync** to have future synchronization performed automatically.
6. Click **Update**.

Next steps

- See [Enabling Avaya Cloud Services profile synchronization](#) on page 60.

Related links

[Configuring Avaya Cloud Services synchronization](#) on page 57

Enabling Avaya Cloud Services profile synchronization

You need to configure Avaya Cloud Services with the file path to the `46xxsettings.txt` of each IP Office that is acting as a SIP registrar for Avaya Workplace Client users.

- Using this process, you can configure the IP Office to automatically send it **SIP Registrar FQDN** and **Profile Name** settings to Avaya Cloud Services.
- Avaya Cloud Services use the values to write a profile for the IP Office that includes the profile name and a URL for the `46xxsettings.txt` file.


Adding that information, allows Avaya Workplace Client users to register their client using their **Unique Identity** email address.

- The user enters their email address when prompted by Avaya Workplace Client.
- Avaya Workplace Client connects to Avaya Cloud Services which matches the email address to the customer domain and to a user.
- If there are multiple IP Office profiles, the user selects from the list of available profile names.
- Avaya Cloud Services provides Avaya Workplace Client with the file path for the settings file for the matching IP Office.

Before you begin

- See [Enabling Avaya cloud services user synchronization](#) on page 59.

Procedure

1. Login to the IP Office using IP Office Web Manager to edit the configuration settings. Using IP Office Web Manager provides access to additional controls to ease configuration.
2. Select **System Settings > System**.
 - If configuring servers in a multi-site network, click on the  icon next to the required server.
3. Select **Avaya Cloud Services**.
4. Set the **Enable Settings file URL sync** value to one of the following values. Settings file synchronization writes the IP Office profile name and SIP Registrar FQDN details into the Avaya Cloud Services app profile.
 - **Enable for current IP Office node** - Automatically write profile details for just this IP Office system.

- **Enable for all IP Office nodes** - Automatically write profile details for all IP Office systems in the network.

5. Click **Update**.

Related links

[Configuring Avaya Cloud Services synchronization](#) on page 57

Checking the Avaya Cloud Services Users

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. Click on **Manage Companies** and click on the existing company name.
3. Select **Manage Users**.
4. The two lists show the details of synchronized IP Office users:

List	Description
Active Invites	This list shows users who have received their email invitation to use spaces and have confirmed the invitation.
Waiting Confirmation	This list shows users that Avaya Cloud Services has sent a welcome email, but who have not confirmed the invitation.


Related links

[Configuring Avaya Cloud Services synchronization](#) on page 57

Using Avaya Cloud Services as the IP Office instant messaging server

The IP Office can use either Avaya one-X Portal or Avaya Cloud Services as its server for instant messaging.

Procedure

1. Login to the IP Office using IP Office Web Manager to edit the configuration settings. Using IP Office Web Manager provides access to additional controls to ease configuration.
2. Select **System Settings > System**.
 - If configuring servers in a multi-site network, click on the  icon next to the required server.
3. Select **System**.
4. Change the **Messaging Server** setting to the required value.

Setting	Description
one-X Portal	<p>Use the system's Avaya one-X Portal server for instant messaging between IP Office clients, including Avaya Workplace Client.</p> <ul style="list-style-type: none"> User's must register directly to the IP Office system. This method is not supported for Avaya Workplace Client users logging in using SSO or email.
Avaya Spaces	<p>Use Avaya Cloud Services for instant messaging for Avaya Workplace Client users and other Avaya Cloud Services clients. It does not include non-Avaya Cloud Services users and clients.</p> <ul style="list-style-type: none"> This requires the IP Office to be configure to support Avaya Cloud Services. This method does not support sending push notifications for instant messages. That is, instant messages are not received by iOS clients when the client is suspended or in the background. Not supported with IPv6.

5. Click **Update**.

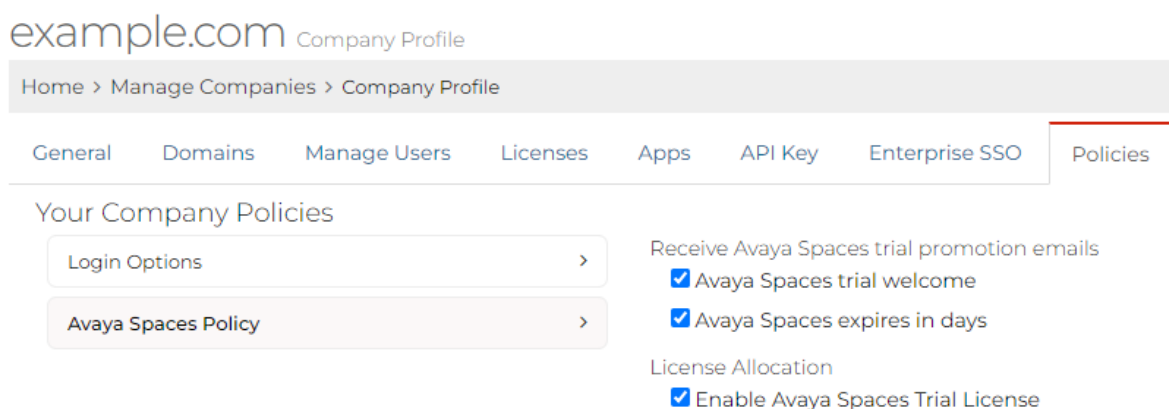
Related links

[Configuring Avaya Cloud Services synchronization](#) on page 57

Set the Avaya Cloud Services user policy

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. Click on **Manage Companies** and click on the existing company name.
3. Select the **Policies** tab.
4. Select **Avaya Spaces Policy**.



5. Select the options which you want enabled for users.
6. Click **Save**,

Related links

[Configuring Avaya Cloud Services synchronization](#) on page 57

Chapter 14: Configuring SSO login support

Using Avaya Cloud Services, you can also configure the IP Office to allow users to login to Avaya Workplace Client using their Google, Office 365, or Salesforce account.

- Not supported with IPv6.

Related links

[SSO/Avaya Cloud authorization checklist](#) on page 64

[Enabling Avaya Cloud authorization](#) on page 64

[Sync the Avaya Cloud Authorization setting](#) on page 65

[Set the Avaya Cloud Services user policy](#) on page 66

SSO/Avaya Cloud authorization checklist

#	Action	Link/Notes	✓
1.	Configure Avaya Cloud Services support.	• See Configuring Avaya Cloud Services support on page 51.	
2.	Enable SSO login support.	• See Enabling Avaya Cloud authorization on page 64.	
3.	Synchronize the setting on all IP Office systems.	• See Enabling Avaya Cloud authorization on page 64.	

Related links

[Configuring SSO login support](#) on page 64

Enabling Avaya Cloud authorization

About this task

This process enables use of client login/registration to the IP Office through Avaya Cloud Services.


- If supporting multi-site network, you must do this configuration on each server configured as a SIP registrar.

- Includes the secondary server to support users registered to the primary server during resilience.

Before you begin

- See [SSO/Avaya Cloud authorization checklist](#) on page 64.

Procedure

1. Login to the IP Office using IP Office Web Manager to edit the configuration settings. Using IP Office Web Manager provides access to additional controls to ease configuration.
2. Select **System Settings > System**.
 - If configuring servers in a multi-site network, click on the  icon next to the required server.
3. Select **Avaya Cloud Services**.
4. Select **Enable Avaya Cloud Account Authorization**.
5. Click **Update**.

Next steps

- Repeat the process for any other servers configured as SIP registrars in the network.
- See [Sync the Avaya Cloud Authorization setting](#) on page 65.

Related links

[Configuring SSO login support](#) on page 64

Sync the Avaya Cloud Authorization setting

About this task

For servers in a multi-site network (not SCN), you can use IP Office Web Manager to ensure that all servers are set to the same **Enable Avaya Cloud Account Authorization**.

Before you begin

- See [Enabling Avaya Cloud authorization](#) on page 64.

Procedure

1. Login to the IP Office using IP Office Web Manager to edit the configuration settings. Using IP Office Web Manager provides access to additional controls to ease configuration.
2. Select the **Solution** tab.
3. Select the servers in the network on which you want to replicate the primary server setting.
4. Click **Actions > Synchronize Single Sign-On configuration**.
5. Click **OK**.

Related links

[Configuring SSO login support](#) on page 64

Set the Avaya Cloud Services user policy

If required, you can restrict the types of account that users can use for SSO. By default, Avaya Cloud Services allows all.

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. Click on **Manage Companies** and click on the existing company name.
3. Select the **Policies** tab.
4. Select **Avaya Spaces Policy**.

Home > Manage Companies > Company Profile

General Domains Manage Users Licenses Apps API Key Enterprise SSO Policies

Your Company Policies

Login Options >

Avaya Spaces Policy >

Allowed login methods

- ☒ Allow All
- ☒ Native login
- ☒ Google Single Sign On
- ☒ Salesforce Single Sign On
- ☒ Office365 Single Sign On
- ☒ Avaya Single Sign On
- ☒ Enterprise SSO

Allowed emails with the following domains can be added into our account.

☐ Allow All

Enter a valid domain to whitelist Add +

Allowed Domains:
example.com

5. Select the options which you want enabled for users.
6. Click **Save**,

Related links

[Configuring SSO login support](#) on page 64

Chapter 15: Enabling Apple Push Notifications

The IP Office can use Apple Push Notification Service (APNS) to send push notifications to Avaya Workplace Client users on iOS devices. If iOS has suspended the client, the user can use controls in the notification to restart the client.

- The IP Office will send push notifications for new calls and for new voicemail messages.
- If using the Avaya one-X Portal as its messaging server, the IP Office will also send push notifications for instant messages.

Related links

[Push notification routing](#) on page 67

[Push notification notes](#) on page 69

[Checklist for configuring push notification support](#) on page 69

[Checking the Avaya Cloud Services timezone](#) on page 70

[Adding the push notification application](#) on page 71

[Enabling Avaya Push Notification Services](#) on page 71

[Synchronizing the enable Apple Push Notifications setting](#) on page 72

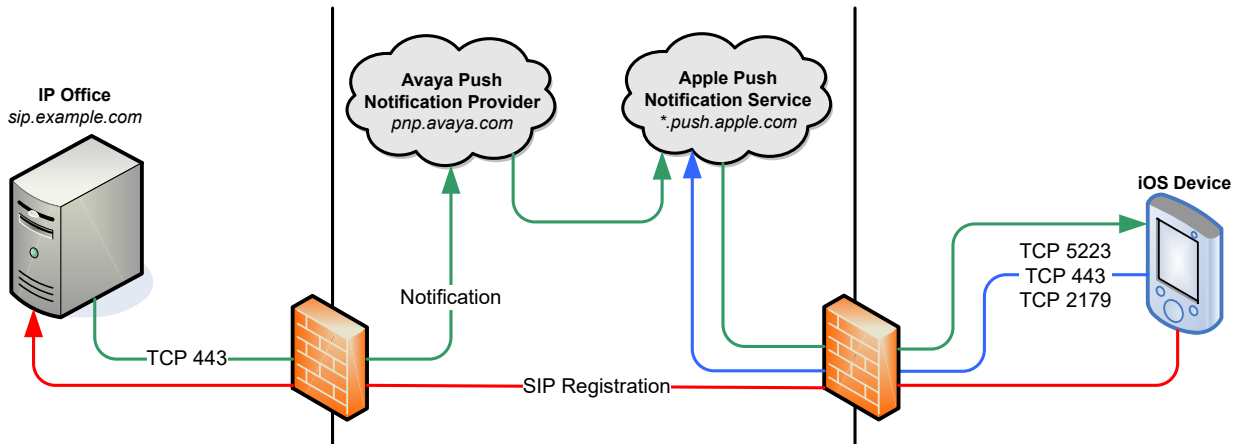
[Synchronizing the Avaya Cloud Services API settings](#) on page 73

[Altering IP Office user and group settings for APNS](#) on page 74

[Updating the Avaya Workplace clients](#) on page 74

Push notification routing

The following diagram summarizes the connections involved in Apple push notifications.



- The IP Office sends push notifications to the Avaya Push Notification Provider (PNP) at `pnp.avaya.com`. It does that using HTTPS and port 443. For scenarios with an ASBCE, the push notifications are not routed through the ASBCE.
- Avaya PNP forwards the push notifications to the Apple Push Notification Service (APNS) at `*.push.apple.com`.
- APNS forward the push notifications to the iOS devices.
- Call details in the push notifications are encrypted end-to-end.

iOS device ports

To support push notifications, the iOS devices must have outgoing access to the following ports and internet addresses.

Ports	Addresses
<ul style="list-style-type: none">• TCP port 5223• TCP port 443• TCP port 2179	<ul style="list-style-type: none">• URLs: <code>*.push.apple.com</code>• Address range: <code>17.0.0.0/18</code>. <p>If you cannot enable access to the full address range, ensure the following are accessible:</p> <ul style="list-style-type: none">- <code>17.249.0.0/16</code>- <code>17.252.0.0/16</code>- <code>17.57.144.0/22</code>- <code>17.188.128.0/18</code>- <code>17.188.20.0/23</code>

Related links

[Enabling Apple Push Notifications](#) on page 67

Push notification notes

- IP Office R11.1 and higher supports push notifications with Avaya Workplace Client 3.06 and higher on iOS.
- iOS automatically suspends the Avaya Workplace Client after 3 minutes of inactivity. Users can manually suspend Avaya Workplace Client by putting the application into the background.
- Push notifications do not require the IP Office user to have a **Unique Identity** synchronized with Avaya Cloud Services.
- The IP Office sends push notification to the last iOS device register by a user.
- It can take several seconds to receive a call push notification, restart the suspended client and answer the call. Therefore, Avaya recommend the following changes to IP Office user settings:
 - Increase the user's **No Answer Time** to at least 20 seconds.
 - If the user is a member of any hunt group, increase the group's **Group No Answer Time**.
 - Ensure that the user has an alternate call coverage destination for their **No Answer Time** expiring. For example; voicemail enabled or a forward on no answer number destination.
 - If the user sets the cellular telephone number of their iOS device as their **Mobile Twinning** destination, set their **Mobile Dial Delay** (sec) to at least 10 seconds. This allows time to answer the push notification using a suspended client before the same call then alerts as a cellular call.
- China does not support the iOS CallKit API used for push notifications. In that locale, call notifications do not provide call controls. However, when clicked they will display a menu to answer or decline the call.
- The IP Office does not send push notifications for instant messages.
- The Avaya Workplace Client setting `VOIPCALLINGENABLED` must be set to 1 (prefer Wi-Fi) or 3 (prefer cellular). Using any other value causes incoming calls that the user cannot answer.

Related links

[Enabling Apple Push Notifications](#) on page 67

Checklist for configuring push notification support

#	Action	Link/Notes	✓
1.	Configure Avaya Cloud Services support.	• See Configuring Avaya Cloud Services support on page 51.	

Table continues...

#	Action	Link/Notes	✓
2.	Check the Avaya Cloud Services timezone.	• See Checking the Avaya Cloud Services timezone on page 70.	
3.	Add the APN application to Avaya Cloud Services.	• See Adding the push notification application on page 71.	
4.	Enable Avaya Cloud Account Authorization.	• See Enabling Avaya Cloud authorization on page 64.	
5.	Enable APNS on the IP Office system.	• See Enabling Avaya Push Notification Services on page 71.	
6.	For a multi-site network (non-SCN), synchronize the settings on the other servers.	See: • Synchronizing the enable Apple Push Notifications setting on page 72. • Synchronizing the Avaya Cloud Services API settings on page 73	
7.	Adjust the IP Office user and group settings.	• See Altering IP Office user and group settings for APNS on page 74.	
8.	Update the Avaya Workplace Client applications.	• See Updating the Avaya Workplace clients on page 74.	

Related links

[Enabling Apple Push Notifications](#) on page 67

Checking the Avaya Cloud Services timezone

About this task

The time zone setting used by Avaya Cloud Services administration and the IP Office system must match.

Before you begin

- See [Checklist for configuring push notification support](#) on page 69.

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. Click on your name top-right and click on **User Settings**.
3. Check that the **Time Zone** matches the timezone of the primary IP Office system.
4. Click **Save**,

Next steps

- Add the push notification application. See [Adding the push notification application](#) on page 71.

Related links

[Enabling Apple Push Notifications](#) on page 67

Adding the push notification application

About this task

To support push notifications, you must add the **Avaya Mobile Push Notification Service** application to the customer domain in Avaya Cloud Services.

Before you begin

- Check the Avaya Cloud Services administrator timezone. See [Checking the Avaya Cloud Services timezone](#) on page 70.

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. Click on **Manage Companies** and click on the existing company name.
3. Select the **Apps** tab.
4. Click **Configure New App+**.
5. From the **Product** drop-down, select **Avaya Mobile Push Notification Service**.
 - The IP Office automatically adds the JSON profile settings to the application after configuration is complete.
6. Click **Save**,

Next steps

- Enable push notifications from the IP Office. See [Enabling Avaya Push Notification Services](#) on page 71.

Related links

[Enabling Apple Push Notifications](#) on page 67

Enabling Avaya Push Notification Services

About this task


This process enables IP Office support for push notifications.

- The process also alters the auto-generated `46xxsettings.txt` file provide to Avaya Workplace Client users. To apply the new settings to the clients, either reregister the clients or wait 24-hours.

Before you begin

- Add the push notification application. See [Adding the push notification application](#) on page 71.

Procedure

1. Login to the IP Office using IP Office Web Manager to edit the configuration settings. Using IP Office Web Manager provides access to additional controls to ease configuration.
2. Select **System Settings > System**.
 - If configuring servers in a multi-site network, click on the  icon next to the required server.
3. Select **Avaya Push Notification Services**.
4. Select **Enable Apple Push Notification Services**.
 - Enabling this setting causes the IP Office to generate a hidden **System-ID** value. Servers in a multi-site network (non-SCN) must all use the same **System-ID** value. You can ensure that using the **Actions > Synchronize APNS configuration** command and then the **Actions > Synchronize APNP System-ID** command after configuring the primary server.
5. The other settings are for information only. You cannot change them.
6. Click **Update**.

Next steps

- If configuring a multi-site network (not SCN), enable push notifications on any other IP Office servers that are acting as SIP registrars for iOS Avaya Workplace Client users. See [Synchronizing the enable Apple Push Notifications setting](#) on page 72.
- Also do the above if using a secondary server for resilience, include that server.
- Otherwise, see [Altering IP Office user and group settings for APNS](#) on page 74.

Related links

[Enabling Apple Push Notifications](#) on page 67

Synchronizing the enable Apple Push Notifications setting

About this task

This process shares the primary IP Office server's **Enable Apple Push Notification Services** settings the selected IP Office servers.

Before you begin

- Add the push notification application. See [Adding the push notification application](#) on page 71.

Procedure

1. Login to the IP Office using IP Office Web Manager to edit the configuration settings. Using IP Office Web Manager provides access to additional controls to ease configuration.
2. Select the **Solution** tab.
3. Select the servers in the network on which you want to replicate the primary server setting.
4. Click **Actions > Synchronize APNS configuration**.
5. Click **OK**.

Next steps

- See [Synchronizing the Avaya Cloud Services API settings](#) on page 73.

Related links

[Enabling Apple Push Notifications](#) on page 67

Synchronizing the Avaya Cloud Services API settings

This process shares the primary IP Office server's **System-ID**, **Avaya Spaces API Key** and **Avaya Spaces Key Secret** values with the selected IP Office servers.

- The **System-ID** is a hidden value generated by an IP Office when the **Enable Apple Push Notification** setting is enabled.

Before you begin

- Ensure that **Enable Apple Push Notification Services** has been enabled on each server. See [Synchronizing the enable Apple Push Notifications setting](#) on page 72.

Procedure

1. Access the configuration of the IP Office system that will be performing the user sync.
2. Select the **Solution** tab.
3. Select the servers in the network on which you want to replicate the primary server setting.
4. Click **Actions > Synchronize APNP System-ID**.
5. Click **OK**.

Next steps

- See [Altering IP Office user and group settings for APNS](#) on page 74.

Related links

[Enabling Apple Push Notifications](#) on page 67

Altering IP Office user and group settings for APNS

About this task

It can take several seconds to receive a call push notification, restart the suspended client and answer the call. Therefore, Avaya recommend the following changes to IP Office user settings:

Before you begin

- See [Synchronizing the Avaya Cloud Services API settings](#) on page 73.

Procedure

1. Login to the IP Office to edit the configuration settings.
2. Make the following configuration changes:
 - Increase the user's **No Answer Time** to at least 20 seconds.
 - If the user is a member of any hunt group, increase the group's **Group No Answer Time**.
 - Ensure that the user has an alternate call coverage destination for their **No Answer Time** expiring. For example; voicemail enabled or a forward on no answer number destination.
 - If the user sets the cellular telephone number of their iOS device as their **Mobile Twinning** destination, set their **Mobile Dial Delay** (sec) to at least 10 seconds. This allows time to answer the push notification using a suspended client before the same call then alerts as a cellular call.

Next steps



- See [Updating the Avaya Workplace clients](#) on page 74.

Related links

[Enabling Apple Push Notifications](#) on page 67

Updating the Avaya Workplace clients

Enabling **Enable Apple Push Notification Services** changes the contents of the auto-generated `46xxsettings.txt` file provided by the IP Office system.

- To apply the new settings to existing Avaya Workplace Client applications:
 - By default, the clients regularly update using the `SETTINGS_CHECK_INTERVAL` setting. The IP Office auto-generated `46xxsettings.txt` file uses the default of 1 day.
 - Otherwise, to force an update:
 - **For desktop clients:** Click the  icon and select **Support**. Then click **Check for Updates**.
 - **For mobile clients:** Click the  icon and select **Exit**. Then restart the application.

Settings file change details

Enabling **Enable Apple Push Notification Services** makes the following changes to the auto-generated `46xxsettings.txt` file:

- The `SET PUSH_NOTIFICATION_ENABLED 0` string changes to `SET PUSH_NOTIFICATION_ENABLED 1`.
- The IP Office adds a `SET TELEPHONY_PUSH_NOTIFICATION_SERVICE_URL` string using the IP Office system's **SIP Registrar FQDN** value. For example:
 - `SET TELEPHONY_PUSH_NOTIFICATION_SERVICE_URL "https://sip.example.com:443/PushNotification"`
 - The port used changes to 411 if **Use Preferred Phone Ports** is enabled.

Related links

[Enabling Apple Push Notifications](#) on page 67

Chapter 16: Supporting Spaces Calling

Spaces calling lets users make and receive IP Office calls through Avaya Cloud Services.

IP Office Support	IP Office R11.1 FP1 SP1 and higher.
User Clients	<p>Users can make and answer calls using the following clients. The client supported is configurable for the customer installation.</p> <ul style="list-style-type: none">• Spaces Calling Extension - This is a Google Chrome extension which uses WebRTC.• Avaya Workplace - Version 3.16 and higher. This client uses SIP for calls.
one-X Portal	<p>The following features require the IP Office system to include a one-X Portal server:</p> <ul style="list-style-type: none">• Chrome Extension - WebRTC for calls using the Chrome extension requires the Avaya one-X Portal. It also requires the WebRTC Gateway service on the same server.<ul style="list-style-type: none">- The IP Office supports resilience on networks with a secondary Avaya one-X Portal.- IP500 V2 systems must use an IP Office Application Server for Avaya one-X Portal and WebRTC.• SSO - Single sign-on support through either of the clients.
Remote Clients	<p>For user connections from remote clients:</p> <ul style="list-style-type: none">• You must route all connections through the customer firewall or an ASBCE.• DNS must resolve all external and internal addresses as required.

Related links

[IP Office Components for Spaces Calling](#) on page 77

[Spaces Calling Limitations](#) on page 77

[Spaces Calling Chrome Extension Schematic](#) on page 77

[Spaces Calling Workplace Client Schematic](#) on page 78

[Spaces Calling Native Remote Worker](#) on page 79

[Spaces Calling Remote Worker Using an ASBCE](#) on page 80

[Spaces Calling Licensing](#) on page 81

[Checklist for configuring Spaces Calling with IP Office](#) on page 81

[Enabling Spaces Calling Support for the Customer Domain](#) on page 82

[Setting the Preferred Spaces Calling Clients](#) on page 85

[Installing the Spaces Calling Extension](#) on page 86

[Blank Calling Extension/Enabling Third-Party Cookies](#) on page 87

[Change the Spaces Calling Client](#) on page 87

[Getting the Chrome Extension Logs](#) on page 88

[Manually Adding a User Phone Number](#) on page 88

IP Office Components for Spaces Calling

Support for Space Calling requires the following IP Office components:

Feature	Component
Spaces Calling	IP Office R11.1 FP1 SP1 or higher.
... with Workplace client	Avaya Workplace Client R3.16 and higher.
... with SSO login	Avaya one-X Portal
... with Chrome extension	Avaya one-X Portal and WebRTC Gateway

Related links

[Supporting Spaces Calling](#) on page 76

Spaces Calling Limitations

The following known limitations apply for Spaces Calling operation in conjunction with IP Office:

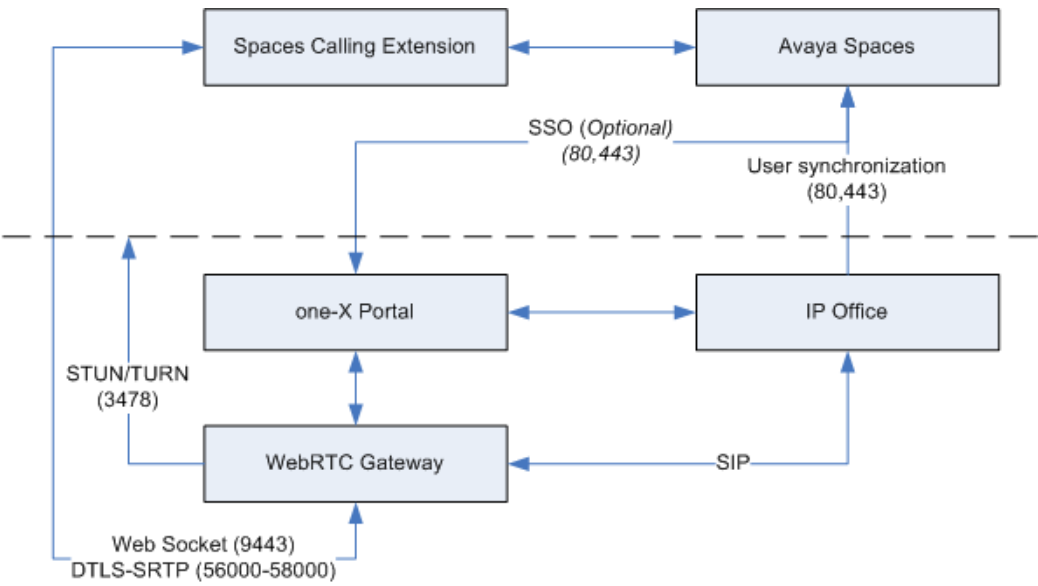
- The directory shown for the Chrome extension is local to the Chrome extension. It does not include the IP Office user and system directory entries.
- The call log shown for the Chrome extension is local to the Chrome extension. It does not include the user's calls made with other IP Office devices.
- The Chrome extension directory only shows and allows calls to IP Office users with a **Unique Identity**. Therefore, Avaya recommended you configure a **Unique Identity** for all IP Office users. That gives all users a free basic account unless specifically licensed for other features.
- The Avaya Workplace Client and Avaya Spaces user presence values do not match.

Related links

[Supporting Spaces Calling](#) on page 76

Spaces Calling Chrome Extension Schematic

The following is a simple schematic of the connections when using the Chrome extension for calls.



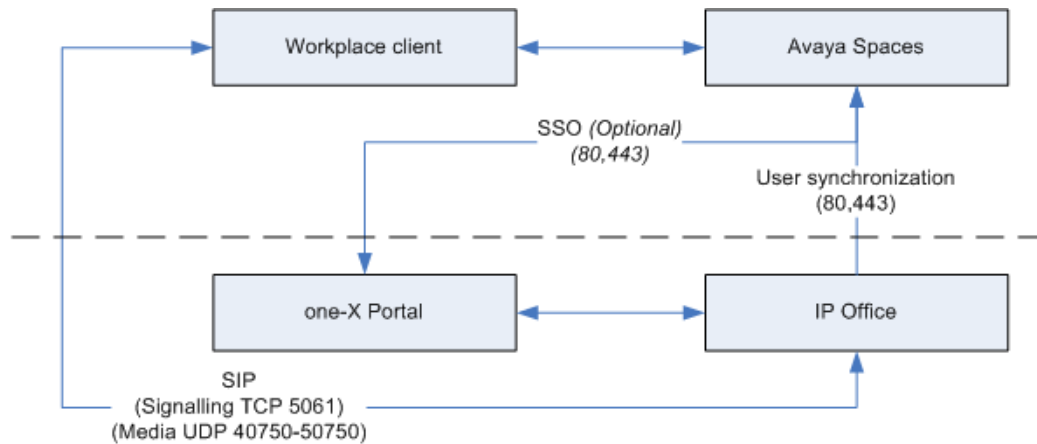
Port	Destination/Description
80, 443	User synchronization operation. SSO operation if enabled.
3478	STUN/TURN connection from WebRTC Gateway service to STUN/TURN server. This can be the STUN service on ASBCE.
9443	Websocket connection to the IP Office WebRTC Gateway service running on the same server as the one-X Portal service.
56000 to 58000	WebRTC call media from the Chrome extension to the IP Office WebRTC Gateway service.

Related links

[Supporting Spaces Calling](#) on page 76

Spaces Calling Workplace Client Schematic

The following is a simple schematic of the connections when using a Workplace client for calls.



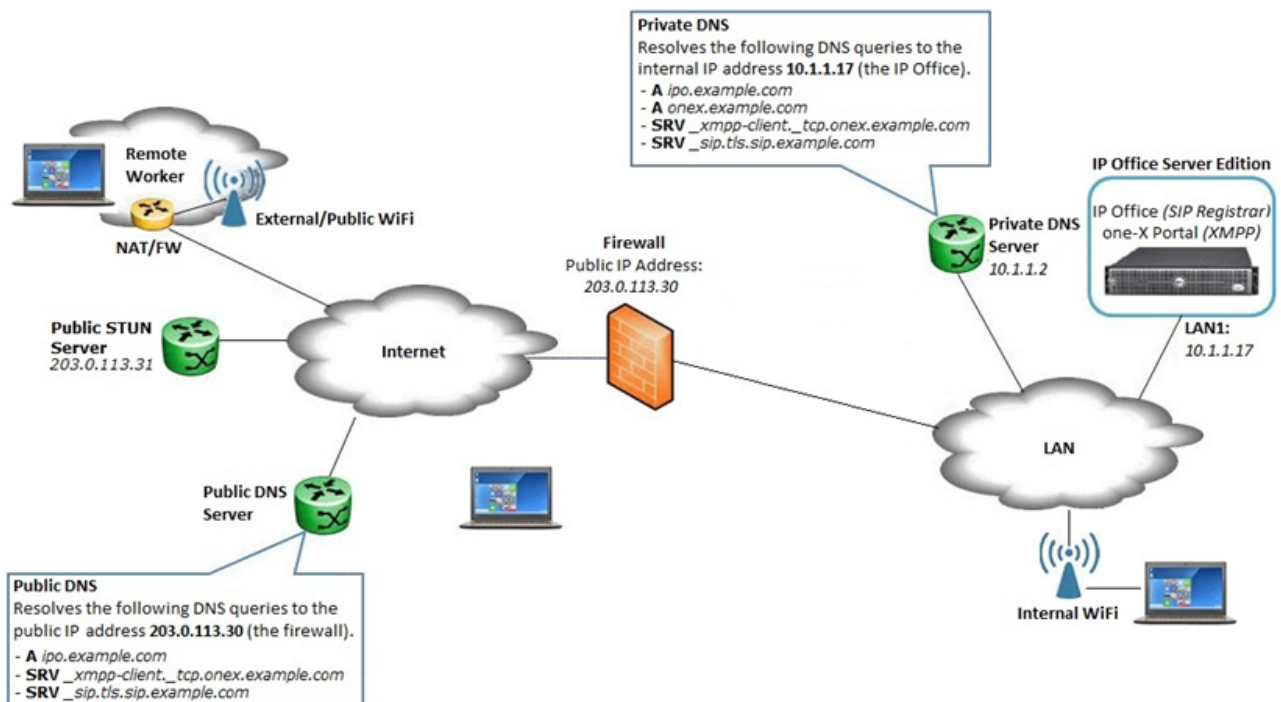
For details of the ports used by the Workplace client, see [Workplace Ports](#) on page 15.

Related links

[Supporting Spaces Calling](#) on page 76

Spaces Calling Native Remote Worker

This diagram is an example for supporting native remote workers.



You must configure the enterprise firewall to:

- Allow Layer 3 NAT only.

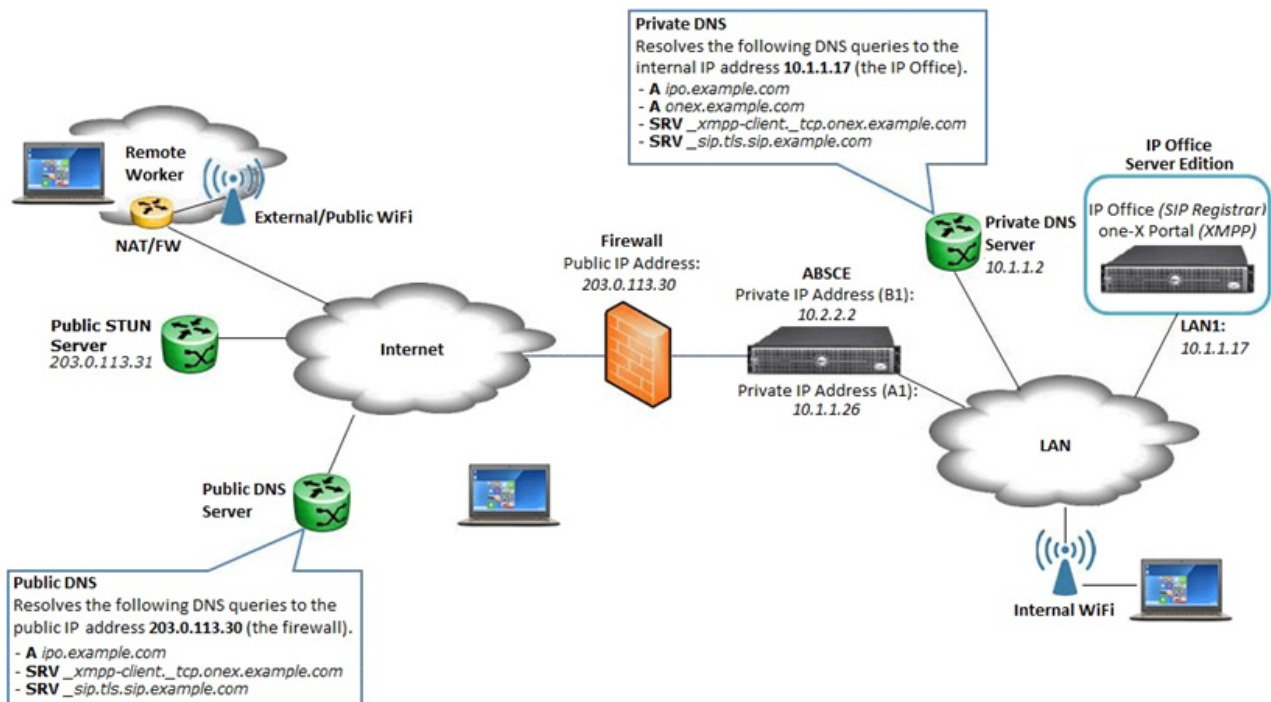
- Disable all SIP aware functionality such as ALG.
- Forward the TCP signaling ports (by default 9443) to IP Office Server Edition system.
- Forward the RTP ports (by default 56000 to 58000) to IP Office Server Edition system.

Related links

[Supporting Spaces Calling](#) on page 76

Spaces Calling Remote Worker Using an ASBCE

The diagram below is an example for supporting remote workers with an ASBCE.



You must configure the enterprise firewall to:

- Allow Layer 3 NAT only.
- Disable all SIP aware functionality such as ALG.
- Forward the TCP signaling ports (by default 9443) to IP Office Server Edition.
- Forward the RTP ports (by default 56000 to 58000) to IP Office Server Edition.

You must configure the ASBCE with:

- An application relay for connections to port 9443 on the portal server.
- STUN and TURN for media relay and NAT resolution to the WebRTC Gateway service

You must configure the WebRTC Gateway with:

- TURN support using the ASBCE for Media Relay.
- Public FQDN/IP Address of the firewall address as **STUNHost**. WebRTC Clients without **STUNHost** configuration initialize using this address.

Configure split DNS entries for the ASBCE FQDN. For the **STUNHost**, the address must resolve to:

- **Public DNS:** The public FQDN/IP address of the enterprise firewall which routes to the external interface of the ASBCE.
- **Private DNS:** The internal interface of the ASBCE.

Related links

[Supporting Spaces Calling](#) on page 76

Spaces Calling Licensing

The IP Office supports Spaces Calling for users with the following IP Office user licenses:

System		System License	User License
Subscription System		–	Unified Communications User
Non-Subscription	Server Edition	–	Power User or Office Worker
	IP500 V2	Preferred Edition	Power User, Office Worker or Teleworker

Related links

[Supporting Spaces Calling](#) on page 76

Checklist for configuring Spaces Calling with IP Office

#	Action	Link/Notes	✓
1.	Configure Avaya Cloud Services support.	• See Configuring Avaya Cloud Services support on page 51.	
2.	Configure IP Office user synchronization.	• See Configuring Avaya Cloud Services synchronization on page 57.	
3.	Enable Spaces Calling support for the customer domain.	• Enabling Spaces Calling Support for the Customer Domain on page 82	

Table continues...

#	Action	Link/Notes	✓
4.	Set the preferred Spaces Calling clients.	• Setting the Preferred Spaces Calling Clients on page 85	
5.	Install the Spaces Calling extension.	• Installing the Spaces Calling Extension on page 86	

Related links

[Supporting Spaces Calling](#) on page 76

Enabling Spaces Calling Support for the Customer Domain

This process adds details of the IP Office system address for Spaces Calling plus additional settings for how Spaces Calling should operate.

Before you begin

- See [Checklist for configuring Spaces Calling with IP Office](#) on page 81.

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. Click on **Manage Companies** and click on the existing company name.
3. Select the **Apps** tab.
4. Click **Configure New App+**.
5. From the **Product** drop-down, select **Avaya Spaces Calling Extension**.
6. Select **JSON**.
7. In the text box, enter the details for the IP Office system. For details of the options, see [Spaces Calling Profile Settings](#) on page 83.
 - You must enclose setting names and values in " " quote marks and separated by : colon. For example: "Name": "server.example.com".
 - The exception to the above are the `true` and `false` values. Do not enclose those values in " " quote marks.
 - You must follow each setting and value pair with a comma, except for the last pair.

For example:

- **Single Login System:**

```
{
  "IP_Office_Server_Profile":
  [{
    "Name": "Head Office",
    "Address": "primary.example.com",
    "AccountsToken": true
  ]
}
```

```
    }
  }
}
```

- **Multiple Login Systems:**

If required, you can list multiple systems in the network. In that case, when logging in, the client prompts the user to select the required system.

```
{
  "IP_Office_Server_Profile":
  [{
    "Name": "West",
    "Address": "west.example.com",
    "AccountsToken": true
  },
  {
    "Name": "East",
    "Address": "east.example.com",
    "AccountsToken": true
  }]
}
```

8. Click **Save**,

Next steps

- Having configured the profile settings, enable Spaces Calling. See [Setting the Preferred Spaces Calling Clients](#) on page 85.

Related links

[Supporting Spaces Calling](#) on page 76

[Spaces Calling Profile Settings](#) on page 83

Spaces Calling Profile Settings

You can use the following settings in the profiles you create for Spaces Calling. See [Enabling Spaces Calling Support for the Customer Domain](#) on page 82.

Connection Settings

Each profile must include values for the following settings:

Setting	Description
Name	This is the name of the profile. If you add multiple profiles, users will see and select the name during login. Maximum 14 characters. For example: "Name": "Office"
Address	Set to match to the address of the IP Office server. For example: "Address": "ipoffice.example.com" <ul style="list-style-type: none"> • For access from both internal and public networks, this FQDN should resolve to the ASBC public address (B1) on public DNS, and ASBC internal address (A1) on internal DNS.

Table continues...

Setting	Description
AccountsToken	This setting controls whether the Chrome extension can use SSO login features: <ul style="list-style-type: none"> • "AccountsToken": true enables SSO login. • "AccountsToken": false disables SSO login.
LogDownload	This setting controls whether users can download extension logs from their Chrome extension. See Getting the Chrome Extension Logs on page 88. <ul style="list-style-type: none"> • "LogDownload": true enables log downloads. • "LogDownload": false disables log downloads.
STUNHost	The address of the STUN host used for WebRTC. For example, "STUNHost": "absce.example.com" <ul style="list-style-type: none"> • For access from both internal and public networks, the FQDN must resolve to the ASBCE public address on public DNS, and ASBCE internal address on internal DNS.
STUNPort	The standard STUN port is 3478. For example: "STUNPort": "3478"
AutoFailover	This setting controls whether the client should use the IP Office resiliency features: <ul style="list-style-type: none"> • If set to "AutoFailover": true, the client will login to the secondary one-X Portal server when the primary one-X Portal is not available. • If set to "AutoFailover": false or not set, the client will not use resiliency.
DialRule	This settings controls how the dialing rules used by the Chrome extension are determined: <ul style="list-style-type: none"> • "DialRule": false enables users to configure their dialing rules in the Spaces Calling extension settings. • "DialRule": true uses the dialing rules defined by the settings in the table below. • Not including DialRule setting disabled dial rules.

Dialing Settings

If you include "DialRule": true in a profile, you can also use the following additional settings.

Setting	Description
OutsidePrefix	Set to match the prefix used on the telephone system for outgoing external calls. For example: "OutsidePrefix": "9"
CountryCode	Set to match the country code for call. For example: "CountryCode": "1" or "CountryCode": "44"
CityCode	Set to the match the area code for the profile users. If the profile covers multiple areas, you can use a common separated list of codes. For example: "CityCode": "555" or "CityCode": "555,777"
PbxPrefix	If the telephone system has its own prefix within a network, specify the prefix.

Table continues...

Setting	Description
LongDistancePrefix	Specify the prefix added to external calls to indicate national (non-local) numbers. In North America this is usually 1. For example: "LongDistancePrefix": "1"
InternationalPrefix	Specify the prefixed added to eternal calls to indicate international numbers. In North America this is usually 011. For example: "InternationalPrefix": "011"
ExtensionLength	Specify the length of internal extension numbers. If necessary, you can use a comma separated list. For example: "ExtensionLength": "3,4"
NationalLength	Specify the length on national numbers, including the area code. If necessary, you can use a comma-separated list of lengths. For example: "NationalLength": "10,11"
RemoveAreaCode	In areas that allow local calls without the area code, set this value to <code>true</code> . For example: "RemoveAreaCode": <code>true</code>
ApplyToPlusNumber	Specifies whether the dialing rules apply to + format numbers. For example: "ApplyToPlusNumber": <code>false</code>

Related links

[Enabling Spaces Calling Support for the Customer Domain](#) on page 82

Setting the Preferred Spaces Calling Clients

After you have added profiles for Spaces Calling within the customer domain, you can configure the supported clients.

- If you enable multiple clients, Avaya Spaces prompts the user to select which client they prefer when they first access Spaces Calling. They can change their choice if required. See [Change the Spaces Calling Client](#) on page 87.

Before you begin

- See [Enabling Spaces Calling Support for the Customer Domain](#) on page 82.

Procedure

1. Login to <https://spaces.avayacloud.com/admin/companies>.
2. Select the customer's company.
3. Select **Settings**.
4. Scroll down to the **AVAYA SPACES CALLING** section.
5. Select **Enable Avaya Spaces Calling**.
6. Select which methods you want to allow users to use to make Spaces calls:


Setting	Description
Avaya Spaces Calling Chrome Extension	Use the Chrome extension for Spaces Calling to make and answer calls. This option users WebRTC via the IP Office's WebRTC Gateway and one-X Portal services.
Avaya Workplace Client	User Avaya Workplace Client to make and answer calls. This option uses SIP via the IP Office service.

7. Click **Save**.

Related links

[Supporting Spaces Calling](#) on page 76

Installing the Spaces Calling Extension

Avaya Spaces prompts the user to select the client they want to use when they first click the  icon. Selecting Spaces Calling Extension triggers this process if the user has not already installed the client.

You can also use this process to pre-install the extension.



Before you begin

- You must have configured the extension as a supported client. See [Setting the Preferred Spaces Calling Clients](#) on page 85.

About this task

The process below installs the Spaces Calling Extension into Google Chrome.

Procedure

1. Login into <https://spaces.avayacloud.com/spaces/dashboard>.
2. Click on  **Downloads**.
3. Click on **Avaya Spaces Calling Chrome Extension**. This opens the extensions page in the Chrome web store.
4. Click **Add to Chrome**.
5. Click **Add extension**.
6. When prompted to allow the extension to view your user settings, click **Accept**.
7. When prompted to allow spaces to use your microphone, click **Allow**.
8. If necessary, open <https://spaces.avayacloud.com/spaces/dashboard> again.
9. Click on the  bottom-right and login using your username and password.
 - If single sign-on has been enabled, you can also login using your details for one of the authenticated single sign-on accounts.

- If the pop-up window that appears is blank or contains an error message, allow the extension to store cookies. See [Blank Calling Extension/Enabling Third-Party Cookies](#) on page 87.

Related links

[Supporting Spaces Calling](#) on page 76

Blank Calling Extension/Enabling Third-Party Cookies

The Spaces Calling extension needs to store data using cookies. If the user's browser does not allow this, the Spaces Calling login screen will appear either blank or with an error message. If this happens, you can use the following process to enable the extension.


Procedure

1. Open a new tab in Chrome.
2. Enter `chrome://settings/cookies`
3. If **Block third-party cookies** is enabled, scroll down to the list of **Sites that can always use cookies** section:
4. Add the following string:
 - `chrome-extension://mjpbjjjcphpikgemoglgnmfojppgaklg`

Related links

[Supporting Spaces Calling](#) on page 76

Change the Spaces Calling Client

If you have enabled support for both the Chrome extension and Avaya Workplace Client (see [Setting the Preferred Spaces Calling Clients](#) on page 85), Avaya Spaces prompts the user to select their preferred client when they first click the  icon. Using this process, a user can change their selection.

Procedure

1. Login into <https://spaces.avayacloud.com/spaces/dashboard>.
2. Click on your name and avatar shown top-right.
3. Click **Preferences**.
4. Scroll down to the **AVAYA SPACES CALLING** settings.
5. Select your preferred client:

Setting	Description
Avaya Spaces Calling Chrome Extension	Use the Spaces Calling Extension in Google Chrome to make and answer Spaces Calling calls.
Avaya Workplace Client	User Avaya Workplace Client to make and answer Spaces Calling calls.

6. Close the **Preferences** settings.

Next steps

Related links

[Supporting Spaces Calling](#) on page 76

Getting the Chrome Extension Logs

Chrome can provide logs for the Avaya Spaces Calling extension. You can use these to help resolve user issues.

- Setting the `LogDownload` option to `false` in the profile disables the downloading of logs. By default, the extension allows log downloads.

Before you begin

- Log the user out of the Avaya Spaces Calling extension.

Procedure

1. Within Chrome, select **⋮ > More Tools > Extensions**.
2. Select **Developer mode**.
3. Locate the Avaya Spaces Calling extension and click on the `background.html` link shown next to **Inspect views**. The link opens in a separate **DevTools** window, showing the **Console** tab.
4. Log the user back into Avaya Spaces Calling and perform any required test actions.
5. When completed, in the **DevTools** window, right-click log messages and select **Save as**.
6. Save the log messages to a file.

Related links

[Supporting Spaces Calling](#) on page 76

Manually Adding a User Phone Number

If you have configured automatic integration for the IP Office systems, that automatically transfers IP Office user details and extension numbers.

However, if you are using manual integration, in addition to manually adding users manually you must add the user extension numbers using the process below. You can also use this process to add additional numbers for calls to the user.

- You cannot mix the two modes. If using automatic synchronization, to support the routing calls to numbers other than the user extension numbers, use IP Office features such as mobile twinning, forwarding controls, and so on.

Before you begin

- Add the user details to Avaya Spaces. See [Manually Adding Individual Users](#) on page 92.

Procedure

1. Login into <https://spaces.avayacloud.com/spaces/dashboard>.
2. Click on your name and avatar shown top-right.
3. Select **Profile & Account**.
4. Select **User Settings**.
5. Select the **Phones** tab.
6. Select **Add a phone number** and enter the details for the number.
7. In the list of phone numbers, click **Verify Now**.
8. Select the method by which you want to receive the verification code (a voice call or a text message).
9. Enter the verification code and click **Verify**.

Related links

[Supporting Spaces Calling](#) on page 76

Chapter 17: Manually configuring IP Office/ Avaya Cloud Services details

Automatic synchronization is the recommended method for linking IP Office systems to Avaya Cloud Services (see [Configuring Avaya Cloud Services synchronization](#) on page 57). However, if automatic synchronization is not enabled, you must manually configure Avaya Cloud Services with details of the IP Office systems to which users connect.

- The profile for each IP Office system uses its **Profile Name** and **SIP Registrar FQDN** settings.

Related links

[Adding the IP Office system details](#) on page 90

[Manually Adding Individual Users](#) on page 92

[Manually Importing Multiple Users to Avaya Cloud Services](#) on page 92

Adding the IP Office system details

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. Click on **Manage Companies** and click on the existing company name.
3. Select the **Apps** tab.
4. Click on **Configure New App+**.
5. For the **Product** field select **Equinox Cloud Client**.

6. In the **Public Settings** field, enter the following settings, altered to match the address of the customer's system.

The screenshot shows the Avaya Equinox Cloud Client Application Settings page. The 'Public Settings' field is highlighted, showing a JSON configuration for the Equinox Cloud Client. The configuration includes the Client Settings File Address, Profile Name, and Client Settings File Url.

```

{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "Head Office",
      "Client_Settings_File_Url": "http://ipoffice.example.com/46xxsettings.txt"
    }
  ]
}

```

- **Single Login System:**

```

{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "Head Office",
      "Client_Settings_File_Url": "http://ipoffice.example.com/46xxsettings.txt"
    }
  ]
}

```

- **Multiple Login Systems:** If you specify multiple servers, the client prompts users to select a profile from a drop-down when they login.

```

{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "East",
      "Client_Settings_File_Url": "http://ipoeast.example.com/46xxsettings.txt"
    },
    {
      "Profile_Name": "West",
      "Client_Settings_File_Url": "http://ipowest.example.com/46xxsettings.txt"
    }
  ]
}

```

7. Click **Save**.

Related links

[Manually configuring IP Office/Avaya Cloud Services details](#) on page 90

Manually Adding Individual Users

If not using automatic synchronization, you can manually add individual users.

Before you begin

- You can only use this process after verifying the customer domain (see [Verifying the company domain](#) on page 52) and adding the IP Office details (see [Manually configuring IP Office/Avaya Cloud Services details](#) on page 90).

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. Click on **Manage Companies** and click on the existing company name.
3. Select the **Manage Users** tab.
4. Create an entry for each IP Office user that you want included:
 - Each entry must use an email address which matches the user's **Unique Identity** in the IP Office configuration.

Next steps

- For Avaya Cloud Services users, add the user's extension number. See [Manually Adding a User Phone Number](#) on page 88.

Related links

[Manually configuring IP Office/Avaya Cloud Services details](#) on page 90

Manually Importing Multiple Users to Avaya Cloud Services

If not using automatic synchronization, you can add multiple users by uploading their details as a CSV format text file.

- Using the import tools, you can specify which characters you used as a value separator and which characters you used to surround quoted values. In addition, you can use CSV files with different levels of content.
- The minimum content is a list of user email addresses within the verified domain. However, you can include additional data which Avaya Cloud Services will use to pre-populate the user information. The following are example header rows:

Simple CSV Example	email user1@example.com user2@example.com
Complex CSV Example:	email,firstname,lastname,workphone user1@example.com,teressa,green,123456 user2@example.com,bob,white,654321

The following fields can appear in the header row, with matching data for each user in the following rows. The only required header field is email:

- email - The user's email address (unique identity).
- firstname
- lastname
- middlename
- workphone
- homephone
- cellphone
- language - The user's preferred language using the two-character language and country pairing. For example: en-UK or en-US.
- address
- city
- region
- postal
- country

Before you begin

This process can only be performed once the domain has been verified (see [Verifying the company domain](#) on page 52) and IP Office details added (see [Adding the IP Office system details](#) on page 90).

Procedure

1. Login to Avaya Cloud Services at <https://accounts.avayacloud.com>.
2. Click on **Manage Companies** and click on the existing company name.
3. Select the **Manage Users** tab.
4. Click **Tools** and select **Import From CSV**.
5. Click **Import From CSV**.
6. Select the settings for separator and quoted value characters that match your CSV file format.
7. Click on **Choose file** and select your CSV file.
8. Click **Import**.

Related links

[Manually configuring IP Office/Avaya Cloud Services details](#) on page 90

Part 3: Further Help

Chapter 18: The IP Office Settings Files

The following pages show examples of the IP Office auto-generated files used for SIP extensions, including Avaya Workplace Client.

- You can view an IP Office system's files by entering `https://` followed by the system address, then `/`, and then the file name. For example: `https://192.168.0.42/46xxsettings.txt`
 - Note: Viewing the files in a browser is not supported if the IP Office system has **System > System > Avaya HTTP Clients Only** enabled.
- You can view both auto-generated and static files using the method above.
- Auto-generated files are ephemeral. The IP Office creates the file when requested and deletes it after delivery.
- The existence of a static file overrides creating of an auto-generated file of the same name.
 - For the `46xxsettings.txt` file, Avaya strongly recommend that you let the IP Office auto-generate the file. Avaya recommend that you put any custom settings in a `46xxspecials.txt` file.
- For IP Office operation, Avaya only supports settings listed as supported by IP Office and by the phone/client with which you are using the setting.

How the phones/clients use the settings:

- If a setting is not included in the settings files, the phones or clients assumes the default value.
- If a setting is included in the settings files, the IP phone/client applies the setting if supported.
- If a previously sent setting is removed from subsequent settings files:
 - Phones return to assuming the setting's default value.
 - Clients continue using the previously received setting value. To default settings values used by clients, you must send a settings file containing either the specific default value or " " as an empty value.

Related links

[Workplace 46xxsettings.txt file settings](#) on page 96

[Sample 46xxspecials.txt file](#) on page 98

[User Agent spoofing](#) on page 100

Workplace 46xxsettings.txt file settings

Below is an example auto-generated 46xxsettings.txt file from a IP Office R11.1.3 system. The sections not relevant to Avaya Workplace Client have been removed.

- The sections labeled **AUTOGENERATEDSETTINGS** contain settings that have values that have been automatically adjusted to match the IP Office system's configuration settings. For example:
 - Addresses with ports 80 and 443, are changed to ports 8411 and 411 respectively when the IP Office **User Preferred Phone Ports** setting is enabled.
- The sections after the **NONAUTOGENERATEDSETTINGS** label contain settings which for IP Office operation have set values.
- The \$MODEL4 model values relate to the different versions of Avaya Workplace Client:
 - aca = Android mobile client.
 - aci = iOS mobile client.
 - acm = macOS desktop client.
 - acw = Windows desktop client.

```
## IPOFFICE/11.1.3.1.0 build 28 192.168.0.76 AUTOGENERATED
...
IF $MODEL4 SEQ aca GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aci GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acm GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acw GOTO SIPXAUTOGENERATEDSETTINGS
GOTO NONAUTOGENERATEDSETTINGS
# SIPXAUTOGENERATEDSETTINGS
IF $SIG_IN USE SEQ H323 GOTO 96X1AUTOGENERATEDSETTINGS
SET RTP_PORT_LOW 46750
SET RTP_PORT_RANGE 4002
SET TLSSRVRID 0
SET ENABLE_OPUS 1
SET ENABLE_G722 1
SET ENABLE_G711A 1
SET ENABLE_G711U 1
SET ENABLE_G729 1
SET ENABLE_G726 0
SET DTMF_PAYLOAD_TYPE 101
SET SIPDOMAIN example.com
SET ENFORCE_SIPS_URI 0
SET DSCPAUD 46
SET DSCPSIG 34
SET HTTPPORT 80
SET TRUSTCERTS WebRootCA.pem
SET COUNTRY UK
SET ISO_SYSTEM_LANGUAGE en_GB
IF $MODEL4 SEQ aca GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aci GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acm GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acw GOTO K1EXAUTOGENERATEDSETTINGS
...
# K1EXAUTOGENERATEDSETTINGS
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 1
SET ENABLE_IPO_PORTAL_MESSAGING 1
SET ENABLE_IM 1
SET SIP_CONTROLLER_LIST sip.example.com:5060;transport=tcp
```



```

SET CONFERENCE_FACTORY_URI "ConfServer@example.com"
SET PSTN_VM_NUM "VM.user@example.com"
SET SETTINGS_FILE_URL "http://sip.example.com:80/46xxsettings.txt"
SET FQDN_IP_MAP "sip.example.com=192.168.0.76"
SET MEDIA_ENCRYPTION 9
SET ENCRYPT_SRTCP 0
SET DSCPVID 46
SET TLS_VERSION 1
IF $MODEL4 SEQ acm GOTO EQNXCOMMONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acw GOTO EQNXCOMMONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aci GOTO EQNXCOMMONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aca GOTO EQNXCOMMONAUTOGENERATEDSETTINGS
...
# EQNXCOMMONAUTOGENERATEDSETTINGS
SET SIPSSO 2
SET MTCTISSO 2
SET AVAYA_CLOUD_ACCOUNTS_URI accounts-ipo.avayacloud.com
IF $MODEL4 SEQ acm GOTO EQNXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acw GOTO EQNXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aci GOTO EQNXIOSSPECIFICSETTINGS
GOTO NONAUTOGENERATEDSETTINGS
...
# EQNXAUTOGENERATEDSETTINGS
SET APPCAST_ENABLED 1
SET APPCAST_URL "https://storage.googleapis.com/avaya-subscription-eap-update/Vantage/
appcast.xml"
SET APPCAST_CHECK_INTERVAL 1
SET AUDIO_DEVICE_CALL_CONTROL_ENABLED 1
GOTO NONAUTOGENERATEDSETTINGS
# EQNXIOSSPECIFICSETTINGS
SET PUSH_NOTIFICATION_ENABLED 1
SET TELEPHONY_PUSH_NOTIFICATION_SERVICE_URL "https://sip.example.com:443/
PushNotification"
SET ENABLE_IPO_PORTAL_MESSAGING_PUSH 1
GOTO NONAUTOGENERATEDSETTINGS
...
# NONAUTOGENERATEDSETTINGS
SET USBLOGINSTAT 0
SET ENHDIALSTAT 0
...
# PRODUCT_LINE_SETTINGS
IF $MODEL4 SEQ aca GOTO SETTINGSK1EX
IF $MODEL4 SEQ aci GOTO SETTINGSK1EX
IF $MODEL4 SEQ acm GOTO SETTINGSK1EX
IF $MODEL4 SEQ acw GOTO SETTINGSK1EX
...
# SETTINGSK1EX
SET SSOENABLED 0
SET EWSSO 0
SET SIPREGPROXYPOLICY "alternate"
SET IPO_PRESENCE_ENABLED 1
SET IPO_CONTACTS_ENABLED 1
SET DND_SAC_LINK 1
SET POUND_KEY_AS_CALL_TRIGGER 0
SET OBSCURE_PREFERENCES
"ESMENABLED,ESMSRV,ESMPORT,ESMREFRESH,ESMUSERNAME,ESMPASSWORD,ACSENABLED,ACSSRV,ACSPOR
T,ACSUSERNAME,ACSPASSWORD,DIRENABLED,DIRSRV,DIRSRVRPRT,DIRTOPDN,DIRSECURE,DIRUSERNAME,D
IRPASSWORD,SSOENABLED,WINDOWS_IMPROVIDER,AUTO_AWAY_TIME,PSTN_VM_NUM"
SET ENABLE_PPM 0
SET ENABLE_OPUS 1
SET SIMULTANEOUS_REGISTRATIONS 1
SET ENABLE_AVAYA_ENVIRONMENT 0
SET DISCOVER_AVAYA_ENVIRONMENT 0
SET ENABLE_IPOFFICE 1
SET ENABLE_IPO_CALL_LOG 1

```

```
SET SUBSCRIBE_LIST_NON_AVAYA "reg,message-summary,avaya-ccs-profile"
SET SDPCAPNEG 1
SET SIPENABLED 1
...
IF $MODEL4 SEQ aca GOTO SETTINGSEQNX
IF $MODEL4 SEQ aci GOTO SETTINGSEQNX
IF $MODEL4 SEQ acm GOTO SETTINGSEQNX
IF $MODEL4 SEQ acw GOTO SETTINGSEQNX
...
# SETTINGSEQNX
SET SETTINGS_CHECK_INTERVAL 1
SET ENABLE_BROWSER_EXTENSION 0
SET WINDOWS_IMPROVIDER 0
SET ENABLE_OUTLOOK_ADDON 1
SET OUTLOOK_CALL_CONTACT 1
SET IPO_CONFERENCE_CONTROLS_ENABLED 1
SET CALL_DECLINE_POLICY 2
SET IPO_ADHOC_CONFERENCE_NAME "Conf fa"
SET IPO_OTHER_PHONE_MODE_ENABLED 1
SET IPO_CALL_RECORDING_ENABLED 1
SET IPO_SHARE_CONTROLLED_SOFTPHONE_ENABLED 1
SET AUTO_ANSWER 1
SET IPO_CALL_HANDOVER_ENABLED 1
GOTO END
...
# END
GET 46xxspecials.txt
```

Related links

[The IP Office Settings Files](#) on page 95

Sample 46xxspecials.txt file

You can browse to <https://<IPOffice>/46xxspecials.txt> to obtain the 46xxspecials.txt file from an IP Office system.

- Browsing the 46xxspecials.txt file on an IP Office system that does not a file, displays an auto-generated 46xxspecials.txt file, see below. You can use the structure of the auto-generated file to apply settings to specific phones and clients. Save and edit that file before uploading it back to the system.
- The 46xxspecials.txt file is supported for the Avaya Workplace Client for IP Office R11.1.2.4 and higher.
- Do not add Avaya Workplace Client IPv6 settings to the 46xxspecials.txt file, for example *SIGNALING_ADDR_MODE* and *MEDIA_ADDR_MODE*. Doing so will cause local Avaya Workplace Client extensions to attempt to use those settings.

Sample auto-generated 46xxspecials.txt file

```
## IPOFFICE/11.1.2.4.0 build 3 192.168.0.76 AUTOGENERATED
IF $MODEL4 SEQ 1603 GOTO 16XXSPECIALS
IF $MODEL4 SEQ 1608 GOTO 16XXSPECIALS
IF $MODEL4 SEQ 1616 GOTO 16XXSPECIALS
IF $MODEL4 SEQ 9620 GOTO 96XXSPECIALS
IF $MODEL4 SEQ 9630 GOTO 96XXSPECIALS
IF $MODEL4 SEQ 9640 GOTO 96XXSPECIALS
IF $MODEL4 SEQ 9650 GOTO 96XXSPECIALS
```

```

IF $MODEL4 SEQ 9608 GOTO 96X1SPECIALS
IF $MODEL4 SEQ 9611 GOTO 96X1SPECIALS
IF $MODEL4 SEQ 9621 GOTO 96X1SPECIALS
IF $MODEL4 SEQ 9641 GOTO 96X1SPECIALS
IF $MODEL4 SEQ J129 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J139 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J169 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J179 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J159 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J189 GOTO J1X9SPECIALS
IF $MODEL4 SEQ K165 GOTO K1XXSPECIALS
IF $MODEL4 SEQ K175 GOTO K1XXSPECIALS
IF $MODEL4 SEQ aca GOTO SETTINGSEQNX
IF $MODEL4 SEQ aci GOTO SETTINGSEQNX
IF $MODEL4 SEQ acm GOTO SETTINGSEQNX
IF $MODEL4 SEQ acw GOTO SETTINGSEQNX
GOTO GENERALSPECIALS
# 16XXSPECIALS
GOTO GENERALSPECIALS
# 96XXSPECIALS
GOTO GENERALSPECIALS
# 96X1SPECIALS
GOTO GENERALSPECIALS
# J1X9SPECIALS
IF $SIG_IN_USE SEQ H323 GOTO J1X9H323SPECIALS
GOTO GENERALSPECIALS
# J1X9H323SPECIALS
GOTO GENERALSPECIALS
# K1XXSPECIALS
GOTO GENERALSPECIALS
# SETTINGSEQNX
GOTO GENERALSPECIALS
# GENERALSPECIALS
# GROUP_SETTINGS
IF $GROUP SEQ 1 GOTO GROUP_1
IF $GROUP SEQ 2 GOTO GROUP_2
IF $GROUP SEQ 3 GOTO GROUP_3
IF $GROUP SEQ 4 GOTO GROUP_4
IF $GROUP SEQ 5 GOTO GROUP_5
GOTO END
# GROUP_1
GOTO END
# GROUP_2
GOTO END
# GROUP_3
GOTO END
# GROUP_4
GOTO END
# GROUP_5
GOTO END
# END

```

Related links

[The IP Office Settings Files](#) on page 95

User Agent spoofing

The IP Office can vary the content of the auto-generated settings files based on the *User Agent (UA)* string of the device that requests the files. Therefore, viewing the files using a browser may not show the file exactly as received by a particular phone or application.

However, it is possible to configure a browser to temporarily use a different *UA* string. This is called *UA spoofing*.

Example User Agent strings

- Goggle Chrome send a *UA* string like *Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36*.
- The following are example *UA* strings sent by Avaya clients.

Regular Expression	Description
Avaya.*	Matches any <i>UA</i> beginning with <i>Avaya</i> . The <i>.</i> matches any character. The <i>.*</i> matches any number of characters.
Avaya J1.*	Matches the <i>UA</i> string of any J100 Series phone.
Avaya (J1 Communicator).*	Matches the <i>UA</i> string of both J100 Series phones and Avaya Workplace clients. The <i>()</i> brackets enclose the potential matches, each potential match separated by a <i> </i> character.

- As shown in the examples above, the *UA* string can vary depending on the software version and/or platform.
- You can view the *UA* sent by a particular phone or softphone in SysMonitor by registering the phone or client.

Related links

[The IP Office Settings Files](#) on page 95

[Changing the User Agent in Google Chrome](#) on page 100

[Changing the User Agent in Safari](#) on page 101

Changing the User Agent in Google Chrome

About this task

This processes temporarily changes the *UA* string used by a Google Chrome browser. You can use this process to have the browser mimic an Avaya phone or application requesting files from the IP Office.

Before you begin Procedure

1. Using the browser, request a file from the IP Office.
2. Right-click on the window and select **Inspect**. The browser displays an inspection panel.
3. Click on the three-dots settings icon in the inspection panel.
4. Select **More tools** and then **Network conditions**.

5. In the **User agent** section, disable **Use browser default**.
6. In the drop-down list, select **Custom....**
7. In the text box below **Custom....**, enter the *UA* string the browser should use.
8. Refresh the browser page. The page is fetched from the IP Office using the custom *UA*.

Related links

[User Agent spoofing](#) on page 100

Changing the User Agent in Safari

About this task

This process temporarily changes the *UA* string used by a macOS Safari browser. You can use this process to have the browser mimic an Avaya phone or application requesting files from the IP Office.

Before you begin**Procedure**

1. Click **Safari > Preferences**.
2. Click **Advanced**.
3. Enable **Show Developer menu in menu bar**.
4. Click **Develop > User Agent > Other....**
5. Enter the custom *UA* string and click **OK**.

Related links

[User Agent spoofing](#) on page 100

Chapter 19: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

[Additional Manuals and User Guides](#) on page 102

[Getting Help](#) on page 102

[Finding an Avaya Business Partner](#) on page 103

[Additional IP Office resources](#) on page 103

[Training](#) on page 104

Additional Manuals and User Guides

The [Avaya Documentation Center](#) website contains user guides and manuals for Avaya products including IP Office.

- For a listing of the current IP Office manuals and user guides, look at the [Avaya IP Office™ Platform Manuals and User Guides](#) document.
- The [Avaya IP Office Knowledgebase](#) and [Avaya Support](#) websites also provide access to the IP Office technical manuals and users guides.
 - Note that where possible these sites redirect users to the version of the document hosted by the [Avaya Documentation Center](#).

For other types of documents and other resources, visit the various Avaya websites (see [Additional IP Office resources](#) on page 103).

Related links

[Additional Help and Documentation](#) on page 102

Getting Help

Avaya sells IP Office through accredited business partners. Those business partners provide direct support to their customers and can escalate issues to Avaya when necessary.

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See [Finding an Avaya Business Partner](#) on page 103.

Related links

[Additional Help and Documentation](#) on page 102

Finding an Avaya Business Partner

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner.

Procedure

1. Using a browser, go to the [Avaya Website](https://www.avaya.com) at <https://www.avaya.com>
2. Select **Partners** and then **Find a Partner**.
3. Enter your location information.
4. For IP Office business partners, using the **Filter**, select **Small/Medium Business**.

Related links

[Additional Help and Documentation](#) on page 102

Additional IP Office resources

In addition to the documentation website (see [Additional Manuals and User Guides](#) on page 102), there are a range of website that provide information about Avaya products and services including IP Office.

- [Avaya Website](https://www.avaya.com) (<https://www.avaya.com>)

This is the official Avaya website. The front page also provides access to individual Avaya websites for different regions and countries.

- [Avaya Sales & Partner Portal](https://sales.avaya.com) (<https://sales.avaya.com>)

This is the official website for all Avaya business partners. The site requires registration for a username and password. Once accessed, you can customize the portal to show specific products and information type that you want to see.

- [Avaya Support](https://support.avaya.com) (<https://support.avaya.com>)

This site provide access to Avaya product software, documentation and other services for Avaya product installers and maintainers.

- [Avaya Support Forums](https://support.avaya.com/forums/index.php) (<https://support.avaya.com/forums/index.php>)

This site provides forums for discussing product issues.

- **International Avaya User Group** (<https://www.iuag.org>)

This is the organization for Avaya customers. It provides discussion groups and forums.

- **Avaya Learning** (<https://www.avaya-learning.com/>)

This site provides access to training courses and accreditation programs for Avaya products.

Related links

[Additional Help and Documentation](#) on page 102

Training

Avaya training and credentials ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the [Avaya Learning](#) website.

Related links

[Additional Help and Documentation](#) on page 102

Index

Special Characters

*.push.apple.com [67](#)

Numerics

46xxsettings.txt [22](#), [95](#)

46xxspecials.txt [22](#), [95](#)

A

Account URL [55](#)

AccountsToken [83](#)

Add

 API Key [54](#)

 Phone number [88](#)

Adding

 IPO system details [90](#)

Admin Password

 Source Number [22](#)

Administrator [102](#)

Advanced [11](#)

agent mode [11](#)

API Key [54](#), [55](#)

 Synchronize [73](#)

APIs [103](#)

APNP System-ID

 Synchronize [73](#)

APNS [67](#)

 Checklist [69](#), [81](#)

 Notes [69](#)

 Routing [67](#)

 user settings [74](#)

App

 Avaya Mobile Push Notification Service [71](#)

Apple Push Notification Services [71](#)

Apple push notifications [67](#)

Application Notes [103](#)

Apps

 Equinix Cloud Client [58](#)

Area Code [83](#)

Authorization [64](#), [65](#)

AutoFailover [83](#)

Automatic Synchronization [59](#), [60](#)

Avaya Cloud

 Automatic synchronization [57](#)

 Synchronization [57](#)

Avaya Cloud Services [51](#), [55](#)

 Check users [61](#)

 Checklist [52](#)

 Policy [62](#)

Avaya Mobile Push Notification Service [71](#)

Avaya one-X Portal [61](#)

Avaya Spaces API Key

 Synchronize [73](#)

Avaya Spaces Key Secret

 Synchronize [73](#)

B

Backlight [22](#)

Bahrain [22](#)

Basic [11](#)

Basic User [10](#)

Block third-party cookies [87](#)

Browser

 User Agent [100](#)

business partner locator [103](#)

C

call steal [42](#)

CallKit API [69](#)

channel notifications [45](#)

Checklist

 APNS [69](#), [81](#)

 Avaya Cloud Account Authorization [64](#)

 Avaya Cloud Services [52](#)

 Push notification [69](#), [81](#)

 Settings file synchronization [57](#)

 SSO [64](#)

 User synchronization [57](#)

China [69](#)

Chrome

 Spaces Calling [76](#)

 Spaces Calling Extension [86](#)

 User Agent [100](#)

Citrix [43](#)

codec

 Workplace [12](#)

Company domain

 Verify [52](#)

Company Domain [55](#)

Contacts [11](#), [37](#)

Cookies

 Spaces Calling [87](#)

Country Code [83](#)

courses [103](#)

Customer Domain

 API Key [54](#), [55](#)

 Key Secret [55](#)

D

defaulting

defaulting (<i>continued</i>)		install	
workplace client	48	local VDI client	44
deskphone		virtual VDI client	46
shared control	39	instant messaging	61
Dialing rules		Instant Messaging	11
Spaces Calling	82	International Prefix	83
DialRules	83	iOS	
Domain	55	Push notifications	67
API Key	54 , 55	IP Office	
Key Secret	55	codecs	12
Spaces	60	User synchronization	57
Verify	52	IPv6	9 , 13
E		J	
Email		J100	
Welcome email	58	FQDN	22
emailing		JSON	
bug report	49	Spaces Calling profile	82
Enable Apple Push Notification Services	71	K	
Synchronize	72	Key Secret	54 , 55
Enable Avaya Cloud Account	55	Synchronize	73
Enable Avaya Cloud Account Authorization	64 , 65	L	
Equinox Cloud Client	58	License	10
Expiry email	62	Licenses	
Extension Length	83	Spaces Calling	81
F		LogDownload	83
Failover	83	Login	
Files		SSO	64
Settings	95	Logs	
forums	103	Spaces Calling logs	88
FQDN	22	Long Distance Prefix	83
G		M	
Goggle Chrome		manual	
User Agent	100	add user	92
Google Chrome		manually	
Spaces Calling	76	adding IPO profile details	90
Spaces Calling Extension	86	Manuals	102
Google login	64	messaging server	61
group		Messaging Server	18
no answer time	74	mobile dial delay	74
H		Mobile Dial Delay	74
Help	102	mobile twinning	74
hidden mode	11 , 45	Mobile Twinning	74
I		Mobile User	10
IM	61	move	42
importing		N	
csv file	92	no answer time	74

notifications	
disable	45
NoUser	22
NoUser Source Numbers	22

O

Office 365 login	64
Office Worker	10
one-X Portal	61
Opus	12
Other Phone	11
Outside Prefix	83

P

Password	
Source Number	22
PBX Prefix	83
Phone number	
Add to Spaces	88
Place and Receive Calls Using... ..	11
PNP	67
pnp.avaya.com	67
Policy	
Avaya Cloud Services	62
SSO	66
Ports	15
Power User	10
Prefix	83
Presence	11
Profile	
Settings	83
Profile Name	55
Push notification	
Checklist	69 , 81
push notifications	
user settings	74
Push notifications	67
Notes	69
Routing	67

Q

Quick Reference Guides	102
------------------------------	---------------------

R

Remote extensions	9
Remove Area Code	83
Reseller	102
Resilience	83
retrieve	42
Role	54

S

Safari	
User Agent	101
sales	103
Salesforce login	64
SDKs	103
self-avatar	37
Settings	
Profile	83
Settings file synchronization	
Checklist	57
Settings files	95
share control mode	39
Shared Control	11
Simultaneous	41
simultaneous mode	11
Single Sign-on	83
Single Sign-On	64 , 65
Sites that can always use cookies	87
Source Numbers	22
Spaces	
Add phone number	88
Allow cookies	87
API Key	54 , 55
Blank pop-up	87
Chrome logs	88
Domain	60
Key Secret	55
Preferences	87
Select client	87
Spaces Calling	76
Synchronization	59 , 60
URL	60
Verify company domain	52
Spaces API Key	
Synchronize	73
Spaces calling	
Call log	77
Chrome schematic	77
Chrome topology	77
Components	77
Directory	77
Limitations	77
Workplace schematic	78
Workplace topology	78
Spaces Calling	
Dialing rules	82
Domain profile	82
Licenses	81
Native remote worker	79
Preferred clients	85
Remote worker with ASBCE	80
SSO	82
Spaces Calling Extension	
Install	86
Spaces Key Secret	

Spaces Key Secret (<i>continued</i>)		VDI installation (<i>continued</i>)	
Synchronize	73	local client	44
Specials file	95	virtual client	46
Spoof		Verify	
User Agent	100	Company domain	52
SSO	64 , 83	User synchronization	61
Policy	66	Virtual desktop	43
steal	42	VMware	43
STUNHost	83		
STUNPort	83	W	
Subscription	10	websites	103
support	103	Welcome email	62
Synchronization	59 , 60	Workplace	48
Avaya Cloud	57	Cellular Direct Numbers	20
Checklist	57	Citrix	43
Synchronize		codec support	12
API Key	73	disable notifications	45
APNP System-ID	73	Google login	64
Enable Apple Push Notification Services	72	modes	11
Synchronize APNS Configuration	55	Office 365 login	64
Synchronize Single Sign-On	64 , 65	Salesforce login	64
System Administrator	102	shared control mode	39
System license	10	Single Sign-On	64
System-ID		Spaces Calling	76
Synchronize	73	VDI installation	44 , 46
		Virtual desktop	43
T		Workplace Client	11
Technical Bulletins	103	Workplace client installation	24
telecommuter mode	11		
Telephony User Plus	10		
Teleworker User	10		
Third-party cookies	87		
This Computer	11		
training	103 , 104		
Trial license	62		
Troubleshooting	48		
U			
Unified Communications User	10		
Unique Identity	58		
user			
add manually	92		
no answer time	74		
User			
Synchronization	57 , 59		
User Agent	100		
User Guides	102		
User Synchronization			
Checklist	57		
V			
VDI	43		
VDI installation			