



IP Office™ Platform 11.0

SIP Telephone Installation Notes

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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. Refer to your sales agreement 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 You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a 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 IF YOU PURCHASE A 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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, and 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. Note that 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

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies 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

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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

Customer acknowledges and agrees that it is responsible for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

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>).

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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

1. IP Office SIP Telephones

1.1 What's New.....	10
1.2 Licensing	10
1.3 Network Assessment.....	11
1.4 Voice Compression Channels.....	12
1.5 Telephone Power Supply.....	12
1.6 DHCP Server Requirements.....	12
1.7 File (Provisioning) Server Requirements.....	13
1.8 Phone File Requests.....	13
1.8.1 File Auto-Generation.....	14
1.8.2 Test the File Server.....	15
1.9 Additional Phone Settings.....	16
1.9.1 46xxspecials.txt.....	17
1.9.2 NoUser Source Numbers.....	17
1.9.3 Config File Editing.....	18
1.10 Polling	18
1.11 Resilience.....	18
1.12 Phone Operation Notes.....	19
1.12.1 Account/Authorization Code Entry.....	19
1.12.2 Auto Answer.....	19
1.12.3 Codec Selection.....	19
1.12.4 Hot Desking.....	20
1.13 Centralized Branch Extensions.....	20
1.14 Additional Documentation.....	21

2. Generic Installation Process

2.1 Enabling SIP Extension Support.....	25
2.2 System Default Codecs.....	27
2.3 DHCP Settings.....	28
2.3.1 System DHCP Support.....	29
2.3.2 System Site Specific Option Numbers.....	30
2.4 SIP User Settings.....	31
2.5 SIP Extension Settings.....	32
2.6 Allowing Extension/User Auto Creation.....	34
2.7 Attaching the Phones.....	35
2.8 Blocking Default Passcodes.....	35

3. File (Provisioning) Server Settings

3.1 System File Server Settings.....	39
3.2 Loading Files onto the System.....	41
3.2.1 Manually Copying Files.....	41
3.2.2 Using Manager to Upload Files.....	42
3.2.3 Using Web Manager to Upload Files.....	43
3.3 Loading Files onto a 3rd-Party Server.....	44
3.3.1 Adding Additional MIME File Types.....	44

4. Alternate DHCP Server Setup

4.1 Checking for DHCP Server Support.....	48
4.2 Creating a Scope.....	49
4.3 Adding an Option.....	50
4.4 Activating the Scope.....	50

5. Security Certificates

5.1 Using the IP Office Certificate.....	52
5.1.1 Downloading the Linux Certificate.....	53

5.1.2 Downloading the IP500 V2 Certificate.....	54
5.2 IP Office Certification.....	55
5.2.1 Adding a Root CA Certificate to the IP Office TC	55
5.2.2 Create an Identity Certificate for the IP Office.....	56
5.2.3 Add the Identity Certificate to the IP Office.....	57
5.3 File Server Certification.....	58
5.3.1 Add the Certificates Snap-In.....	58
5.3.2 Add the Trusted Root CA Certificate to the Windows Certificate Store.....	58
5.3.3 Create an Identity Certificate for the File Server.....	59
5.3.4 Add the Identity Certificate to the File Server.....	60

6. Monitoring SIP Phones

6.1 Viewing SIP Phone Communications.....	62
6.2 Viewing Registrations.....	62
6.3 Registration Blacklisting.....	62
6.4 Syslog Monitoring.....	63

7. J100 Series Phone Installation Notes

7.1 J129	66
7.1.1 Restrictions/Limitations.....	66
7.1.2 Known Problems.....	67
7.1.3 Files.....	67
7.1.4 Simple Installation.....	68
7.1.5 Static IP Address Configuration.....	68
7.1.6 SIP Settings Configuration.....	69
7.1.7 Changing the Phone SSON.....	69
7.1.8 Viewing the Phone Settings.....	69
7.1.9 Factory Reset.....	69
7.2 J169/J179	70
7.2.1 System Settings.....	70
7.2.2 Simple Installation.....	70
7.2.3 Complex Installation.....	71
7.2.4 Additional Processes.....	72
7.2.5 Troubleshooting.....	74
7.2.6 Pre-R11.0 H.323 Support.....	75

8. Vantage K100 Series Installation Notes

8.1 Phone Files.....	79
8.2 File Server Options.....	80
8.3 The Administrator Password.....	81
8.4 Emergency Call Restrictions.....	81
8.5 Power Options.....	81
8.6 Installation.....	82
8.6.1 Installation Summary.....	82
8.6.2 Downloading the Vantage Software.....	83
8.6.3 Configuring the Settings Files.....	85
8.6.4 Initial Phone Startup.....	88
8.6.5 Blurred Office Workers Background.....	88
8.6.6 Red Background.....	89
8.6.7 Logging In.....	90
8.7 Bluetooth Handset Operation.....	91
8.7.1 Pairing the Bluetooth Handset.....	91
8.7.2 Handset Lamp.....	92
8.8 Additional Processes.....	93
8.8.1 Switching to Wireless Connection.....	93
8.8.2 Rebooting a Vantage Phone.....	93

8.8.3 Changing the File Server Address	94	12.2 Example 46xxspecials.txt File	141
8.8.4 Changing the Phone's Group Setting.....	94	12.3 Document History.....	141
8.8.5 Clearing the User Data.....	95	Index	143
8.8.6 Factory Defaulting the Phone.....	95		
8.8.7 Checking the Firmware Version.....	96		
8.8.8 Checking the Dialer Application Version.....	96		
8.8.9 Starting an Immediate Upgrade	96		
8.8.10 Application Pinning.....	97		
8.9 Error Messages.....	98		
8.9.1 The Configured Phone Application Was Not Found.....	98		
8.9.2 Please note Vantage Basic is not functional	98		
8.9.3 BT Handset is Not Paired.....	98		
8.9.4 Red Screen/Enter PIN Code	98		
8.9.5 Error syncing IP Office Contacts.....	98		
8.9.6 IP office contacts directory not available.....	98		

9. Avaya Equinox Installation Notes

9.1 Operating System Support.....	100
9.2 Standalone/Simultaneous Mode	100
9.3 User Licensing	101
9.4 Codec Support.....	101
9.5 IP Office Configuration.....	102
9.5.1 System SIP Configuration.....	102
9.5.2 User Configuration	102
9.6 Zang Configuration.....	104
9.6.1 Verify the Company Domain.....	104
9.6.2 Add IP Office Details.....	106
9.6.3 Add Avaya Equinox Users.....	107
9.7 Client Installation.....	108
9.7.1 Windows Client.....	108
9.7.2 macOS Client.....	110
9.7.3 iOS Client.....	111
9.7.4 Android Client.....	111
9.7.5 Initial Configuration.....	112
9.7.6 Calendar Integration.....	114
9.7.7 Contact Integration.....	115
9.8 Troubleshooting	116
9.8.1 Defaulting Equinox.....	116
9.8.2 Emailing a Bug Report.....	116
9.8.3 Setting the Email Address.....	116

10. Other Avaya SIP Phones

10.1 1010, 1040 Telephones	118
10.2 1100/1200 Series.....	118
10.3 B100 Series (B179).....	118
10.4 D100 Series (D160).....	118
10.5 E100 Series (E129, E159, E169).....	119
10.5.1 E129.....	119
10.5.2 E159, E169.....	126
10.6 H100 Series (H715).....	126

11. 3rd-Party SIP Phones

11.1 General Notes.....	131
11.2 Simultaneous Calls	131

12. Appendix

12.1 Example 46xxsettings.txt File.....	134
---	-----

Chapter 1.

IP Office SIP Telephones

1. IP Office SIP Telephones

IP Office supports a range of SIP telephones. These can be SIP phones, SIP softphone clients or traditional analog telephones attached to the SIP Analog Telephony Adapter (ATA).

This document covers the general installation of SIP telephones with IP Office 11.0 or higher systems, including third-party SIP telephones. It assumes that you are familiar with IP Office configuration using IP Office Manager, System Status and System Monitor. It does not cover SIP softphone clients (except for the case of clients hosted on an Vantage telephone).

It begins with a [generic installation process](#)^[24] which is suitable for most types of SIP telephone. [Additional notes](#)^[118] are then provided for specific phone models where applicable. In some cases, full installation manuals for certain phones on IP Office may also exist, in which case this manual directs installers to those documents (see [Additional Documentation](#)^[24]).

Supported Avaya SIP Telephones

The following Avaya SIP telephones are supported on IP Office Release 11.0 systems.

- [1000 Series](#)^[118]: 1010, 1040.
- [1100 Series](#)^[118]: 1120E, 1140E.
- [1200 Series](#)^[118]: 1220, 1230.
- [B100 Series](#)^[118]: B179.
- [D100 Series](#)^[118]: These D160 DECT handsets use a base station that connects to the IP Office system using a SIP trunk and appear on the IP Office as SIP extensions.
- [E129](#)^[124]: A simple SIP desk phone.
- [E159, E169](#)^[126]: SIP telephones that supports the docking of mobile telephones.
- [H175](#)^[126]: SIP video telephone.
- [J129](#)^[66]: A simple SIP desk phone. Supported from IP Office Release 10.0 SP2.
- [J169/J179](#)^[70]: Advanced SIP desk phones. Supported from IP Office Release 11.0.
- [K165/K175 \(Vantage\)](#)^[78]: These are Android telephones that can host a different dialer applications. However, aspects of their installation and maintenance are similar to that required for standard SIP desk phones so IP Office specific notes are included in this manual.

When used as a branch system in a [centralized Avaya Aura network](#)^[20], a wider range of Avaya SIP telephones is supported but only during failover operation.

3rd-Party SIP Telephones

The IP Office supports non-Avaya SIP telephones but only guarantees basic telephony functions. Example of installation for some are covered by the publication of [application notes](#)^[24] issued by the Avaya Solution & Interoperability Test Lab.

1.1 What's New

IP Office Release 11.0 adds the following features specific to the installation of SIP telephones:

- [J169 and J179 Telephones](#) ^[70]
The J169 and J179 telephones are Avaya telephones. They provide similar menus and features to those on other IP Office phones such as the 1600 and 9600 Series telephones.
- [Vantage Telephones](#) ^[78]
The Vantage telephones are Android telephones that host dialer applications. These connect to IP Office as SIP extensions. For IP Office Release 11.0, the supported dialer application is Vantage Basic.
- **Avaya Equinox**
The range of Avaya Equinox softphones for Windows, macOS, iOS and Android are supported as SIP softphone applications. Note that Android support does not include Vantage telephones.
- [SIP Extension Phone Password](#) ^[32]
SIP extension entries in the IP Office system configuration now include a **Phone Password** setting. When set, this password is used for registration of the telephone with the IP Office system. When not set, the login code of the user associated with the extension is used as per previous operation.
 - **! Important:**
For J169/J179 telephones, the extension **Phone Password** must be used for initial registration of the telephone.
- [Use of Auto-Create Requires a Default Password](#) ^[34]
When auto-create extensions is enabled, the system now requires a default phone password to be set. That password is then assigned to all new extensions created by auto-create whilst it remains enabled.
- [Extension Password Required When Creating a New User Extension](#) ^[31]
When creating a new user in the system configuration, IP Office Manager/IP Office Web Manager prompt whether to also create a matching SIP or H323 extension. For this release the menu also prompts for the phone password to be used with the new extension.
- [Block Default IP Phone Passcodes](#) ^[35]
Previously it has been possible to register some types of IP phone using default phone passwords such as 0000 or matching the extension number. That behaviour is now blocked by default on new systems and repeated attempts to register with a default password may cause the extension to be [blacklisted](#) ^[62]. The blocking of default IP phone passwords is controlled through the system security configuration setting **Block Default IP Phone Passcodes** (*Security | General*).
- [Preferred Ports Control for Phone Firmware/Settings Download](#) ^[39]
Previously, IP phone requests to download their firmware, system settings and user data has been supported on a range of ports that including those also used for IP Office system administration access. In this release, the system can be configured to indicate to IP phones that they should use ports 411 and 8411 for their file requests.
- [Special Settings File \(46xxspecials.txt\) Support](#) ^[17]
For systems using the auto-generated 46xxsettings.txt file, an option to add an additional manual file called 46xxspecials.txt is now supported. This is done using the NoUser source number **ENABLE_46XXSPECIALS_TXT**. When enabled, the last line of the auto-generated settings files instructs IP phones to then read the settings in the additional file. This can be used to add additional settings not included in the auto-generated file or to override selected settings in the auto-generated file

1.2 Licensing

The type of license required for SIP telephones varies:

- Avaya SIP desk phones require **Avaya IP Endpoint** licenses.
- Avaya SIP softphone applications require various user licenses that may vary depending on the particular application and the type of IP Office system.
- 3rd-party SIP telephones and extensions require **3rd Party IP End-points** licenses.

When using **Avaya IP Endpoint** and **3rd Party IP End-points** licenses, successful registration consumes one license count. There must be sufficient licenses of each type for the number of extensions required. On IP Office Server Edition systems, the user must be configured to a licensed user profile with a user license such as the **Basic User** license. Unlicensed users cannot login to an extension.

1.3 Network Assessment

All IP trunks and telephone extensions connect to the system via the customers data network. It is therefore absolutely imperative that the customer network is assessed and reconfigured if necessary to meet the needs of VoIP traffic.

- **! WARNING: A Network Assessment is Mandatory**

When installing IP phones on any IP Office system, it is assumed by Avaya that a network assessment has been performed. If a support issue is escalated to Avaya, Avaya may request to see the results of a recent network assessment and may refuse to provide support if a network assessment with satisfactory results has not been performed.

Current technology allows optimally configured networks to deliver VoIP services with voice quality that matches that of the public phone network. However, few networks are optimally configured and so care should be taken to assess the VoIP quality achievable within a customer network.

Not every network is able to carry voice transmissions. Some data networks have insufficient capacity for voice traffic or have data peaks that will occasionally impact voice traffic. In addition, the usual history of growing and developing a network by integrating products from many vendors makes it necessary to test all the network components for compatibility with VoIP traffic.

A network assessment should include a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet both current and planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies and setting voice quality objectives.
- The assessment should leave you confident that the network will have the capacity for the foreseen data and voice traffic.

Network Assessment Targets

The network assessment targets are:

- **Latency:** *Less than 180ms for good quality. Less than 80ms for toll quality.*
This is the measurement of packet transfer time in one direction. The range 80ms to 180ms is generally acceptable. Note that the different audio codecs used each impose a fixed delay caused by the codec conversion as follows:
 - **G.711:** 20ms.
 - **G.722:** 40ms.
 - **G.729:** 40ms.
- **Packet Loss:** *Less than 3% for good quality. Less than 1% for toll quality.*
Excessive packet loss will be audible as clipped words and may also cause call setup delays.
- **Jitter:** *Less than 20ms.*
Jitter is a measure of the variance in the time for different packets in the same call to reach their destination. Excessive jitter will become audible as echo.
- **Duration:** *Monitor statistics once every minute for a full week.*
The network assessment must include normal hours of business operation.

1.4 Voice Compression Channels

In order to support VoIP trunks and phones, the IP Office system must be fitted with voice compression channels, also known as VCM channels.

In summary, an available voice compression channel is required:

- During incoming or outgoing call setup with the system.
- During any call to or from a non-IP trunk or phone.
- During any call to or from an IP trunk or phone that is using a different codec than the telephone.

IP Office Server Edition

For Linux based IP Office systems no additional hardware is required.

IP500 V2 Systems

For IP500 V2 systems, voice compression channels can be added to a system using a combination of the following options.

- **IP500 VCM Base Cards**
For IP500 and IP500v2 systems, installation of up to 2 IP500 VCM base cards. There are 2 types of card available, the IP500 VCM 32 and the IP500 VCM 64, each providing 32 and 64 VCM channels respectively. Note that each IP500 VCM card also enables 12 Avaya IP endpoints without requiring licenses
- **IP500 Combination Cards**
For IP500v2 systems only, installation of up to 2 IP500 Combination cards. These cards provide a mix of digital extension ports, analog trunk ports and trunk ports. Each card also provides 10 voice compression channels. These cards do not enable any unlicensed Avaya IP endpoints.

1.5 Telephone Power Supply

The IP Office system does not supply power to the phones.

Each phone requires its own power supply. Depending on the particular phone model, it can use either power over ethernet (PoE) or a separate power supply unit. The latter requires each phone to have access to a mains power outlet.

1.6 DHCP Server Requirements

Use of DHCP is strongly recommend for ease of both installation and maintenance. In addition to providing the telephone with an IP address, the DHCP server also provides the telephone with address details of the SIP and file server it should use.

DHCP support can be done in two ways:

- **[IP Office DHCP](#)** ²⁸
The IP Office system can act as the DHCP server for telephones. This is the recommended method if the customer does not already have a separate DHCP server.
- **[Third-Party DHCP](#)** ⁴⁸
For customers with a separate DHCP server, that server can be used to support DHCP for IP phone if it can be configured with additional OPTIONS settings.

1.7 File (Provisioning) Server Requirements

When starting, Avaya IP phones request various files from a file server, normally a configuration file and a firmware file. By default it does this using the address of an HTTP or HTTPS file server. The 'file server' is also frequently called the 'provisioning server'.

For IP Office operation, the IP Office system can act as the file server for most phones. This is the recommend method since normally the appropriate firmware files to be used by phones are already present on the system and are automatically upgraded if necessary when the system is upgraded.

If necessary a third-party file server can be used though this then means that the files on that server need to be manually updated and maintained.

If using the IP Office system for DHCP, the IP Office system tells the telephone which file server to use using [file server settings within its configuration](#)^[38]. If using a third-party DHCP server, the file server address is set through the addition DHCP options.

1. For H175 and Vantage telephones, a separate HTTP/HTTPS file server must be used. This is due to issues with the size and quantity of the firmware files for those phones. If the IP Office is set as the file server for these phones, it automatically redirects their firmware file requests to its **HTTP Server IP Address** settings (regardless of whether **HTTP Redirection** is enabled or not).
2. For 96x1 Series and J100 Series phones, the **HTTP Redirection** setting can be enabled. When that is the case, the IP Office system redirects firmware requests for .bin files from those phone to the system's **HTTP Server IP Address**.

1.8 Phone File Requests

When starting, most Avaya IP phones go through a process of requesting various files from a file server:

1. Usually this starts with a request an upgrade file. That file will indicate what firmware the phone should be running. If this differs from the firmware it is running, it will add the software files listed to those it will download. The last line of the upgrade file tells the phone the name of settings file it should request.
2. The phone requests a settings file. This passes a large number of configuration settings to the phone. It may also list additional files that the phone should request such as language files and screen savers.
3. The phone requests additional files:
 - Any firmware files indicated by the upgrade file.
 - Any additional files indicated by the settings file.
 - Any additional settings files.
4. The phone can also request a user settings file.

The above is just a general summary. Depending on the phone, the order of file request may vary. In addition, if requesting firmware for an upgrade, the phone may not request other files until the firmware upgrade has been completed and it has restarted.

When the IP Office system is used as the file server, it has the ability to [auto-generate](#)^[14] many of the files requested by the phone.

1.8.1 File Auto-Generation

Avaya IP phones request a number of files from the file server when the phone is restarted. For example phone configuration and firmware files.

When using the IP Office system as the file server, when the phone requests a file, if that file is not available the system may auto-generate a file. The auto-generated file will use a combination of default options and settings from the system configuration. Once supplied to the requesting phone the auto-generated file is not retained on the system.

This feature is used for most of the file types except for actual firmware files (eg. .bin, .zip, .tar) and certificate files. If an actual file is [uploaded to the system](#)^[4], auto-generation of that particular file stops.

Within the auto-generated 46xxsettings.txt file:

- Those settings based on IP Office configuration entries, for example language settings, appear in the sections labeled "AUTOGENERATEDSETTINGS".
- Those settings that remain the same for all IP Office systems using the same release of software appear in the section labeled "NONAUTOGENERATEDSETTINGS".

You can use a web browser to perform a basic test of the file server. For example, if using HTTP, entering ***http://<server_address>/46xxsettings.txt*** should display the file contents.

If using the IP Office system to auto-generate files, the settings file includes text indicating that it was automatically generated by the system in response to the file request. This is useful to not only check the file server operation but to also see the settings being supplied by the IP Office system.

1.8.2 Test the File Server

You can use a web browser to perform a basic test of the file server. For example, if using HTTP, entering ***http://<server_address>/46xxsettings.txt*** should display the file contents.

If using the IP Office system to auto-generate files, the settings file includes text indicating that it was automatically generated by the system in response to the file request. This is useful to not only check the file server operation but to also see the settings being supplied by the IP Office system.

1.9 Additional Phone Settings

The [auto-generated](#) ^[14] 46xxsettings.txt settings files are suitable for most installations. However, in some scenarios it may be necessary to amend the value of the file settings or to add additional settings. This can be done in a number of ways:

- **Using Static Files:**

Replace the auto-generated file with an actual file. The method is only recommended for those experienced with the editing of Avaya phone settings files. The major drawback is that you no longer benefit from the automatic changing of settings to match changes in the IP Office configuration. See [Config File Editing](#) ^[18].

- **Use a 46xxspecials.txt File:**

If a file called 46xxsettings.txt is present on the system, then the auto-generated 46xxsettings.txt file instructs the phone to request that file. This allows you to upload a special file that contains any additional settings or override selected settings in the auto-generated file. See [46xxspecials.txt](#) ^[17].

- **Use NoUser Source Numbers:**

There are a number of NoUser source number settings that can be used to add special values to the auto-generated settings file. See [NoUser Source Numbers](#) ^[17].

Common Additional Commands

The following are some of the frequently used additional commands. For full details of commands available refer to the appropriate Avaya administrator's manual for the particular series of phones.

Function	Description	Setting File Command
Password/CRAFT	Set the PROCPSWD specified in the auto-generated 46xxsettings.txt file where X is the password. This is useful scenarios such as TLS operation which cannot be enabled on phones with the default PROCPSWD.	SET PROCPSWD X
Administrators Password	Set the Vantage phone administrator password ^[87] specified in the auto-generated 46xxsettings.txt file where X is the password.	SET ADMIN_PASSWORD X
Headset Operation	By default, the phone headset goes back on-hook when the other party disconnects. Setting this source number changes that behavior so that headset remains off-hook when the other party disconnects.	SET HEADSYS 1
Backlight Timer	Sets the timer in minutes for the phone backlight timer.	SET BAKLIGHTOFF 60
Screen Saver	This set of commands 1) enable the screen saver, 2) set the name of screen saver to download and 3) sets the name of the current downloaded file to use.	SET SCREENSAVERON SET SCREENSAVER_IMAGE J179scr SET SCREENSAVER_IMAGE_DISPLAY
Background Image	This set of commands 1) set the name of the background image to download and 2) the name of the current downloaded file to use.	SET BACKGROUND_IMAGE J179bck SET BACKGROUND_IMAGE_DISPLAY

- There are several **NoUser** source numbers used for remote extension. 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 *"IP Office SIP Phones with ABSCE"* manual.

1.9.1 46xxspecials.txt

For systems using the [auto-generated](#) 46xxsettings.txt file, one option to add additional manual settings is to use a file called *46xxspecials.txt*. When such a file is added to the system, the command **GET 46xxspecials.txt** appears as the last line of the auto-generated 46xxsettings.txt file requested by phones.

The *46xxspecials.txt* file needs to be [manually created](#) and then [placed](#) on the phone file server. It can be a simple text file containing a single command or a complex settings file with settings based on phone type, model and/or group.

To obtain an example of a complex structure, you can browse to <http://<IPOffice>/46xxspecials.txt> to [obtain an empty file](#). [Save and edit](#) that file before [uploading](#) it back to the system.

1.9.2 NoUser Source Numbers

Most values in the auto-generated 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 files. This can be done using the values entered 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 *"IP Office SIP Phones with ABSCE"* manual.

Example NoUser Source Numbers

- **SET_46xx_PROCPSWD=X**
This NoUser source number adds the command **SET PROCPSWD X** to the auto-generated settings file where X is the password set.
- **SET_ADMINPSWD=X**
This NoUser source number adds the command **SET ADMINPSWD X** to the auto-generated settings file where X is the password set.
- **SET_HEADSYS_1**
This NoUser source number adds the command **SET HEADSYS 1** to the auto-generated settings file.
- **REM_BAKLIGHTOFF=N**
This NoUser source number adds the command **SET BAKLIGHTOFF N** to the auto-generated settings file provided to a remote extension. N is the timeout in minutes.

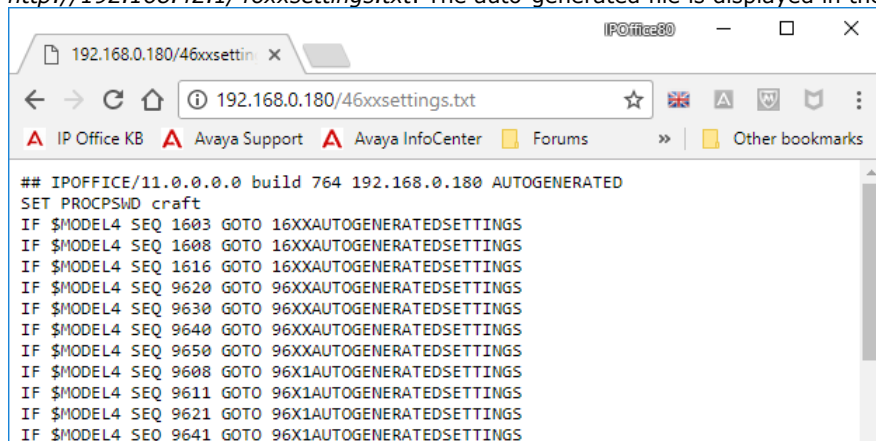
1.9.3 Config File Editing

Most Avaya IP phones download a settings file when restarted. This file contains a range of settings.

- **Note:** Where possible that you use the IP Office system's as the file server and let it auto-generate the settings files. This helps as the system automatically adjusts the settings provided to phones to match changes made in the system configuration.

To download and edit a settings file:

1. Browse to the system and enter the name of the particular phone settings file required, for example <http://192.168.42.1/46xxsettings.txt>. The auto-generated file is displayed in the browser.



- **Most Phones:** *46xxsettings.txt*
 - **1100/1200 Series:** *11xxsettings.txt*
 - **H175:** *H1xxsettings.txt*
2. Save the file as a local text file. The method will depend on your browser.
 - **Chrome:** Right-click on the window and select **Save as ...**.
 - **Explorer:** Select **File | Save as ...**.
 - **Firefox:** Right-click on the window and select **Save Page As ...**.
 3. The downloaded file can now be edited using a text editor. The supported fields are described in the appropriate administration manual for the phone series, see [Additional Documentation](#) ².
 4. When completed, upload the file to the file server being used by the telephones. To upload to the IP Office if that is the file server, see [Loading Files onto the System](#) ⁴.
 5. Restart the phone or phones in order for them to reload their files including downloading the edited settings file.

1.10 Polling

By default many Avaya SIP phones poll their configured file server hourly to check for new or changed files. This applies to H175, J100 Series and Vantage K100 Series phones. This allows the phones to download new settings without being restarted. They can also download new firmware and then automatically upgrade.

The *46xxsettings.txt* file can be edited to include settings to control the frequency of polling and set when phones will automatically upgrade if not rebooted. Refer to the relevant administrators manual for the phone series for details of the available settings.

1.11 Resilience

Resilience allows phones registered on one IP Office system in a network to automatically re-register on another system when their current system is not accessible for some reason. For IP Office Release 10.0 and higher, resilience is supported for Avaya SIP telephones.

Resilience is configured in the IP Office system configurations. Refer to the *"IP Office Resilience Overview"* manual, see [Additional Documentation](#) ².

1.12 Phone Operation Notes

The following known differences/limitations apply to the operation of SIP phones on IP Office.

- [Account/Authorization Code Entry](#) ^[19]
- [Auto Answer](#) ^[19]
- [Codec Selection](#) ^[19]
- [Hot Desking](#) ^[20]

1.12.1 Account/Authorization Code Entry

On SIP phones, the IP Office cannot drive the display to indicate when the entry of an account or authorization code is required. Instead a single tone is played after which the appropriate code should be entered followed by a #.

1.12.2 Auto Answer

For Avaya phones that support the ability to auto-answer calls when requested to do so by the system, that feature is enabled automatically and does not require any configuration.

However, for 3rd-party SIP phones there are multiple methods of signalling that a call should be auto-answered. If the phone supports one of those methods, that needs to be configured through **3rd Party Auto Answer** field in the [extension settings](#) ^[32]. Supported options are:

- **None**
The extension device does not support auto answer.
- **RFC 5373**
The extension device supports auto answer using an RFC 5373 header added to the call invitation message.
- **answer-after**
The extension device supports auto answer using a 'answer-after' header message.
- **device auto answers**
The system relies on the extension device auto answering calls, ie. it does not specifically indicate to the phone to that the call should be auto answered.

1.12.3 Codec Selection

Unlike Avaya H323 IP telephones which always support at least one G711 codec, SIP devices do not support a single common audio codec. Therefore, it is important to ensure that any SIP device is configured to match at least one system codec configured on the system.

1.12.4 Hot Desking

SIP phone can use the IP Office user hot desking features, for example the default *35 and *36 short codes. However, when a different user logs in using those functions, the existing user information stored on the phone (personal directory, call log, etc) is not changed or replaced. Similarly, any local call log maintained by the phone will retain details of the hot desk users calls and other dialing. This is similar to hot desk operation on analog phones.

In addition, SIP phones continue to display the details of the user account used to originally register the phone with the system, such as typically the original user name on the display.

For IP Office Release 10.1, the support of hot desking on J129 and H175 telephones is blocked by default. This is to reflect the fact that these phones download data (call logs and personal directories) from the telephone system, rather than storing them locally, but do not replace that data when a different user hot desks onto the phone. If required, hot desking operation for those phones can be enabled using the NoUser source number **SIP_ENABLE_HOT_DESK**.

Hot-desking is not supported for SIP softphone applications. That includes clients running on Vantage telephones.

1.13 Centralized Branch Extensions

Centralized IP Office branch deployments refers to scenarios where IP Office systems act as local branches within a larger Avaya Aura network. In these scenarios, Avaya SIP telephones registered with the Avaya Aura can failback to registering with the IP Office when the connection to the Avaya Aura is not available for some reason. These are called centralized extensions.

This document does not cover the installation and configuration of SIP centralized extensions.

1.14 Additional Documentation

Installation/Administration Manuals

The following manuals cover the installation of specific Avaya SIP telephones with IP Office.

Series	Supported SIP Models	Documentation
1100 Series	1120E, 1140E	<ul style="list-style-type: none"> IP Office 1100/1200 Series Phone Installation
1200 Series	1220, 1230	
B100 Series	B179	<ul style="list-style-type: none"> Installing and Administering the IP Office B179 SIP Conference Phone
D100 Series	D160	<ul style="list-style-type: none"> Installing and Administering IP Office D100 SIP Wireless Terminal
E100 Series	E129	<ul style="list-style-type: none"> Installing and Maintaining Avaya E129 SIP Deskphone Administering Avaya E129 SIP Deskphone
	E159, E169	<ul style="list-style-type: none"> Installing and Maintaining the Avaya E149 and E169 IP Media Stations
H100 Series	H175	<ul style="list-style-type: none"> Installing and Maintaining Avaya H100-Series Video Collaboration Stations
		<ul style="list-style-type: none"> Administering Avaya H100-Series Video Collaboration Stations
J100 Series	J129	<ul style="list-style-type: none"> Installing and Administering J100 Series IP Deskphones SIP
General		<ul style="list-style-type: none"> IP Office SIP Phones with ASBCE IP Office Resiliency Overview

To download Avaya manuals:

1. Browse to <http://support.avaya.com> and log in.
2. Select **Support by Product** and click **Documents**.
3. In the **Enter Your Product Here** box enter the product name and select the matching option from the displayed list.
4. Use the **Choose Release** drop-down to select the required IP Office release.
5. Select the content type you want included in the list of documents.
6. Click **ENTER**.

Application Notes

Through the its Solutions & Interoperability Lab, Avaya issues a range of application notes. These include application notes for particular models of third-part SIP telephones. Application notes can be downloaded from the Avaya DevConnect web site (http://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.jsp).

Brand	Model	Brand	Model
Algo	8028 SIP Door Phone	Grandstream	GXV3240
	8036 SIP Multimedia Intercom		GXV3275
	8128 SIP Strobe Light	LiveSentinel	SIP Video Door Intercom
	8180 SIP Audio Alerter	Polycom	SoundStation Duo
	8188 SIP Ceiling Speaker	QSC	Q-Sys SIP Softphone
	8301 SIP Paging Adapter	Revolabs	FLX UC 1000
	3226 Trunk Port FXO Doorphone	Valcom	One-Way IP Speakers PagePro IP
Ascom	i62 VoWiFi handset i75 VoWiFi Handset Myco Wireless Smartphones	Yealink	T-18 SIP Phones T-20 SIP Phones T-28 SIP Phones T-26 SIP Phones T-22 SIP Phones VP530 SIP Video Phone
Interquartz	Endurance 10CS		
Cetis	3300IP Series SIP Telephones 9600IP Series SIP Telephones		
G-Tek	AQ-10x		
	ASP-8210-SMK		
	ASP-6210-S		
	AAX-4100	Teledex	SIP ND2000 Series SIP NDC2000 Series SIP LD4200 Series

Chapter 2.

Generic Installation Process

2. Generic Installation Process

This section details the simplest installation method. This method is suitable for customer sites that do not have a separate DHCP server. This simple installation processes assumes:

- **SIP Registrar/Proxy**
The IP Office system is the SIP registrar.
- **DHCP Server**
The IP Office system acts as the DHCP server. To use a separate DHCP see [Alternate DHCP Server Setup](#)^[48].
- **File Server**
The IP Office acts as the file server for IP telephones. It auto-generates the necessary settings and upgrade files for Avaya IP phones. To use a separate file server, see [File \(Provisioning\) Server Settings](#)^[38].
- **TLS Certificate**
If TLS is enabled, the IP Office system's own default identity certificate is used. For additional options see [Server Certification](#)^[52].

The general process for connecting SIP telephones to an IP Office system can be done in two ways. The steps are summarized below.

Using manual configuration:

This method requires configuration of the user and extension entries in the system configuration before connecting of the actual phones.

1. Check that the system has the appropriate [licenses](#)^[10] to support both the SIP telephone extensions (Avaya and third-party) and the extension users.
2. [Enable SIP extension support](#)^[25].
3. [Adjust the system Codecs](#)^[27] (Optional).
4. [Check the system DHCP settings](#)^[28].
5. [Add SIP Users to the configuration](#)^[31].
6. [Add SIP Extensions to the configuration](#)^[32].
7. [Attach the phones](#)^[35].

Using auto-create configuration:

This method allows the system to automatically create user and extension entries in its configuration when the phones are connected.

1. Check that the system has the appropriate [licenses](#)^[10] to support both the SIP telephone extensions (Avaya and third-party) and the extension users.
2. [Enable SIP extension support](#)^[25].
3. [Adjust the system Codecs](#)^[27] (Optional).
4. [Check the system DHCP settings](#)^[28].
5. [Enable Auto-Creat Extn/User](#)^[34].
6. [Attach the phones](#)^[35].
7. [Modify the IP Office user and extension settings](#)^[31].
8. [Disable Auto-Creat Extn/User](#)^[34].

2.1 Enabling SIP Extension Support

The IP Office system support SIP extensions on its LAN1 and/or LAN2 interfaces. For phone's being supported using auto-generated files, these values are included in the auto-generated settings file downloaded by the phones when they restart.

- **Reboot Required**

Note that changing the SIP registrar settings of an IP Office system requires the IP Office system to be rebooted.

To enable SIP extension support:

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** or **System Settings | System**.
3. Select **LAN1** or **LAN2** as required and then select the **VoIP** tab.

The screenshot shows the IP Office Web Manager configuration page for LAN1 VoIP settings. The left sidebar lists various system settings, with 'LAN1' selected. The main content area has tabs for 'LAN Settings', 'VoIP', and 'Network Topology', with 'VoIP' selected. The 'H.323 GATEKEEPER' section includes 'H.323 Gatekeeper Enable' (YES), 'H.323 Signaling Over TLS' (Preferred), and 'Auto-create Extension' (NO). The 'H.323 Remote Extension Enable' is set to YES, and the 'Remote Call Signaling Port' is 1720. The 'SIP REGISTRAR' section, highlighted with a red box, includes 'SIP Trunks Enable' (YES), 'SIP Remote Extension Enable' (NO), 'Challenge Expiry Time (sec)' (10), 'SIP Registrar Enable' (YES), 'Auto-create Extension/User' (NO), 'SIP Domain Name' (example.com), and 'SIP Registrar FQDN' (storm1.example.com). The 'LAYER 4 PROTOCOL' section, also highlighted with a red box, includes 'UDP' (YES), 'TCP' (YES), 'TLS' (NO), 'UDP Port' (5060), 'TCP Port' (5060), and 'TLS Port' (5061).

- **SIP Registrar Enable**
Check that **SIP Registrar Enable** is selected.
- **Auto-create Extn/User: Default = Off**
When this option is selected, the IP Office automatically creates user and SIP extension entries in its configuration based on SIP extension registration.
 - **! WARNING**
Leaving this settings enabled is strongly deprecated. For Release 9.1 and higher, the system automatically disables the settings 24-hours after it is enabled.
 - **Not Supported with WebLM Licensing**
The auto-create extension and user options are not useable on systems configured to acquire licenses from a WebLM service.
- **SIP Remote Extn Enable: Default = Off**
Currently remote SIP extension options are only supported for Avaya SIP client applications. Remote connection is not supported for third-party SIP telephones.
- **SIP Domain Name: Default = Blank**
This value is used by SIP endpoints for registration with the system. If left blank, registration uses the LAN IP address. The entry should match the domain suffix part of the **SIP Registrar FQDN** below, for example *acme.com*.
 - Note: For Avaya SIP telephones supported for resilience, the **SIP Domain Name** must be common to all systems in the network.
 - This is the local SIP registrar domain name that needed by SIP telephones in order to register with the IP Office. If you are using TLS, this value needs to be included in the [security certificates](#)^[52] applied to the IP Office and, if used, separate HTTP file server.

- **SIP Registrar FQDN:** *Default = Blank*

This is the fully-qualified domain name, for example *example.acme.com*, to which the SIP endpoint should send its registration requests. This address must be resolvable by DNS to the IP address of the IP Office system.

- **Layer 4 Protocol:** *Default = Both TCP & UDP*

These fields set the transport protocol for SIP traffic between the IP Office and SIP extensions.

- **! Important**

Do not enable a protocol unless it is intended to be used. Many phones only use the first enabled protocol that they support in the order TLS, TCP, UDP. They will not fallback to another enabled protocol if problems are encountered in the first protocol. For example, if TLS is enabled, that is indicated to phones through the IP Office's auto-generated phone settings files. The phones will then attempt to use TLS (for example requesting certificates etc) and will not fallback to TCP or UDP if TLS operation is not fully or correctly configured.

- **UDP Port:** *Default = Enabled/5060*

The SIP port if using UDP. The default is 5060.

- **TCP Port:** *Default = Enabled/5060*

The SIP port if using TCP. The default is 5060.

- **TLS Port:** *Default = Disabled/5061*

The SIP port if using TLS. The default is 5061. This option requires server certification to be applied to the IP Office system and to the file server. Do not enable TLS and connect phones until the correct server [certification](#)^[52] has been complete.

- **Challenge Expiry Time (sec):** *Default = 10*

The challenge expiry time is used during SIP extension registration. When a telephone registers, the system sends back a challenge and waits for a response. If the response is not received within this timeout the registration fails.

5. If you have made any changes, save the configuration back to the IP Office.

2.2 System Default Codecs

By default, all VoIP extensions added to the configuration use the system's default codec preferences. This is shown by the **Codec Selection** settings on the individual IP trunk or extension being set to **System Default**.

For most installations these settings do not need to be changed, however it is important to understand how the options are set and used by the system.

Whilst the codec preferences used by an individual trunk or extension can be adjusted, the use of the system default settings is strongly recommend to ensures codec consistency between the trunks and extensions involved in any call. This helps minimizes the need for the system to use additional system resources such as VCM channels. It also allows the use of options such as direct media connection during calls.

- **SIP Codec Selection**

Unlike H323 IP devices which always support at least one G711 codec, SIP devices do not support a single common audio codec. Therefore, it is important to ensure that any SIP device is configured to match at least one system codec configured on the system.

- **G.723/G.729b**

These codecs are not available on Linux based IP Office systems. They are supported on IP500 V2 systems with VCM channels.

To change the system default codec preferences:

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** or **System Settings | System**.
3. Select **VoIP**.

4. The **Available Codecs** list shows the codecs the system supports. Those codecs that are enabled in other configuration forms including the default codec selection.

- **! WARNING:**

Deselecting a codec automatically removes it from any line, system or extension codec list that was using it.

- **SIP Codec Selection**

Unlike H323 IP devices which always support at least one G711 codec, SIP devices do not support a single common audio codec. Therefore, it is important to ensure that any SIP device is configured to match at least one system codec configured on the system.

- **G.723/G.729b**

These codecs are not available on Linux based IP Office systems. They are supported on IP500 V2 systems with VCM channels.

5. The **Default Codec Selection** section is used to set the default codec preference order. This is used by all IP (H323 and SIP) extensions and lines on the system that have their **Codec Selection** setting set to **System Default**. This is the default for all new added IP extension and lines.
6. If these settings need to be changed, do so and then save the configuration back to the system.

2.3 DHCP Settings

The recommendation for SIP telephone installation is to use DHCP, especially if a large number of phones are being installed. Using DHCP simplifies both the installation and maintenance.

- If the IP Office system is to be used as a DHCP server for the network, use the following processes to check and configure the system's DHCP settings.
- If a separate DHCP server is used by the customer's network, that DHCP server needs to be configured to support DHCP requests from IP phones, see [Alternate DHCP Server Setup](#)^[48].
- The IP Office can be configured to only provide DHCP support for Avaya phones. That option can be used to allow it to be used in conjunction with a separate customer DHCP server. This removes the need to configure the customer's DHCP server for IP phone support.
- **! WARNING**
Enabling an additional DHCP server in a network can cause connection issues for all devices on the network. Ensure that you and the customer's network administrator all agree upon the correct choice of DHCP server options.

Enabling IP Office DHCP Support

The following are the main steps for enabling the IP Office system to support DHCP operation for IP phones.

1. [Enable DHCP and Set the Number of Addresses](#)^[29]
2. [Check the Site Specific Option Numbers](#)^[30]
The IP Office defaults match the defaults used by Avaya IP phones. However it is important to check these values and to be aware of their potential usage.
3. [Set the File Server Settings](#)^[38]
If the IP Office system is set to provide DHCP for IP phones, that role includes telling the phones the location of the file server they should use for phone firmware, even if that file server is not the IP Office system.

2.3.1 System DHCP Support

To change the system's DHCP settings:

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** or **System Settings | System**.
3. Select **LAN1** or **LAN2** as required and then select the **LAN Settings** tab.

The screenshot shows the 'LAN Settings' tab for LAN1. The configuration includes:

- IP Address:** 192.168.0.210
- IP Subnet Mask:** 255.255.255.0
- Primary Transfer IP Address:** 0.0.0.0
- RIP Mode:** None
- Enable NAT:** NO
- Number Of DHCP IP Addresses:** 1
- DHCP Mode:** Server
- Advanced:** YES (highlighted)
- Apply to Avaya IP Phones Only:** YES
- DHCP POOLS:**

Start IP Address	IP Subnet Mask	Default Router	Pool Size
192.168.0.31	255.255.255.0	0.0.0.0	4

- **DHCP Mode**

If the **DHCP Mode** is set to **Server**, the **Number of DHCP IP Addresses** value set how many IP addresses the system can issue. Those addresses use the IP Address of the system as the starting point.

- **Advanced**

The **Advanced** button displays the options for **DHCP Pools** if required. These settings allow adjustment of the DHCP settings including adding multiple ranges of DHCP numbers that the IP Office system can support. Note that address ranges outside those of the IP Office systems own subnet may also require the creation of appropriate IP routes to ensure traffic routing between the subnets.

- Note: Changes to the DHCP pools do not require a reboot of the IP Office system. However, they will cause a reboot of Avaya H323 and SIP telephones connected to the system. Non-Avaya IP phones are not rebooted but may need to be manually restarted in order to obtain a valid address from the new pools configuration.

- **Apply to Avaya IP Phones Only**

If selected, the IP Office will act as a DHCP server for Avaya phones only. This option cannot be used if also supporting 1100 Series and 1200 Series phones.

4. If the settings have been changed, save the configuration back to the system.

2.3.2 System Site Specific Option Numbers

When requesting address settings from a DHCP server, each phone also requests additional information that the DHCP server may have. It does this by sending a Site Specific Option Number (SSON) request. If the DHCP server has information matching the requested SSON, that information is included in the DHCP response.

By default, most Avaya SIP telephones use the SSON 242 to request additional information (the E129 uses 60). Depending on the particular phone model, it may be possible to change the SSON number it uses.

To changing the system's SSON settings:

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** or **System Settings | System**.
3. Select **LAN1** or **LAN2** as required and then select the **VoIP** tab.

The screenshot displays the configuration interface for the LAN1 VoIP settings. The left sidebar contains a navigation menu with the following items: System, Voicemail, System Events, SMTP, DNS, SMDR, LAN1 (selected), LAN2, VoIP, VoIP Security, Voice Compression Module (VCM), Directory Services, Telephony, and Contact Center. The main configuration area is divided into several sections:



- System**: A toggle switch set to 'NO' and a dropdown menu set to '5061'.
- RTP**: Includes 'Port Number Range (Min-Max)' set to 46750 - 50750, 'Port Number Range (NAT) (Min-Max)' set to 46750 - 50750, and 'Enable RTCP Monitoring on Port 5005' set to 'YES'.
- KEEPAIVES**: A 'Scope' dropdown menu set to 'Disabled'.
- DIFFSERV SETTINGS**: Includes 'DSCP (Integer - Hex)' set to 46 - B8, 'Video (Integer - Hex)' set to 46 - B8, and 'DSCP Mask (Integer - Hex)' set to 63 - FC.
- SIG DSCP (Integer - Hex)**: Set to 34 - 88.
- DHCP SETTINGS**: Includes 'Primary Site Specific Option Number (4600/5600)' set to 176, 'Secondary Site Specific Option Number (1600/9600)' set to 242 (highlighted with a red box), 'VLAN' set to 'Not Present', '1100 Voice VLAN Site Specific Option Number (SSON)' set to 232, and '1100 Voice VLAN IDs'.

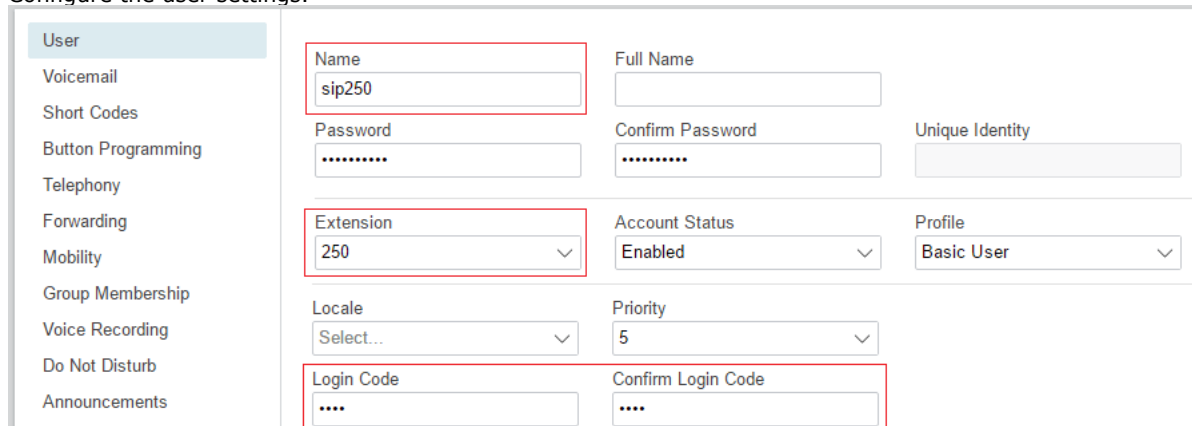
4. Check that the site specific option number settings match those required for the phones being supported. The default for most Avaya SIP phones is 242.
5. If this setting needs to be changed, save the configuration back to the system.

2.4 SIP User Settings

This section looks at just the key configuration settings that affect SIP telephones.

To configure a basic SIP user:

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




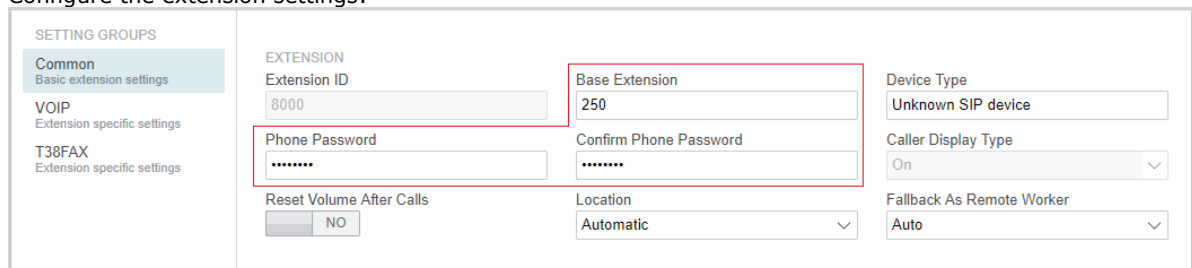
- The key settings used for SIP telephone registration are:
 - Extension**
This should match the SIP ID of the SIP extension and the **Base Extension** setting of the [SIP extension](#) ³² in the IP Office configuration.
 - Login Code**
If the SIP extension has not been configured with an **Phone Password**, this field is used for phone registration. If using IP Office Manager, this setting is on the **User | Telephony | Supervisor** settings tab.
- If creating a new user, after clicking **OK** or **Create**, you are prompted whether to also automatically create a new extension. Select **SIP Extension**.

2.5 SIP Extension Settings

This section looks just at the key configuration settings that affect SIP extensions. For full details of all the fields shown, refer to the "IP Office Manager Manual".

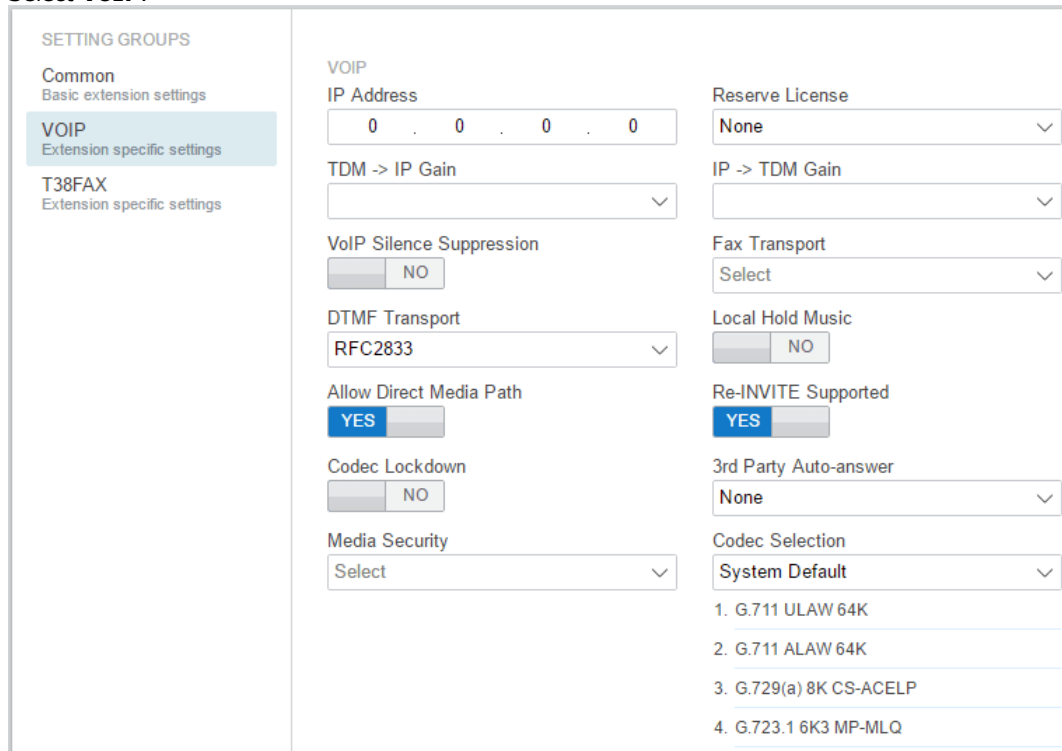
To configure a SIP extension:

- Using either IP Office Manager or IP Office Web Manager, load the system configuration.
 - If using IP Office Manager:**
 - Select the system on which the extension record should be created.
 - Select  | **SIP Extension**.
 - If using IP Office Web Manager:**
 - Select **Call Management | Users**.
 - Click **+Add Extension**.
 - Select SIP Extension and the system on which the extension record should be created and click **OK**.
- Configure the extension settings:



- Base Extension**
This should match the **Extension** setting of the [SIP user](#) ³ added to the IP Office configuration.
- Phone Password/Confirm Phone Password**
This password is used for the extension registration. If no password is set, then the **Login Code** of the user with the same extension number is used.
- ! Important:**
For J169/J179 telephones, the extension **Phone Password** must be used for initial registration of the telephone.

- Select **VoIP**.



- IP Address**
The IP address of the phone. The default setting accepts connection from any address. If an address is entered, registration is only accepted from that address.

- **Codec Selection**

If the **Codec Selection** is left set to **System Default**, the extension will use the [system codec preferences](#)^[27]. In most cases this is preferred and any changes required should be made at the system level to ensure consistency for all IP trunks and extensions. However, if required, the **Codec Selection** of each individual trunk and extension can be adjusted to differ from the system defaults.

- **Reserve License:**

Avaya IP desk phones require a **Avaya IP Endpoint** license. Non-Avaya IP phones requires a **3rd Party IP End-points** license. Normally the available licenses are issued in the order that extensions register. This option allows an extension to be pre-licensed before the extension has registered. On system's using WebLM licensing, this option is fixed to reserve a license.

- **TDM->IP Gain**

Allows adjustment of the gain on audio from the system's TDM interface to the IP connection.

- **IP->TDM Gain**

Allows adjustment of the gain on audio from the IP connection to the system's TDM interface.

- **DTMF Support**

This can be set to one of the two common methods used by SIP devices; **RFC2833** or **Inband**. The selection should be set to match the method used by the SIP extension. However, if the method is not known or can vary on a per call basis, de-selecting **Allow Direct Media Path** allows a VCM channel to be used for DTMF support when necessary.

- **3rd Party Auto Answer**

The ability of an extension to auto answer calls allows the system to page that extension. However, for 3rd-party SIP extensions the ability to auto answer and the method used to enable that function may vary.

- **None**

The extension device does not support auto answer.

- **RFC 5373**

The extension device supports auto answer using an RFC 5373 header added to the call invitation message.

- **answer-after**

The extension device supports auto answer using a 'answer-after' header message.

- **device auto answers**

The system relies on the extension device auto answering calls, ie. it does not specifically indicate to the phone to that the call should be auto answered.

- **Media Security**

These settings allow the adjustment of the settings for SRTP security if used. Normally these are adjusted at the system level for the whole system rather than at the individual extension level.

- **VoIP Silence Suppression**

When selected, this option detects periods of silence during a call and does not send any data during those silences.

- **Local Hold Music**

Select this option if the SIP device supports its own hold music source.

- **Re-invite Supported**

If the SIP device is able to receive REINVITE messages select this option. This option should be selected for extensions that support video as it is necessary to enable switching between audio only and video operation.

- **Codec Lockdown**

In response to a SIP offer with a list of codecs supported, some SIP user agents supply an answer that also lists multiple codecs. This means that the user agent may switch to any of those codecs during the session without further negotiation. The system does not support multiple concurrent codecs for a session, so loss of speech path will occur if the codec is changed during the session. If **Codec Lockdown** is enabled, when the system receives an SDP answer with more than one codec from the list of offered codecs, it sends an extra re-INVITE using just a single codec from the list and resubmits a new SDP offer with just the single chosen codec.

- **Allow Direct Media Path**

This settings controls whether IP calls must be routed via the system or can be routed alternately if possible within the network structure. If enabled, IP calls can take routes other than through the system. This removes the need for a voice compression channel. Both ends of the calls must support Direct Media and be using the same protocol (H.323 or SIP). Enabling this option may cause some vendors problems with changing the media path mid call. If disabled or not supported at on one end of the call, the call is routed via the system. RTP relay support allows calls between devices using the same audio codec to not require a voice compression channel.

2.6 Allowing Extension/User Auto Creation

The IP Office system can be set to automatically create extension and user entries in its own configuration as each SIP telephone registers with the system. This can speed up installation when installing several devices and then disable the setting once the installation has been completed.

The auto-created users are automatically linked to the **IP Auto-create** user rights settings. By default that set of user rights has outgoing calls barred.

- **! WARNING**

Leaving this settings enabled is strongly deprecated. For Release 9.1 and higher, the system automatically disables the settings 24-hours after it is enabled.

- **Not Supported with WebLM Licensing**

The auto-create extension and user options are not useable on systems configured to acquire licenses from a WebLM service.

- **Reboot Required**

Note that changing the SIP registrar settings of an IP Office system requires the IP Office system to be rebooted.

To enable SIP extension/user auto creation:

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** or **System Settings | System**.
3. Select **LAN1** or **LAN2** as required and then select the **VoIP** tab.

The screenshot shows the IP Office configuration interface. On the left is a navigation menu with options: System, Voicemail, System Events, SMTP, DNS, SMDR, LAN1 (selected), LAN2, VoIP, VoIP Security, Voice Compression Module (VCM), and Directory Services. The main area has tabs for LAN Settings, VoIP (selected), and Network Topology. Under the VoIP tab, there are sections for H.323 GATEKEEPER and SIP REGISTRAR. In the H.323 GATEKEEPER section, 'H.323 Gatekeeper Enable' is set to YES, 'H.323 Signaling Over TLS' is set to Disabled, and 'Auto-create Extension' is set to NO. In the SIP REGISTRAR section, 'SIP Trunks Enable' is set to YES, 'SIP Registrar Enable' is set to YES, and 'Auto-create Extension/User' is set to YES. A red box highlights the 'Auto-create Extension/User' setting and a warning message: 'SIP Auto-create Extension/User option is active. Please provide a password.' Another red box highlights the 'Password' and 'Confirm Password' fields, which are currently empty. A third red box highlights the 'SIP Registrar Enable' setting.

4. Change the **Auto-create Extension/User** settings to the state required.
5. When enabled, you need to set and confirm a **Password**. This becomes the **Phone Password** for any extension entries created using auto-creation. The phone password is used for extension registration.
6. If enabled, enter and confirm the default **Phone Password** that should be assigned to auto-created extensions whilst the auto-create extension setting remains enabled. The password is used for phone registration.
7. Send the configuration back to the IP Office.

2.7 Attaching the Phones

The menus shown by phones when first connected to the system depend on the particular model of phone. This section can only provide a general summary.

For most Avaya SIP phones, the general process is as follows:

1. Using DHCP, the phone requests IP address information from a DHCP server. That includes using its DHCP SSN setting to request file server address information from the matching DHCP server option.
2. Using the file server address provided, the phone requests an upgrade text file appropriate for its particular model from the file server.
 - a. If the IP Office is the file server, it auto-generates an appropriate file unless one has been uploaded to its file storage.
 - b. Using the upgrade file, it compares the details of the firmware it is already running and that which the file says it should be running in order to work with the IP Office system.
 - c. If necessary the phone requests the new firmware files from the file server.
 - d. Typically as part of loading any new firmware the phone reboots and restarts the process.
3. The phone now requests the settings text file appropriate for its particular model from the file server. This file contains a wide range of phone settings including details of the SIP server and protocols it should use and the certificate name if using TLS.
 - a. If the IP Office is the file server, it auto-generates an appropriate file and adjust various settings in that auto-generated file to match settings in the IP Office system configuration.
4. The phone requests any further files indicated in the settings file, for example language files and security certificates.
5. If the phone has previously been connected, it attempts to re-register with the system using the previous account settings.
6. If the phone is new or its registration is rejected, it will display menu options for registering with the system:
 - a. When prompted for a username or similar, enter the IP Office user's **Extension** number.
 - b. When prompted for a password or similar, enter the **Phone Password** ⁽³²⁾ set for the extension entry in the configuration. If no password is set, enter the user's **Login Code**.

2.8 Blocking Default Passcodes

For IP Office R11.0 and higher, the default security settings block the use of default phone passwords such as 0000 for extension registration.

To disable default passcode blocking:

1. Using IP Office Manager, access the system's security configuration.
2. On the **General** tab, de-select **Block Default IP Phone Passcodes**.
3. Save the settings.

Chapter 3.

File (Provisioning) Server Settings

3. File (Provisioning) Server Settings

As part of their installation process, Avaya IP phones request files from a file server. If being installed using DHCP, they obtain the address of the file server as part of the DHCP response. If being statically installed, the file server address is entered into the phone as part of the static addressing process.

The file server options are:

- For IP500 V2 systems, the IP Office system's own memory card can be used as the source for the files.
- For IP Office Server Edition systems, the system's own disk can be used as the source for the files used by the phones.
- When using either of the above, [file auto-generation](#)^[14] is supported for settings and upgraded text files for supported Avaya SIP phones.
- If either of the options above are not acceptable, a 3rd party HTTP/HTTPS file server is required. The necessary phone firmware and settings files need to be loaded onto that server.
- Avaya H175 and Vantage phones always require a 3rd party HTTP/HTTPS files server to host and deliver their firmware. They can accept settings files, including auto-generated settings files, from the IP Office as a file server, but the system will always redirect their request for .tar firmware files to the system's configured **HTTP Server IP Address**.

3.1 System File Server Settings

If the IP Office system is being used for [DHCP support](#)^[28] for the IP phones, various settings in the IP Office system's configuration are used to set the file server addresses sent to the phones in the DHCP responses.

To change the file server settings:

- Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
- Select **System** or **System Settings | System**.

The screenshot shows the 'System' configuration page. The left sidebar lists various system settings: System, Voicemail, System Events, SMTP, DNS, SMDR, LAN1, LAN2, and VoIP. The main content area is titled 'System' and contains several configuration sections. A red rectangular box highlights the following settings:

- Name:** SystemA
- Location:** None
- Locale:** United States (US English)
- Device ID:** (empty field)
- TFTP Server IP Address:** 192 . 168 . 0 . 210
- HTTP Server IP Address:** 192 . 168 . 0 . 210
- Phone File Server Type:** Memory Card
- HTTP Redirection:** Off
- Manager PC IP Address:** 255 . 255 . 255 . 255
- Avaya HTTP Clients Only:** NO
- Use Preferred Phone Ports:** NO
- Enable Softphone HTTP Provisioning:** NO

- Check the file server settings. These are used in DHCP responses used by the system and when the system is asked to provide files.

• Phone File Server Type

- **Memory Card** (IP500 V2) / **Disk** (IP Office Server Edition)

Use the system's own memory. The system's IP address is provided as the TFTP and HTTP file server values in the DHCP response. This is the default setting.

- **Manager**

Use the IP Office Manager application as the TFTP and HTTP file server. This option is only supported for a maximum of 5 IP phones. This option uses the separate **Manager PC IP Address** set in the configuration. The default of 0.0.0.0 is used by the system to broadcast for any available IP Office Manager application running on the network. Note that by default the IP Office Manager option for TFTP support is disabled (**File | Preferences | Preferences | Enable BootP and TFTP Servers**).

- **Custom**

This option uses the separate **TFTP Server IP Address** and **HTTP Server IP Address** values set in the configuration as the file server addresses in the DHCP response given to phones.

• HTTP Server IP Address

This field is used if the **Phone File Server Type** is set to **Custom**. It is also used if **HTTP Redirection** is set to **Phone Binaries**.

- When used, this server address is used for file requests by devices on both LAN1 and LAN2. Therefore, the address must be reachable by devices on both LAN. If necessary additional network configuration and or addition of IP route settings are required.
- H175 and Vantage phones always use this setting for their firmware (.tar, .sig) and application (.apk) files. They will do this regardless of the **HTTP Redirection** setting.
- The [PUBLIC HTTP](#)^[17] [NoUser](#)^[17] source number can be used to provide a separate address to remote worker/SBC connected phones.

• HTTP Redirection (Default = Off)

Supported for 96x1 H.323 phones and J100 Series SIP (except J129) phones only. Allows for the use of an alternate HTTP file server for the download of large binary files. This field is available when the **Phone File Server Type** is set to **Memory Card** or **Disk**. When this field is set to **Phone Binaries**, requesting their binary files are redirected to the HTTP server defined in the **HTTP Server IP Address** field.

• Use Preferred Phone Ports

This setting can be used to reduce the use of the HTTP/HTTPS ports configured in the system's security configuration (by default ports 80 and 443) for phone file requests. The system will still provide files on those ports in order to support legacy phones but its auto-generated file response directs newer phones to use ports 441 and 8441.

- When not enabled:
 - Auto-generated phone settings files provided by the system to locale phones indicate the ports 80/411 or 80/443 depending on the phone type.
 - Auto-generated phone settings files provided by the system to remote phones indicate the ports 8411/411 or 8411/443 depending on the phone type.
- When enabled:

-
- Auto-generated phone settings files for locale phones will indicate port 8411 for HTTP and 411 for TLS.

- **Avaya HTTP Clients Only**

This option can be used to restrict the system to responding to file requests from Avaya phones and applications only. This option should not be used if the system is also supporting 1100 and or 1200 Series phones.

5. If any changes have been made, save the configuration back to the system.

3.2 Loading Files onto the System

For IP Office Server Edition and IP500 V2 systems, normal installation includes installing the supported phone firmware files onto the server. Therefore, no further action is normally required if using the system as the file server for phone installation. No other firmware should be used with an IP Office system unless specifically documented.

For IP Office operation, only the phone firmware files need to be present on the memory card. Other files required by the phones are [automatically generated](#)¹⁴ by the system in response to requests from the phones.

The firmware is also included as part of IP Office Manager and is copied onto the PC when IP Office Manager is installed. Only the firmware included in an IP Office release should be used with IP Office systems. Different firmware should only be loaded on to the system's file server if instructed by Avaya. If so, this can be done by a number of methods.

IP500 V2 Control Unit

The system's System SD card is used to store the files. This is a mandatory card that is present in all IP500 V2 systems. The firmware files are loaded onto the card in a number of ways:

- **! WARNING**

A memory card should never be removed from a running system without either the card or the system first being shutdown. IP Office Manager should be used to shutdown the memory card before it is removed from the system.

- If the system was upgraded using the **Recreate SD Card** option in IP Office Manager, the firmware is automatically copied onto the card as part of that process.
- If the system was upgraded using IP Office Manager's Upgrade Wizard, if the **Upload System Files** option was selected, the firmware is copied onto the card as part of that process. The **Upload System Files** option is enabled by default.

3.2.1 Manually Copying Files

Files can be copied onto the IP500 V2 memory card by placing it into a PC with a suitable memory card slot.

- **! WARNING**

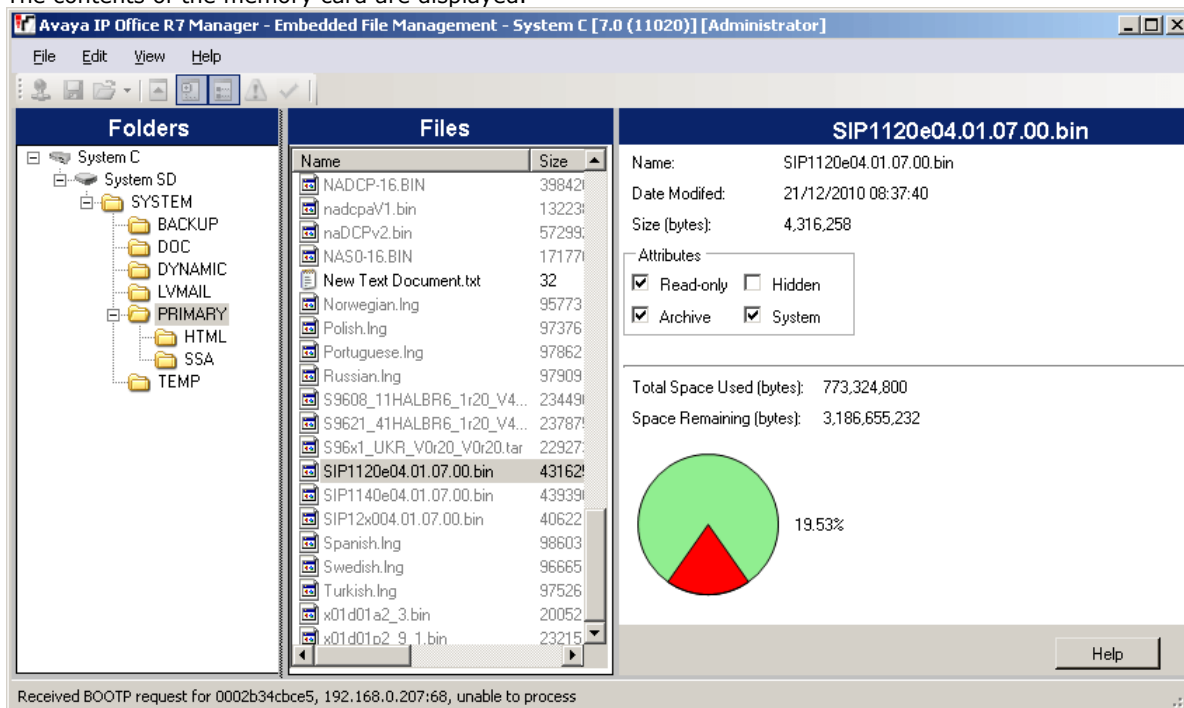
A memory card should never be removed from a running system without first being shutdown. IP Office Manager should be used to shutdown the memory card before it is removed from the system.

1. First shutdown the memory card using IP Office Manager or IP Office Web Manager:
 - **IP Office Web Manager**
Click **Solution**. Click **Actions** and select **Service Commands | Memory Card Stop**. Select **System** and click **OK**.
 - **IP Office Manager**
 - a. Select **File | Advanced | Memory Card Command | Shutdown**.
 - b. The **Select IP Office** menu is displayed. Select the system and enter the administrator details when requested.
 - c. When prompted for which card to shutdown, select **System** and click **OK**.
2. On the back of the control unit, check that the LED for the memory card slot is off before removing the memory card.
3. Place the card into the PC's memory card slot and examine the contents.
4. Add any new files to the **System SD\SYSTEM\PRIMARY** folder.
5. When the card is reinserted into the system, card usage is automatically restarted.

3.2.2 Using Manager to Upload Files

Embedded file manager allows you to remote see the files on the memory card used by the telephone system. It also allows you to upload new files.

1. In IP Office Manager, select **File | Advanced | Embedded File Management**.
2. The **Select IP Office** menu is displayed.
3. Select the telephone system and click **OK**. Enter the name and password for the system. These are the same as used for configuring the system.
4. The contents of the memory card are displayed.



5. For an IP500 V2, use the folder tree to navigate to **System SD | SYSTEM | PRIMARY**. For a IP Office Server Edition system, use the folder tree to navigate to **system | primary**.
6. Individual files can be copied onto the card by using drag and drop or by selecting **File | Upload System Files**. The whole set of phone firmware files that IP Office Manager has available can be copied by selecting **File | Upload Phone Files**.

3.2.3 Using Web Manager to Upload Files

Within IP Office Web Manager you can use file manager to view files and if necessary upload new files.

1. Log into the system using IP Office Web Manager. Note: This process is not supported in Chrome.
2. Click **Applications** and select **File Manager**.

System Status : 192.168.0.210

Used Space (GB) Free Space (GB)

Total Disk Capacity: 3.6GB

Folders

- System Volume Information
- SYSTEM
 - BACKUP
 - backup_appl
 - DOC
 - DYNAMIC
 - LVMAIL
- PRIMARY
 - ACCS
 - certificates
 - EMAIL
 - HTML

Name	Date modified	Type	Size (kB)
1400Boot25.bin	Thu Apr 22 10:28:54 GMT...	bin	78 kB
1400LngR10v11Pack01.bin	Wed Sep 12 13:11:26 GM...	bin	101 kB
1400R46.BIN	Mon Apr 11 18:46:02 GM...	BIN	124 kB
1403Boot03.bin	Tue Apr 27 01:14:50 GMT...	bin	18 kB
1403R07.BIN	Mon Sep 30 19:47:00 GM...	BIN	175 kB
2410_R6.BIN	Fri Mar 06 06:49:40 GMT...	BIN	65 kB
2420_R6.BIN	Fri Mar 06 06:49:46 GMT...	BIN	75 kB
4601dbte1_82.bin	Mon Nov 13 03:32:56 GM...	bin	751 kB
4602dbte1_82.bin	Mon Nov 13 03:32:58 GM...	bin	747 kB
4602sbte1_82.bin	Mon Nov 13 03:32:58 GM...	bin	747 kB
5410_R6.BIN	Fri Mar 06 06:49:50 GMT...	BIN	66 kB
5420_R6.BIN	Fri Mar 06 06:49:56 GMT...	BIN	76 kB
5601bte1810.bin	Mon Mar 13 18:05:44 GM...	bin	751 kB
5602dbte1806.bin	Mon Mar 13 18:05:46 GM...	bin	747 kB
5602sbte1806.bin	Mon Mar 13 18:05:46 GM...	bin	748 kB
9500BootR15.bin	Tue Mar 22 09:52:00 GMT...	bin	20 kB

3. Open the **SYSTEM | PRIMARY** or **DISK | SYSTEM | PRIMARY** folder.
4. Click on the **+** icon to upload a new file.
5. Browse for and select the file to upload. Click **Upload File**.
6. Repeat the previous step to upload another file, otherwise click **Cancel**.

3.3 Loading Files onto a 3rd-Party Server

The phone firmware files are installed as part of the IP Office Manager application and are found in the application's installation directory. By default, the directory is found at **c:\Program Files (x86)\Avaya\IP Office\Manager**.

Note that these sets of files include firmware files that are also used for other devices including the system itself.

3.3.1 Adding Additional MIME File Types

Most HTTP/HTTPS file servers are already configured by default to serve common file types such as .txt, .zip and .tar files. However, there may be additional configuration required in order for the server to correctly respond to requests for newer file types such as .apk, .sig and .sig256 files.

The method used on most file servers is to add additional MIME types to the server's configuration (also called media or content types). The MIME type tells both the file server and the requesting device how to handle the particular file. In most cases, MIME types are configured based on file extensions. The exact method depends on the 3rd-party file server being used.

Example MIME Types:

File Extension	MIME Type
.apk	<i>application/vnd.android.package-archive or application/octet-stream</i>
.sig	<i>file/download</i>
.sig256	<i>file/download</i>

- The required setting for .apk files can vary depending on the version of Android requesting the file, so testing using either option is necessary.

To add a MIME type to an IIS Server:

1. Open the **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, go to the site, application or directory for which you want to add a MIME type.
3. In the **Home** pane, double-click **MIME Types**.
4. In the **Actions** pane, click **Add...**
5. In the **Add MIME Type** menu, add the file name extension and MIME type required and then click **OK**.

To add a MIME type to an IIS Sever configuration file:

1. Locate the server's configuration file. For example C:\Windows\System32\inetsrv\config\applicationHost.config.
2. Add the additional MIME types required to the <staticContent> section. For example:

```
<staticContent>
  <mimeTypeMap fileExtension=".apk" mimeType="application/vnd.android.package-archive" />
  <mimeTypeMap fileExtension=".sig" mimeType="file/download" />
  <mimeTypeMap fileExtension=".sig256" mimeType="file/download" />
</staticContent>
```

To add a MIME type to an Apache server:

MIME types can be added to the servers **httpd.conf** file. However, this requires the server to then be restarted for any changes to take effect. Alternatively, the new MIME types can be added to a **.htaccess** file placed in the same directory as the files. In either case, the MIME entries take the format:

```
AddType application/vnd.android.package-archive
AddType file/download .sig .sig256
```


Chapter 4.

Alternate DHCP Server Setup

4. Alternate DHCP Server Setup

The recommended installation method for IP phones uses a DHCP server. This section outlines by example, the basic steps for using a Windows server as the DHCP server for IP phone installation. The principles of defining a scope are applicable to most DHCP servers.

You will need the following information from the customer's network manager:

- The IP address range and subnet mask the IP phones should use
- The IP Gateway address
- The DNS domain name, DNS server address and the WINS server address
- The DHCP lease time
- The IP address of the IP Office unit
- The IP address of the PC running Manager (this PC acts as a file server for the IP phones during installation)

4.1 Checking for DHCP Server Support

To check the DHCP server support:

1. On the server, select **Start | Program | Administrative Tools | Computer Management**.
2. Under **Services and Applications** in the Computer Management Tree, locate **DHCP**.
3. If DHCP is not present then you need to install the DHCP components. Refer to the Microsoft documentation.

If the DHCP server role is supported, the first stage is to [create a scope](#)^[49] of addresses for use by IP phones.

4.2 Creating a Scope

A DHCP scope defines the IP addresses that the DHCP server can issue in response to DHCP requests. Different scopes may be defined for different types of devices.

To create a scope:

1. Select **Start | Programs | Administrative Tools | DHCP**.
2. Right-click on the server and select **New | Scope**.
3. The scope creation wizard will be started, click **Next**.
4. Enter a name and comment for the scope and click **Next**.
5. Enter the address range to use, for example, from 200.200.200.1 to 200.200.200.15 (remember the host part cannot be 0).
6. Enter the subnet mask as either the number of bits used or the actual mask, for example, 24 is the same as 255.255.255.0 and click **Next**.
7. You can specify addresses to be excluded. You can do this either by entering a range (e.g. 200.200.200.5 to 200.200.200.7) and clicking **Add**, or by entering a single address and clicking **Add**.
Note: You should exclude the IP Office from this range, as the DHCP Options in the IP Office should be disabled. This is only a recommendation. You can also accomplish this by leaving available addresses outside of the scopes range.
8. Click **Next**.
9. You can now set the lease time for addresses. If set too large, addresses used by devices no longer attached will not expire and be available for reuse in a reasonable time. This reduces the number of addresses available for new devices. If set too short, it will generate unnecessary traffic for address renewals. The default is 8 days. Click **Next**.
10. The wizard gives the option to configure the most common DHCP options. Select **Yes** and then click **Next**.
11. Enter the address of the gateway and click **Add**. You can enter several addresses. When all are entered, click **Next**.
12. Enter the DNS domain (eg. example.com) and the DNS server addresses. Click **Next**.
13. Enter the WINS server addresses and click **Add** and then click **Next**.
14. You will then be asked if you wish to activate the scope. Select **No** and then click **Next**.
15. Click **Finish**. The new scope will now be listed and the status is set to **Inactive**.

Having created the scope that will be used by the IP phones, [a set of options](#) need to be added matching the Site Specific Options Number (SSON) that the phones will use. The SSON used by 1600 and 9600 Series phones by default is 242.

4.3 Adding an Option

In addition to issuing IP address information, DHCP servers can issue other information in response to specific DHCP option number requests. The settings for each option are attached to the scope.

Most Avaya SIP phones use site specific option number (SSON) 242 to request additional information from a DHCP server (the E129 uses option 60). The option should include defining the address of the phone's file server.

To add an option:

1. Right-click on the DHCP server.
2. From the pop-up menu, select **Predefined options**.
3. Select **Add**.
4. Enter the following information:
 - **Name:** FileOptions
 - **Data type:** String
 - **Code:** 242
 - **Description:** IP Phone settings
5. Click **OK**.
6. In the string value field, enter the following options as a comma -separated string, for example **HTTPSRVR=xxx, HTTPPORT=y, HTTPDIR=z**:
 - **HTTPSRVR=** the HTTP file server DNS name or IP address.
 - **HTTPPORT=** the destination HTTP port. Only needed is the port differs from the default (80).
 - **HTTPDIR=** the HTTP file directory where the IP phone files are located. This entry is not required if those files are in the server's root directory.
 - **TLSSVR=** the HTTPS file server DNS name or IP address.
 - **TLSPORT=** the destination HTTP port. Only needed is the port differs from the default (443).
 - **TLSDIR=** the HTTPS file directory where the IP phone files are located. This entry is not required if those files are in the server's root directory.
 - Additional values can also be used, refer to the appropriate administration manual for the phone type, see [Additional Documentation](#) ^[2].
7. Click **OK**.
8. Expand the server by clicking on the **[+]** next to it.
9. Click on the scope you just created for the phones.
10. In the right-hand panel, right-click on the scope and select **Scope Options**.
11. In the general tab, make sure option number, for this example **242**, is checked.
12. Verify the String value is correct and click **OK**.

Having created a 242 option and associated with the scope we want used by the IP phones, we now need to [activate the scope](#) ^[5].

4.4 Activating the Scope

The scope can be manually activated by right-clicking on the scope, select **All Tasks** and select **Activate**. The activation is immediate.

You should now be able to start installing IP phones using DHCP. If Manager is being used as the HTTPS/HTTP file server, ensure that it is running on the specified PC.

Chapter 5.

Security Certificates

5. Security Certificates

The phone allow an initial connection to an HTTPS file server without validating the certificate chain as long as the server certificate name is validated. Then the phone will download TRUSTCERTS from the HTTPS server which should include a root CA for the HTTPS server certificate. So when the phone is rebooted it will have the proper TRUSTCERTS to fully validate the HTTPS connection.

- **Local Extension**

If the phone is installed in the local network, the phone initially downloads the system's root certificate using an unsecured HTTP connection. You need to ensure that the system's root certificates have been installed in the system's Trusted Secure Certificate store, see [Adding a Root CA Certificate to the IP Office TCS](#) ^[55].

- **Remote Worker Extensions**

In case when the phone is installed in the remote network, the IP Office system's root certificate need to be pre-installed on the phone. This can be done as follows:

- **Option 1:**

Connect the phone to the local network and make sure that the phone's HTTP server points to the IP Office system. In the initial installation, the phone will download the IP Office's root certificates.

- **Option2:**

Using a 3rd-party HTTP server, place the IP Office root certificate **WebRootCA.pem** that on the file server. Configure the remote phone to use that HTTP server

5.1 Using the IP Office Certificate

For Avaya SIP phones, the **TRUSTCERTS** setting in the downloaded settings file indicates the name of the certificate that the phone should request from the file server. The default name is **WebRootCA.pem**.

If using the IP Office as the file server and auto-generated phone settings files, no further configuration is required. The certificate name is automatically set in the settings file and the IP Office automatically provides its own identity certificate in response to requests for that file.

If using an alternate file server then:

- The setting file for the phones on the file server must have a **TRUSTCERTS** entry specifying the name of the certificate file the phones should request.
- The matching certificate file must be placed onto the file server.

If the certificate to use is still the IP Office system's own certificate, it can be downloaded from the system using web manager as follow:

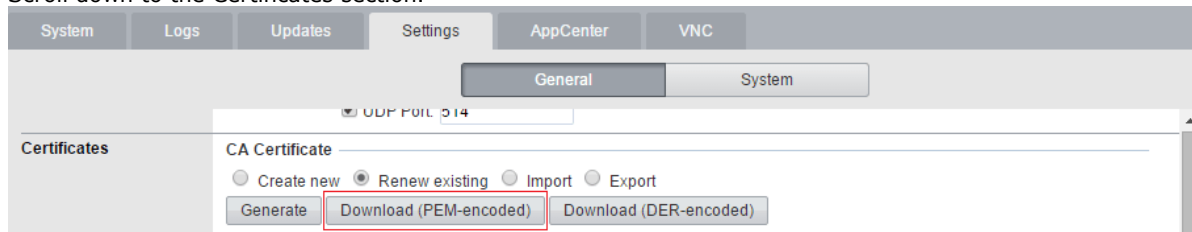
- [Downloading the IP Office certificate from an IP500 V2](#) ^[54]
- [Downloading the IP Office certificate from a Linux based IP Office](#) ^[53]

5.1.1 Downloading the Linux Certificate

Use the following process to download the system's current identity certificate. The certificate file can then be renamed and uploaded to the file server being used by the IP Phones.

To download the root certificate from a Linux based IP Office system:

1. Browse to the IP Office system IP address, ie. http://<server_address> and select **IP Office Web Manager**.
2. Login with an administrator account.
3. Click on **Solution**.
4. Click on the ☰ icon next to the system and select **Platform View**.
5. Select Settings | General.
6. Scroll down to the Certificates section.



7. Click Download (PEM-encoded) to download the system's certificate file.
8. Rename the file as **WebRootCA.pem**. This is the default name set in the settings file using the **TRUSTCERTS** parameter.
9. [Upload the file to the file server](#)^[44] being used by the phones. .

5.1.2 Downloading the IP500 V2 Certificate

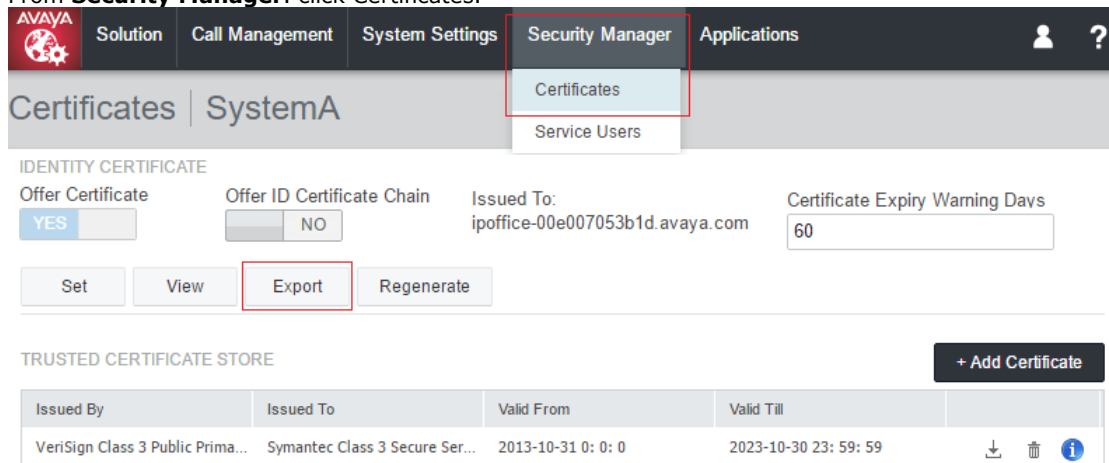
Use the following process to download the system's current identity certificate. The certificate file can then be renamed and uploaded to the file server being used by the IP Phones.

To downloading the root certificate from an IP500 V2:

1. Browse to the IP Office system IP address, ie. http://<server_address>.



2. From the web page select **IP Office Web Manager** and login to the system.
3. From **Security Manager**, click Certificates.



4. Click **Export** to download the system's certificate file.
5. Rename the file as **WebRootCA.pem**. This is the default name set in the settings file using the **TRUSTCERTS** parameter.
6. [Upload the file to the file server](#) being used by the phones.

5.2 IP Office Certification

5.2.1 Adding a Root CA Certificate to the IP Office TC

When deployed, the phone attempts to download the root CA certificate from its file server. It then stores that file in its **Trusted Certificate Store**.

To add certificates to the IP Office system's trusted certificate store using IP Office Web Manager:

- Obtain the root CA certificate from whichever source you use for certification.
 - IP Office Own Certificate**
If the IP Office signs its own certificates, no further steps are required. The system has its own root CA certificate already installed in its **Trusted Certificate Store** and provides that certificate when requested by the phone.
 - Another IP Office**
If you are using another IP Office to generate certificates, download the root CA certificate from that IP Office. See [Using the IP Office Certificate](#) ^[52].
 - Other Certification**
If you use another source for signing certificates, you will need to add the root CA certificate from that source to the IP Office's trusted certificate store.
- If you are using a certificate from another IP Office or other source, you need to add the root CA certificate to the IP Office systems trusted certificate store.
 - IP Office Manager:** Access the system's security settings. Click **System** and select the **Certificates** tab.
 - IP Office Web Manager:** Click Security Manager and select Certificates.

Issued By	Issued To	Valid From	Valid Till	
VeriSign Class 3 Public Primary Certifica...	Symantec Class 3 Secure Server CA - G4	2013-10-31 0: 0: 0	2023-10-30 23: 59: 59	↓ 🗑️ ⓘ
VeriSign Class 3 Public Primary Certifica...	VeriSign Class 3 International Server CA...	2010-2-8 0: 0: 0	2020-2-7 23: 59: 59	↓ 🗑️ ⓘ
SIP Product Certificate Authority	SIP Product Certificate Authority	2003-7-25 0: 33: 17	2027-8-17 5: 19: 39	↓ 🗑️ ⓘ

- Click **Add** or **+Add Certificate** and select the root CA certificate.
- Ensure that you save a copy of the certificate. It also needs to be added to the certificate stores of the file server is using HTTPS for provisioning.

To add a certificate using file manager:

Certificate files (.PEM and .DER) can be placed directly into the system memory. Those files are loaded into the system's trusted certificates store the next time the system is restarted or its security settings reset.

- Using one of the methods for [loading files onto the system](#) ^[41], add the certificate to the **/SYSTEM/PRIMARY/certificates/TCS/ADD** folder.

5.2.2 Create an Identity Certificate for the IP Office

This example assumes that the IP Office Server Edition server is the certificate authority. In that role it can also be used to create identity certificates for other servers including other IP Office's. That includes creating an identity certification for the IP Office service.

To create an identity certificate for the IP Office:

1. Within the server's web management menus, select **Platform View**.
2. Select **Settings** and then **General**.
3. Locate the **Certificates** section and select **Create certificate for a different machine**.

☒ Create certificate for a different machine

Machine IP:

Password:

Confirm Password:

Subject Name:

Subject Alternative Name(s):

Duration (days):

Public Key Algorithm:

Secure Hash Algorithm:

Password complexity requirements:

- Minimum password length: 8
- Minimum number of uppercase characters: 1
- Minimum number of lowercase characters: 1
- Maximum allowed sequence length: 4

4. In the fields below that, enter the details for the IP Office's SIP server. The **Subject Alternative Name(s)** field should include the following entries, each separated by a comma. Multiple entries are required if using both LAN1 and LAN2:
 - DNS entries for the system's LAN1 and/or LAN2 SIP Domain Name, eg. **DNS:example.com**
 - DNS entries for the system's LAN1 and/or LAN2 SIP Registrar FQDN, eg **DNS:ipoffice.example.com**
 - IP entries for the system's LAN1 and/or LAN2 IP addresses, eg. **IP:192.168.42.1, IP:192.168.43.1**
 - If supporting remote workers, add an IP entry with the public IP address of the IP Office.
 - SIP URI entry for the LAN1 and/or LAN2 SIP Domain Name, eg. **URI:sip:example.com**
 - SIP URI entry for the LAN1 and/or LAN2 IP address, eg. **URI:sip:192.168.42.1**
 - If using a separate HTTPS file server, add a SIP URI entry for the file server's domain name.
5. Click on the lower **Regenerate** button.
6. Click on **Download (PEM-encoded)** to download the file.

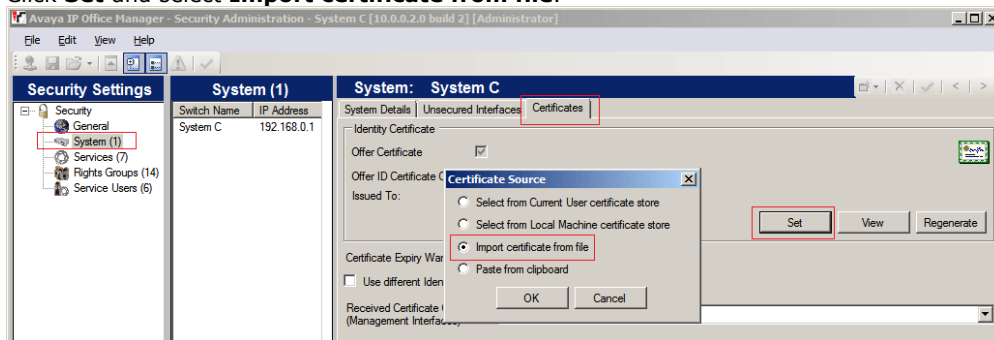
5.2.3 Add the Identity Certificate to the IP Office

To add the identity certificate to the IP Office:

- Using IP Office Manager, access the system's security settings.

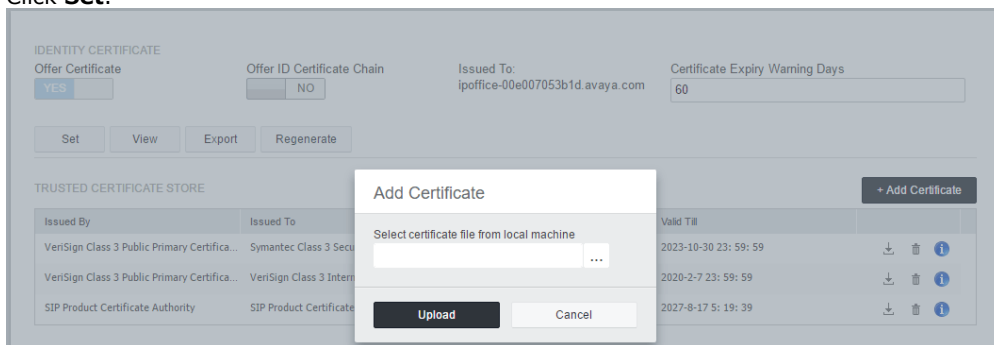
- **IP Office Manager:**

- Access the system's security settings. Click **System** and select the **Certificates** tab.
- Click **Set** and select **Import certificate from file**.



- **IP Office Web Manager:**

- Click **Security Manager** and select **Certificates**.
- Click **Set**.



- Select the [previously generated IP Office identity file](#) and load it.
- The IP Office now has a trusted root CA certificate and an identity certificate signed by that root certificate. The identity certificate has the alternate name values required by the phone for proper security.

5.3 File Server Certification

The same root CA certificate [added to the IP Office system](#)^[58] should also be added to the file server. If the IP Office is signing its own certificate, this is the PEM certificate downloaded from the IP Office system.

5.3.1 Add the Certificates Snap-In

To install certificates, you must first enable the Certificates Snap-in for the Microsoft Management Console (mmc).

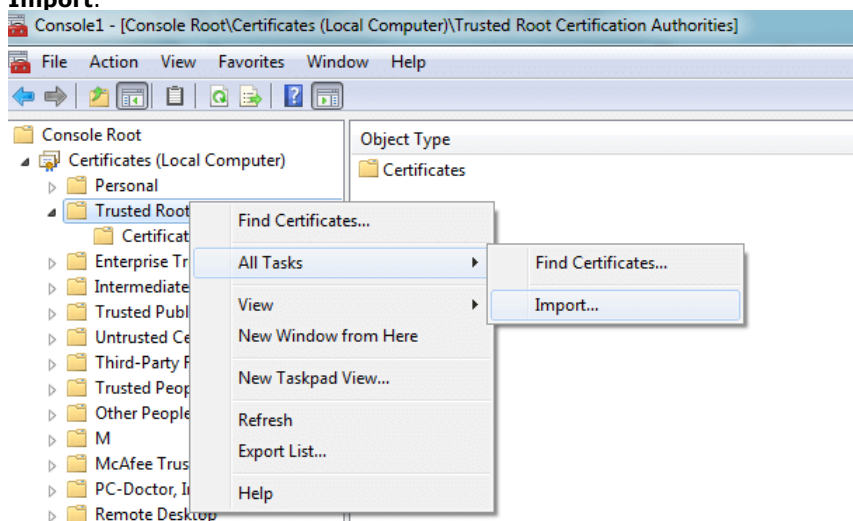
To enable the Certificates Snap-In:

1. Click the **Start Button**.
2. Select **Run** and type **mmc**.
3. Click **File** and select **Add/Remove Snap in**.
4. Select **Certificates** from the **Available Snap-ins** box and click **Add**.
5. Select **Computer Account** and click **Next**.
6. Select **Local Computer** and click **Finish**.
7. Click **OK**.
8. Return to the MMC.

5.3.2 Add the Trusted Root CA Certificate to the Windows Certificate Store

To add the trusted root CA certificate to the Windows certificate store@

1. Click the **Start Button**.
2. Select **Run** and type **mmc**.
3. Expand the **Certificates** and right-click **Trusted Root Certification Authorities**. Click **All Tasks** and select **Import**.



4. This starts the **Certificate Import Wizard**:
 - a. Click **Next** and the file import dialog opens.
 - b. Locate the trusted root CA certificate file (**root-CA.pem**) downloaded earlier and click **Next**.
 - c. Click **Next** to confirm the location **Trusted Root Certification Authorities**.
 - d. When the wizard is completed, click **OK**.
5. If you have any intermediate signing authorities, use the similar process to add them to the **Intermediate Certification Authorities** store.
6. You can exit console now.

5.3.3 Create an Identity Certificate for the File Server

When the phone sends an HTTP request to the IP Office, it receives a 307 redirect message pointing to the HTTP server and resends the request to that server. But to open an HTTPS connection to the server, it needs to validate the server's identity by verifying the IIS server's identity certificate against a known signing authority.

We have just given the phone a trusted root CA certificate from our signing authority, so if we give the IIS server an identity certificate signed by the same signing authority, the same trusted root CA certificate on the phone can be used. To do this we can give the server the same root CA certificate and its own identity certificate.

To create an IP Office identity certificate for file Server:

In this example, the IP Office Server Edition is being used to sign certificates (it is the certificate authority). Therefore, it can also be used to create identity certificates for other PCs that it will sign, in this case an identity certificate for the IIS server.

1. Within the server's web management menus, select **Platform View**.
2. Select **Settings** and then **General**.
3. Locate the **Certificates** section.
4. Select **Create certificate for a different machine**.

☒ Create certificate for a different machine

Machine IP:

Password:

Confirm Password:

Subject Name:

Subject Alternative Name(s):

Duration (days):

Public Key Algorithm:

Secure Hash Algorithm:

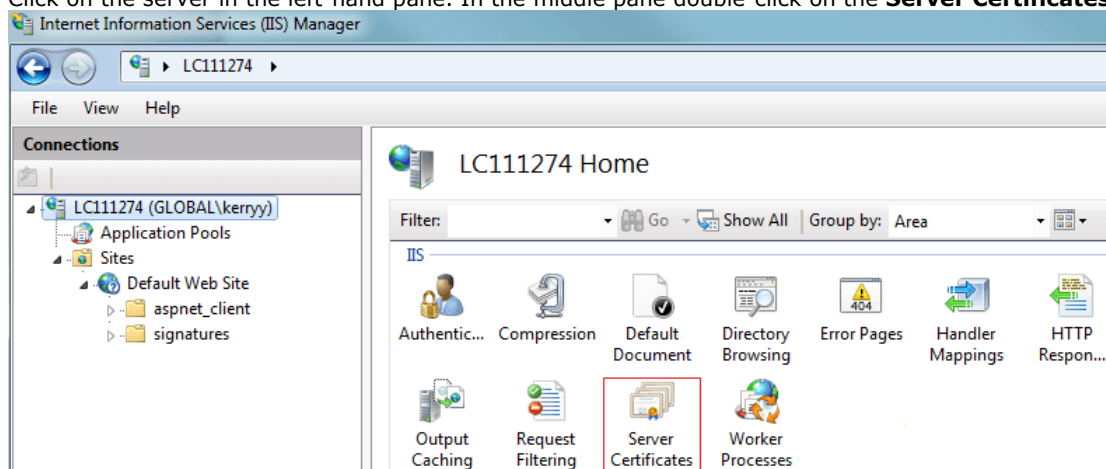
5. In the fields below that, enter the details for that PC. In this example, the computer hosting the IIS server has a single FQDN and numerous IP addresses. This information is all added to the Subject Alternative Names field:
DNS:fileserver.example.com, IP:192.168.0.201, IP:203.0.113.10
6. Click on the lower **Regenerate** button.
7. Click on **Download (PEM-encoded)** to download the file.
8. The identity certificate can now be [added to the web server](#).

5.3.4 Add the Identity Certificate to the File Server

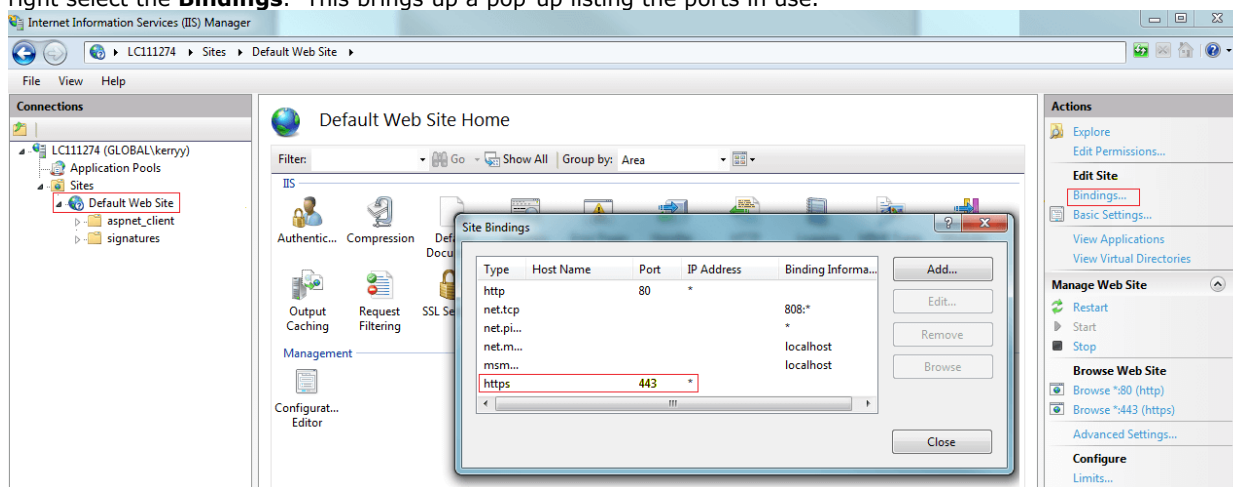
The identity certificate [generated for the server](#)^[59] needs to be added to the HTTP server.

To add an identity certificate to a Microsoft IIS server:

1. Open the **Internet Information Services (IIS) Manager** by entering **iis** in the Start Menu and selecting the program.
2. Click on the server in the left-hand pane. In the middle pane double-click on the **Server Certificates** icon.



- a. On the far right of the window that appears click on **Import...**
 - b. Browse to P12 format certificate file and select it.
 - c. After importing the certificate, you can right click on it and select details. Scroll down to verify that the **Subject Alternative Name** contains all of the fields that you set when you [created the identity certificate](#)^[56].
3. You now need to configure the web server to use the certificate. Within IIS, select the web site to use and on the right select the **Bindings**. This brings up a pop-up listing the ports in use.



- a. Select the **https** binding on the default secure port **443**, and click on **Edit**.
 - b. In the SSL certificate drop-down, select the certificate to use. Click **OK**.
 - c. Click **Close**.
4. Close IIS Manager.

Chapter 6.


Monitoring SIP Phones

6. Monitoring SIP Phones

6.1 Viewing SIP Phone Communications

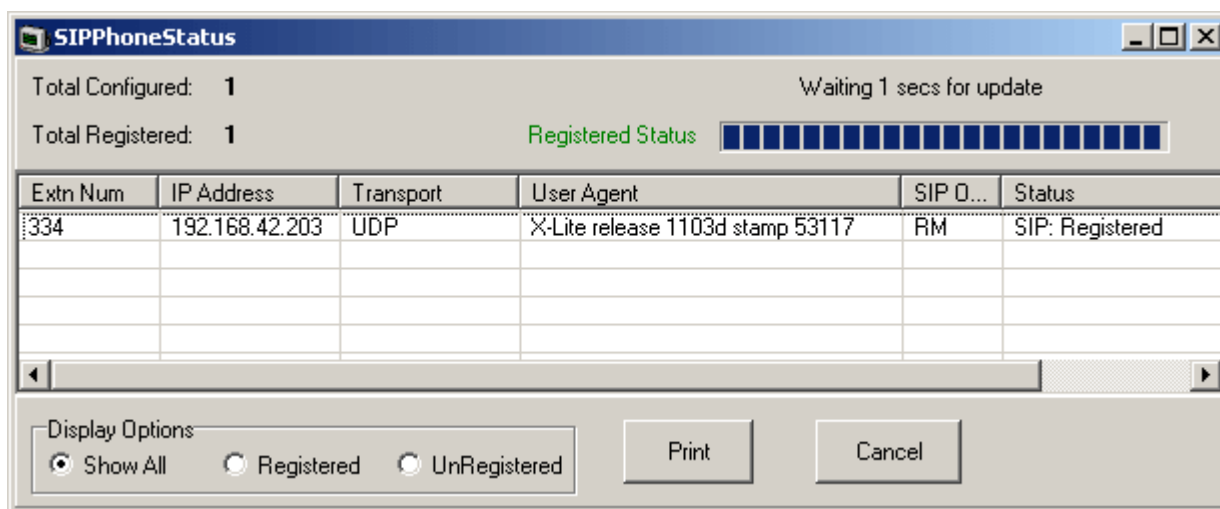
The System Monitor trace can be set to include SIP registration traffic, DHCP requests and HTTP file transfers.

To monitor SIP extension registration process:

1. Click the  **Trace Options** icon. Alternatively, press Ctrl+T or click **Filters** and select **Trace options**.
2. On the **Services** tab, select **HTTP** and **DHCP**.
3. On the **SIP** tab, select **SIP Reg/Opt Rx** and **SIP Reg/Opt Tx**.
4. If more detail are required, also select **SIP** and set the level to **Verbose**.
5. Click **OK**.

6.2 Viewing Registrations

The status of the SIP extensions in the IP Office configuration can be viewed using the System Monitor application. Select **Status | SIP Phone Status** to display the SIP extension list.



The screenshot shows the SIPPhoneStatus window. At the top, it displays 'Total Configured: 1' and 'Total Registered: 1'. A green bar indicates the 'Registered Status'. Below this is a table with the following data:

Extn Num	IP Address	Transport	User Agent	SIP O...	Status
334	192.168.42.203	UDP	X-Lite release 1103d stamp 53117	RM	SIP: Registered

At the bottom, there are 'Display Options' with radio buttons for 'Show All' (selected), 'Registered', and 'UnRegistered'. There are also 'Print' and 'Cancel' buttons.

6.3 Registration Blacklisting

The IP Office system logs failed H323/SIP registration requests. Multiple failed attempts can lead to the extension and/or IP address becoming blocked for a period.

Blocking applies as follows:

- **Extension Blocking**
Registration attempts to an existing extension using the wrong password are blocked for 10 minutes after 5 failed attempts in any 10 minute period.
- **IP Address Blocking**
Registration attempts to a non-existent extension or using the wrong password of an existing extension are blocked for 10 minutes after 10 failed attempts in any 10 minute period.

When blocking occurs, the system generates an alarm in System Status and adds an entry to its audit log. A system alarm is also generated and can be output using any of the supported system alarm routes (SMTP, SNMP, Syslog). System Monitor can display details of blacklisted IP addresses and extensions, select **Status | Blacklisted IP Addresses** and **Status | Blacklisted Extensions**.

6.4 Syslog Monitoring

The J100 Series stimulus phones (J169, J179) support syslog output. This can be directed to a syslog server and used to capture details of the phone operation.

To configure and enable syslog output:

1. Access the **Admin** menu.
2. Select **Log**
3. Select the **Log level** required. The options are ***Emergencies, Alerts, Critical, Errors, Warnings, Notices, Information*** and ***Debug***.
4. Set **Remote logging enabled** to on.
5. Select the **Remote log server** and enter the address to which the syslog records should be sent.
6. Click **Save** to save the changes.

Chapter 7.

J100 Series Phone Installation Notes

7. J100 Series Phone Installation Notes

The IP Office supports the J129 telephone from IP Office Release 10.0 SP2 onwards. The J169 and J179 are supported from IP Office Release 11.0.

7.1 J129

The J129 is a basic desk phone that supports 2 call appearances with a single line call display. The phone does not have any user programmable buttons for local or IP Office features.

This section provides additional notes on installation and operation of these phones with IP Office systems. For additional information refer to the *"Installing and Administering J100 Series IP Deskphones SIP"* manual. See [Additional Documentation](#) ^[2].

The IP Office supports the J129 telephone from IP Office Release 10.0 SP2 onwards.

7.1.1 Restrictions/Limitations

- **Emergency Calls**

The **Emerg** soft key feature is not supported. Emergency calls are not available when the phone is not registered.

- **Conferencing**

When used with IP Office, the phone's conference button creates a 3-way conference hosted locally on the phone rather than the IP Office.

- Conferencing using other IP Office methods such as short codes is supported.
- IP Office based ad-hoc conferences are not supported.
- For the phone hosted conference, the other parties cannot hear each other when the J100 Series phone puts the conference on hold.

- **Distinctive Ringing**

There is no support for distinctive ringing on this phone (no different ringing for trunk calls compared to local calls).

- **# Key Usage**

J100 telephones do not use # to indicate dialing complete, instead the # key is treated as part of the dialed number. Dialing is completed by time out of the inter digit dialing timer set in the phone configuration file (default 5 seconds, minimum 1 second, maximum 10 seconds).

- **Media Security/SRTP**

SRTP with AES-256 crypto suite is not supported.

- **Certificates**

- SCEP certificate handling is not supported.
- The phone only requests a certificate during its first connection if TLS is enabled and it has no certificate with the same name already present.

- **Unsupported Phone Features:**

The following options are

- **Call Frwd** menu.
- **Contacts** menu.
- **Transfer on Hangup.**
- **Automatic Callback.**

7.1.2 Known Problems

- **Persistent "Acquiring Service" State**

This message can be seen if the phone is attempting to register using TLS on a system where TLS is not enabled or the certificates were not properly configured for TLS phone support before connecting the phones. The resolution is to disable TLS or upload a suitably configured certificate and then perform a [factory reset](#)^[69] on the phone.

- **Changing IP Office Systems**

To switch a phone between different IP Office systems requires a [factory reset](#)^[69] of the phone. This is due to root certificate name for the **TRUSTCERTS** settings on each system being the same (**WebRootCA.pem**). The phones cannot distinguish between different certificates with the same name.

- **Changing HTTPS Servers**

To switch between different HTTPS servers may require a [factory reset](#)^[69]. This is needed to ensure clearing any previously installed HTTPS file server root certificate. This is not necessary if both HTTPS servers have identity certificates signed by the same root certificate authority.

- **Changing from HTTPS server to HTTP server:**

To switch the phone from a HTTPS file server to a HTTP file server when TLS is configured on the IP Office, requires a [factory reset](#)^[69] on the phone. This is needed since IP Office initially configures the phone to use HTTPS when TLS is configured.

7.1.3 Files

During a restart, J100 Series telephones requests a series of files, using HTTPS or HTTP, from the [configured file server](#)^[38]. The various files, in the order that the phone requests them, are:

- **J100Upgrade.txt**

Details the firmware supported by the IP Office system. Used by the phone to request those firmware files if necessary. If using the IP Office system as the file server, the file is [auto-generated](#)^[14] if not physically present.

- **46xxsettings.txt**

Details the phone settings for various different models of supported phones including the SIP server settings. If using the IP Office system as the file server, the file is [auto-generated](#)^[14] from the system settings if no file is physically present.

- **FW_S_J129_R1_0_0_0_35.bin (example)**

This type of file is the phone firmware file. The file name indicates the particular model of phone the file is for and the release number of the firmware. If the phone downloads new firmware, the firmware upgrade takes up to 10 minutes. From IP Office Release 10.0 SP3 onwards, the supported firmware is part of the IP Office Manager for each release and is installed on the system as part of the upgrade process.

- **WebRootCA.pem**

If using TLS, the phone requires an appropriate certificate downloaded from the file server.

- **Language .XML Files**

The settings file will indicate if the phone should request any language files. If using the IP Office system as the file server, for IP Office Release 10.0 SP3 onwards, the file is [auto-generated](#)^[14] from the system settings if no file is physically present.

7.1.4 Simple Installation

The following is an outline for simple J129 installation. It assumes that the IP Office is being used as both the DHCP and file server and is using its own security certificate.


Process Summary:

1. For IP Office R10 SP2:
 - a. Download the J129 firmware file set from the IP Office download pages on support.avaya.com.
 - b. Unpack the files to a temporary folder.
 - c. [Upload the files to the system's primary folder](#) ⁴¹.
2. [Enable SIP extension support on the system](#) ²⁵.
3. Create the [SIP users](#) ³¹ and [SIP extensions](#) ³².
4. [Attach and register the phones](#) ³⁵.

7.1.5 Static IP Address Configuration

The following process is used for static address administration on J100 Series phones.

To statically set the telephone IP address:

1. If already shown on the display, select **Admin**, otherwise press the  **Menu** button and select **Admin**.
2. In the **Access code** field, enter the admin password and press **Enter**.
3. Scroll down to **IP Configuration** and press **Select**.
4. Scroll to **IPv4** and press **Select**.
 - a. For the **Use DHCP** option, press **Change** to set the mode to **No**.
 - b. Press **Save**.
5. Scroll to **IPv4** again and press **Select**.
 - a. Set **Phone** to the IP address required for the phone. Use the * key to enter a '.' character in IP addresses.
 - b. Scroll down and set **Gateway** to the IP Office LAN address.
 - c. Scroll down and set **Netmask** to the network subnet mask.
 - d. Press **Save**.
4. Scroll down to **Servers** and press **Select**.
 - a. Set the **HTTP Server** and/or **HTTPS Server** address to the file server IP address. When both are set, HTTPS is tried before HTTP. If the IP Office is used as the file server, enter the IP Office LAN1 or LAN2 address.
 - b. Set the **DNS Server** address. This must be configured when using static addressing.
 - c. Select **Save**.
5. Press **Back** to exit from the **IP Configuration** and then the **Admin** menus. The phone restarts automatically.
6. When prompted to enter the user credentials, at the **Username** prompt enter the user extension number and then the user password.

7.1.6 SIP Settings Configuration


The J100 settings file downloaded by the phone includes the settings for the SIP servers and protocols it should use. If the settings file is [auto-generated](#)^[14], then those settings are based on the SIP values set in the IP Office system configuration. Otherwise, if using a manual settings file uploaded to the file server, the [file should be edited](#)^[15] to specify the SIP server settings.

7.1.7 Changing the Phone SSON

The default SSON used by most Avaya SIP phones is 242. When using DHCP for installation, this SSON value needs to be matched by a DHCP option defining the file (provisioning) server addresses.

If necessary, the SSON used by the telephone can be changed.


To change the SSON of a J100 Series phone:

1. If already shown on the display, select **Admin**, otherwise press the  **Menu** button and select **Admin**.
2. In the **Access code** field, enter the admin password and press **Enter**.
3. Scroll down to **SSON** and press **Select**.
4. Enter the new setting between 128 to 254.
5. Press **Save**.

7.1.8 Viewing the Phone Settings


The current key settings being used by a J100 Series phone can be inspected.

To view the phone's settings:

1. If already shown on the display, select **Admin**, otherwise press the  **Menu** button and select **Admin**.
2. In the **Access code** field, enter the admin password and press **Enter**.
3. Scroll down to **View** and press **Select**.
4. Use the cursor keys to scroll through the settings and their current values.
5. Press **Back** to return to the normal menu.

7.1.9 Factory Reset

To factory reset a J100 Series telephone:

1. If already shown on the display, select **Admin**, otherwise press the  **Menu** button and select **Admin**.
2. In the **Access code** field, enter the admin password and press **Enter**.
3. Scroll down to **Reset to defaults** and press **Select**.
4. Press **Reset**.

7.2 J169/J179

The J169/J179 SIP phones are supported from IP Office Release 11.0. They support an operating mode referred to as 'stimulus' mode, enabled by the setting `SET ENABLE_IPOFFICE 2` in the settings file. In that mode they support the full set of IP Office phone menus

They can largely be installed using the [generic installation process](#)^[24], which provides the phones with the required *J100Supgrade.txt* and *46xxsettings.txt* files. Both phones support PoE or an optional separate 5V dc. power supply unit.

7.2.1 System Settings

If adding these phones to an existing system with a static *46xxsettings.txt* file, it is recommended that you first examine the settings in the system's auto-generated *46xxsettings.txt* file and compare them to your static file. The key sections relevant to J169/J179 telephone operation are in labeled `J1X9AUTOGENERATEDSETTINGS`, `STIMULUSPHONECOMMONSETTINGS` and `STIMULUSSETTINGS`. See [The 46xxsettings.txt File](#)^[134].

If the correct settings are not specified, the J169/J179 phones will operate as standard SIP telephone with no IP Office specific menus.

7.2.2 Simple Installation

This is the simplest method of initial phone connection. It assumes that the phone receives its address from DHCP.

This process takes approximately 10 minutes to complete. If a software upgrade is required, the whole process takes approximately 15 minutes to complete.


To initially configure the phone:

1. Connect the LAN cable to the phone. If not using PoE, connect the power adapter cable.
2. The lamp (top-right) comes one though the screen remains blank.
3. The phone goes through its software loading cycle. During this it displays the Avaya logo above a progress bar, followed by displaying the Avaya splash screen.
4. At the **Do you want to activate Auto Provisioning now?** prompt select **Yes** or **No**.
5. The phone displays **Starting....** followed by **Waiting for DHCP....**
6. If the DHCP response did not include the file server address the phone should use, the phone displays at the **Configure provisioning server** or **Enter file server address** prompt. Select **Config**.
 - a. Enter the address of the server holding the *J100Supgrade.txt* file. You must prefix the address with **http://** or **https://**.
 - b. Check the address and click **Save**. If **Connection Error** is displayed, check and correct the file server address.
7. The phone displays **Restarting...** and then repeats its software loading cycle.
8. If the phone needs to load new software from the file server, it displays **Updating software** and a progress bar after which it restarts again.
9. When the phone displays **Login**. Enter the following:
 - For the **Username**, enter the extension number.
 - For the **Password**, enter the extension's **Phone Password** as set in the IP Office configuration.

7.2.3 Complex Installation

This method can be used to configure the phone for scenarios such as not using DHCP.

To configure the phone:


1. Attach the network cable.
2. Access the administration menu:
 - a. If shown on the display, press **Admin**. Otherwise, press **More** and **Admin** or press  and select **Administration**.
 - b. Enter the administration password and press **Enter**. These phones do not support pressing **#** to enter the password.
3. **If you want the phone to use WiFi: (J179)**
Wireless connection is supported on J179 phones with the optional WiFi module installed.
 - a. Select **Network interfaces**.
 - b. Change the **Network mode** from **Ethernet** to **Wi-Fi**.
 - c. Press **Save**.
 - d. The phone scans for available wireless networks.
 - e. Select the required network and click **Connect**. Press **OK**.
 - f. In the **Password** field, enter the password for the wireless network and press **Connect**.
 - g. If the phone is able to connect to the network, it is restarted.
4. Select **IP Configuration**.
5. **If you want to use a static address rather than DHCP:**
 - a. Select **Ethernet IPv4** or **Wi-Fi IPv4** depending on whether the phone was connected to the network using a wired connection or WiFi.
 - b. Change **Use DHCP** to off.
 - c. Set the **Phone**, **Gateway** and **Mask** details to match the requirements of the customer network.
 - d. Click **Save**.
6. **Set the File Server:**
If the phone has not obtained the file server address through its initial DHCP start-up (for example it is not getting DHCP from the IP Office or from a DHCP server configured with Option 242), then the file server address needs to be configured manually:
 - a. Select **Servers**.
 - b. Enter the **HTTPS server** and or **HTTP server** address of the file server containing the J100 settings and firmware files.
 - c. Press **Save**.
7. Press **Back** until you exit the admin menus. At this point the phone is restarted with its new settings.
8. After restarting, the phone should display the login menu. Enter the IP Office extension number and phone password.
 - **! Important:**
For J169/J179 telephones, the extension **Phone Password** must be used for initial registration of the telephone.
 - If the phone displays "*SIP proxy list is empty*" check the file server settings are correct. The SIP proxy details are provided by the *46xxsettings.txt* file.

7.2.4 Additional Processes

7.2.4.1 Restart

This process restarts the phone.



To reset the phone:

1. Access the administration menu.
 - a. If shown on the display, press **Admin**. Otherwise, press **More** and **Admin** or press  and select **Administration**.
 - b. Enter the administration password and press **Enter**. These phones do not support pressing **#** to enter the password.
2. Scroll down to and select **Restart phone**.
3. Press **Restart**.

7.2.4.2 Reset

This process returns the phone to its default settings, that is DHCP client operation through the wired Ethernet connection.


To reset the phone:

1. Access the administration menu.
 - a. If shown on the display, press **Admin**. Otherwise, press **More** and **Admin** or press  and select **Administration**.
 - b. Enter the administration password and press **Enter**. These phones do not support pressing **#** to enter the password.
2. Scroll down to and select **Reset to Defaults**.
3. Press **Reset**.
4. When the phone restarts, follow the process for [initial configuration](#) .

7.2.4.3 Enabling WiFi

The J179 phone can be fitted with a wireless module. This then allows it to connect to the telephone system via the customer's WiFi network. This option allows the phone to be used in a location where a wired ethernet connection is not available.

To enable wireless operation:

1. Access the administration menu.
 - a. If shown on the display, press **Admin**. Otherwise, press **More** and **Admin** or press  and select **Administration**.
 - b. Enter the administration password and press **Enter**. These phones do not support pressing **#** to enter the password.
2. Then:
 - a. Select **Network interfaces**.
 - b. Change the **Network mode** from **Ethernet** to **Wi-Fi**.
 - c. Press **Save**.
 - d. The phone scans for available wireless networks.
 - e. Select the required network and click **Connect**. Press **OK**.
 - f. In the **Password** field, enter the password for the wireless network and press **Connect**.
 - g. If the phone is able to connect to the network, it is restarted.

7.2.4.4 Branch Deployment

In addition to support as local IP Office extensions, J169/J179 phones are also supported as Avaya Aura extensions which, in rainy-day scenarios, can failover to the IP Office for basic call functions. Within the IP Office configuration these are referred to as 'centralized' extensions. This is called 'branch deployment'.

In this scenario, it is important to ensure that the centralized extensions do not start using the settings files intended for local extensions. This is done through the use of the GROUP setting on the phones:

- Natively IP Office extensions should be left with the default **GROUP** setting of **0**.
- Centralized Avaya Aura extensions be configured with a **GROUP** setting between 1 and 5 (see below).
- Add **GROUP** Redirection to the Settings File:
 - **If the system is using an auto-generated settings file:**
Add the NoUser source number **BRANCH_PHONES_GROUP X** to the IP Office configuration, where **X** is the GROUP number between 1 and 5 that the centralized extensions should use. The NoUser source number adds the setting *GET 46xxBranchsettings.txt* to the IP Office system's auto-generated 46xxsettings.txt file.
 - **If the system is using a static 46xxsettings.txt file:**
Manually add the settings to ensure that GROUP X phones are instructed to *GET 46xxBranchsettings.txt*.
- Add a 46xxBranchsettings.txt file to the IP Office or IP Office file server. Use that file to specify the settings for centralized extensions. This is covered in the IP Office branch deployment documentation.

7.2.5 Troubleshooting

7.2.5.1 No "Features" Menus

If the J169/J179 telephone does not receive the correct [settings](#)^[70], it will not display the IP Office specific menus. Principally the **Features** menu is not shown on the main screen. The key setting is `SET ENABLE_IPOFFICE 2`.

7.2.5.2 Monitoring


The J169/J179 phones can be monitored in the same way as for normal SIP extensions, see [Monitoring SIP Phones](#)^[62]. However, in addition the 'stimulus' traffic can be monitored using the following trace options:

- **Filters | Trace Options... | H.323 | CCMS Send**
- **Filters | Trace Options... | H.323 | CCMS Receive**
- **Filters | Trace Options... | SIP | SIP: Verbose**

7.2.5.3 Logging

The J169/J179 phones support logging to a Syslog server. This is configured through the phone's administrator menus.

To enable logging:

1. Access the administration menu:
 - a. If shown on the display, press **Admin**. Otherwise, press **More** and **Admin** or press  and select **Administration**.
 - b. Enter the administration password and press **Enter**. These phones do not support pressing **#** to enter the password.
2. Select **Log**.
 - Using **Log levels**, select the alarm level of events to include in the log output.
 - Using **Log categories**, select the types of events to include in the log output and click **Save**.
 - Using **Remote log server**, set the address of the server which should receive the log outputs.
 - Select **Remote logging enabled** and enable the function.
3. Click **Save**.

7.2.6 Pre-R11.0 H.323 Support

On IP Office R11.0 and higher systems, the J169/J179 phones are supported as SIP telephones only. However, for pre-R11.0 systems it is also possible to support J169/J179 phones in a mode that emulates H.323 phones using a special release of firmware. In this mode, the phones are seen by the IP Office system as being 9611 phones.

- **[Pre-IP Office 10.1 SP3 Systems](#)**

These systems require the manual addition of the firmware and editing of the settings files.

- **[IP Office 10.1 SP3 and later 10.1 service packs](#)**

These systems include the changes necessary to support J169/J179 telephones in H.323 mode. That assumes that the system is using the auto-generated 46xxsettings.txt file. If not, manual changes to the settings files being used will be required similar to those needed on pre-IP Office 10.1 SP3 systems.

- **IP Office R11.0 and higher**

These systems only support J169/J179 phones running SIP firmware. Existing systems with J169/J179 phones running H.323 emulation firmware will require the phones to be converted to SIP firmware after the upgrade of the IP Office to R11.0.

7.2.6.1 Pre-IP Office 10.1 SP3 Systems

The processes below cover the steps necessary to support J169/J179 phones on pre-IP Office 10.1 SP3 systems.

- **! Warning**

Once these processes have been complete, additional steps are required if the system is subsequently upgraded to IP Office 10.1 SP3 or higher. See [Upgrading Systems](#).

A. Add the H.323 Firmware

Add the J169/J179 H.323 firmware file (for example **FW_H_J169_J179_R6_7_0_0H.bin**) to the IP Office system or its file server. The file can be obtained from within the IP Office 10.1 SP3 software download.

B. Modify the 96x1Hupgrade.txt File

1. Using a browser, obtain a copy of the system's current 96x1Hupgrade.txt file.
2. Add the following to the start of the file.

```
IF $MODEL4 SEQ J169 GOTO J100PHONES
IF $MODEL4 SEQ J179 GOTO J100PHONES
GOTO 96X1PHONES
# J100PHONES
GET J100Hsettings.txt
GOTO END
# 96X1PHONES
```

3. Load the file back onto the system.

C. Create and Load a J100Hsettings.txt File

1. Open the system's current 46xxsettings.txt file and locate the section containing 9611 telephone settings. This file is needed for reference for the following changes.
2. Using a text file editor, create a new text file called J100Hsettings.txt.
3. Add the following text.

```
## J169 / J179 H323 Phones
IF $MODEL4 SEQ J169 GOTO J100FW
IF $MODEL4 SEQ J179 GOTO J100FW
GOTO END
# J100FW
## Specify FW Version
SET APPNAME FW_H_J169_J179_R6_7_0_0H.bin
## Copy 9611 Settings from 46xxsettings.txt file here
SET TRUSTCERTS "Root-CA-0206233E.pem"
SET TLSSRVVERIFYID 1
SET NVTLSRV 192.168.42.6
SET BRURI "https://192.168.42.6:411/user/backuprestore/"
SET HTTPPORT "8411"
SET SCREENSAVERON 240
SET SCREENSAVER 96xxscr.jpg
SET LANG1FILE "mlf_96x1_v148_spanish.txt"
SET LANG2FILE "mlf_96x1_v148_french_paris.txt"
SET LANG3FILE "mlf_96x1_v148_dutch.txt"
SET LANG4FILE "mlf_96x1_v148_german.txt"
SET UNNAMEDSTAT 0
# END
```

4. Edit the setting values to match the system's existing values from its 46xxsettings.txt file.

-
5. Edit the **SET APPNAME** value to match the supplied J100 H323 firmware file.
 6. Save the file as J100Hsettings.txt and upload the file to the system.

D. IP Office Configuration

Create IP Office user and H.323 extension entries as normal for H.323 IP telephone installation.

E. Setting the J169/J179 Phone to H.323 Mode

The J169/J179 phones ship from the factory running SIP firmware.

1. Power up the phone and as soon as possible access the admin menus.
2. Select **Signaling**.
3. Change the signaling from **Default** to **H.323**.
4. Click **Save**.
5. Click **Back**. The phone will restart using the new mode.

7.2.6.2 IP Office 10.1 SP3 Systems

IP Office 10.1 SP3 and higher service packs already include changes to support J169/J179 phones in H323 mode. If using auto-generated settings, no changes are required. If using static files, use the auto-generated J100Hsettings.txt and 96x1Hupgrade.txt files as templates for changes required.

A. IP Office Configuration

Create IP Office user and H323 extension entries as normal for H323 IP telephone installation.

B. Setting the J169/J179 Phone to H323 Mode

The J169/J179 phones ship from the factory running SIP firmware.

1. Power up the phone and as soon as possible access the admin menus.
2. Select **Signaling**.
3. Change the signaling from **Default** to **H.323**.
4. Click **Save**.
5. Click **Back**. The phone will restart using the new mode.

7.2.6.3 Upgrading Systems with H.323 J169/J179 Phones

Upgrading from Pre-IP Office 10.1 SP3 to IP Office 10.1 SP3

Delete the manually created J100Hsettings.txt file. The system will auto-generate a suitable temporary file when requested by a phone. If a static file is required, use the auto-generated file as a template.

Upgrading from IP Office 10.1 SP3 to IP Office R11.0 or Higher

1. Depending on the type of 96x1Hupgrade.txt file:
 - a. **If using the auto-generated file:**
Add the source number **FORCE_J100_H323_TO_SIP** to the NoUser user in the system configuration.
 - b. **If using a static file:**
Added the following lines to the start of the 96x1Hupgrade.txt file being used.

```
IF $MODEL4 SEQ J169 GOTO J100PHONES
IF $MODEL4 SEQ J179 GOTO J100PHONES
GOTO 96X1PHONES
# J100PHONES
GET J100Supgrade.txt
GOTO END
# 96X1PHONES
```

2. In the IP Office configuration, replace the J169/J179 phone H.323 Extension records with SIP extension records.
3. Saving the configuration changes with an immediate reboot. The J169/J179 phones will restart and switch to using SIP firmware.

Chapter 8.

Vantage K100 Series Installation Notes

8. Vantage K100 Series Installation Notes

The Avaya Vantage devices are Android desk phones that are supported with IP Office Release 11.0 and higher. This section provides notes on their IP Office installation and operation. These notes should be used in conjunction with the information provided in the full Avaya Vantage documentation available from Avaya.

An operation Vantage phone consists of several elements, the desk phone, optional handset modules and a dialer applications:

- **Desk Phones:**

The following K100 Series phones are currently supported with IP Office.

- **K165 Audio Desk Phone**

This is an android desk phone designed for audio calls. The phone supports handsfree audio calls and connections a wide range of headset types.

- **K175 Audio Video Desk Phone**

This model is similar to the K165 but also includes an integrated camera and so can be used for both audio-only and video calls.

- **Handset Modules:**

- **J1B1 Wired Handset Module**

This optional module provides the Vantage phone with a standard telephone handset.

- **J2B1 Wireless Handset Module**

This optional module provides the Vantage phone with a wireless Bluetooth handset. The handset is charged directly from its phone cradle using contactless charging.

- **Dialer Applications:**

- **Vantage Basic**

This application provides a simple telephone to make and receive calls. It supports IP Office contacts and a local call log. This application is supported with IP Office R11.0.

- **Avaya Equinox**

This is a Vantage specific version of the Avaya Equinox client for Android devices. Currently not supported for IP Office R11.0.

- **Power Options**

- **K100 Power Adapter**

The Vantage phones can be powered through Power over Ethernet (PoE). However, if necessary it can be powered using this mains power adapter. See [Power Options](#) ⁸⁷.

IP Office Requirements

In order to deploy Vantage phones with IP Office, the following requirements apply:

- IP Office Server Edition, IP Office Select or IP500 V2 system running IP Office Release 11.0.
- A separate HTTP file server to host the Vantage firmware.
- For Vantage Basic Use: Each phone will use an **IP Endpoint** license.

8.1 Phone Files

The Vantage phone is configured, either manually or via DHCP option 242, with the address of a file server. That address is used by the phone to request a variety of files. The phone requests files whenever it is restarted. By default, it also [polls the file server](#)^[18] hourly to check for updated files.

When requesting files, the phone uses the following files/types of file in the approximate order listed. Those files marked * can be [auto-generated](#)^[14] by the IP Office system if it is the file server.

- **Upgrade File:** *K1xxSupgrade.txt*

This file specifies the name and version of the main firmware file. The phone will load the file if it differs from the phone's existing firmware version. The upgrade file then specifies the phone to request the settings file.

- **Settings File:** *46xxsettings.txt*

This file specifies settings for Avaya IP (H323 and SIP) phones supported by IP Office. For the Vantage phone it specifies the supported dialer application mode and a range of other settings.

- **Firmware Files:** *.tar/.sig/.sig256*

This set of files are used to upgrade the Android operating system on the phone. The name and version of the main firmware file is specified by the *K1xxSupgrade.txt* file. That first file then specifies any other firmware files that the phone should install as part of the firmware upgrade.

- These files cannot be hosted by the IP Office system. Using its **HTTP Server IP Address** setting, the IP Office system always redirects requests for these files to the file server specified. This is regardless of the system's **HTTP Redirection** setting.

- **! Important**

A firmware upgrade can take up to 2 hours. During that time the phone should not be switched off.

- For new installations, it may be practical to configure a temporary HTTP file server that can be used to upgrade new Vantage phones before taking them to the customer site or end user desk.

- **Application Files:** *.apk*

Through the settings files you specify the dialer mode supported by the phone and the name of the dialer application file that it should install.

- If the name differs from the existing application file it is using, it will install the new version.
- Like the firmware files above, requests to the IP Office for these files are automatically redirected to the **HTTP Server IP Address** setting.
- If the specified file is not available when requested, the phone will not continue to use its existing copy. This means that the file server providing the .apk files to the phones must be permanently available.

- **Additional Settings File:** *46xxspecials.txt*

If using the auto-generated files, they may not include all the settings you require. This additional file can be used to provide the additional settings. See [Additional Phone Settings](#)^[18] and [Other Settings](#)^[88].

8.2 File Server Options

Vantage phone installation with IP Office requires a permanent HTTP file server. The decision affects where the different [phone files](#)^[79] are located and whether auto-generated files can be used or not.

File Server Method	Files on the IP Office	Separate HTTP/HTTPS File Server	IP Office Settings
Dual File Servers	K1xxUpgrade.txt 46xxsettings.txt	.tar/.sig files .apk files	<ul style="list-style-type: none">• HTTP Server IP Address: The separate HTTP server's IP address.
Single File Server	-	.tar/.sig files .apk files K1xxUpgrade.txt 46xxsettings.txt	<ul style="list-style-type: none">• HTTP Server IP Address: The separate HTTP server's IP address.• Phone File Server Type: Set to Custom.

- **Dual File Servers (IP Office and 3rd-Party HTTP File Server)**

In this mode, the phone settings files are hosted by the IP Office system whilst the firmware and application files are hosted by the separate HTTP file server. The address of the IP Office system is used as the **File Server** set in the phone's own menus (either by DHCP or manual entry). This mode allows the option of using the auto-generated *46xxsettings.txt* file.

- **Single File Server (3rd-Party HTTP File Server Only)**

In this mode, all files for Vantage installation are hosted by the separate HTTP file server. The address of the file server is used as the **File Server** set in the phone's own menus (either by DHCP or manual entry).

- **! WARNING: The 3rd-Party HTTP File Server Must Be Permanently Available**

In both scenarios, the 3rd-party HTTP file server must be permanently available. That is, it must be available during any subsequent reboots of the Vantage telephones. If the phone is not able to validate the dialer application during following a reboot it will not allow the continued use of the application even if already installed.

- **! IMPORTANT: Adding Additional MIME Content Types**

The Vantage phones request file types which by default are not recognized or handle correctly by some 3rd-party file servers. You must ensure that the file types above (.apk, .sig, .sig256) are listed in the MIME, media or content type settings of the file server. See [Adding Additional MIME File Types](#)^[44].

8.3 The Administrator Password

The Vantage phones require an administrator's password to be entered in order to access certain menus, for example factory defaulting the phone. This password is set using the **SET ADMIN_PASSWORD** and/or **SET PROCPSWD** commands in the settings file.

- If the ADMIN_PASSWORD is configured, the Vantage phone uses that password and ignores any PROCPSWD value.
- If the ADMIN_PASSWORD is not configured and PROCPSWD has a non-default value, the Vantage phone uses the PROCPSWD value.
- If the ADMIN_PASSWORD is not configured and PROCPSWD uses the default value (27238), you cannot access administrator settings on the Vantage phone.

8.4 Emergency Call Restrictions

There are restrictions on the calls that can be made in some scenarios. The customer and their users must be made aware of these restrictions:

- **If the phone is logged out**

If the phone is logged out, it cannot be used to make any calls including emergency calls.

- **If the phone is locked**

If the phone is locked, then by default it cannot be used to make any calls including emergency calls.

- By default, the IP Office auto-generated settings file disables the screen lock function using the **ENABLE_PHONE_LOCK** command. However, this cannot be guaranteed if using non auto-generated files. Also it cannot be guaranteed if users are able to access the phone settings to manually enable the screen lock functions.
- If the **PHNEMERGNUM** and/or **PHNMOREEMRGNMS** commands are added to the settings files, the phone is able to make calls to the numbers specified with those commands when logged out. See [Other Settings](#) ⁸⁸.

8.5 Power Options

The Vantage phones can be powered through a number of methods.

- **Power over Ethernet (PoE)**

The power class depends on the following:

- **802.3af:** The Vantage phone will act as a Class 3 device. The phone's USB socket supports 100mA output.
- **802.3at:** The Vantage phone will act as a Class 4 device. The phone's USB socket supports 500mA output.

- **Mains Power**

If PoE is not available, mains power can be used. This may also be used if connecting the phones to the network using Wi-Fi.

- An optional 48V dc. adapter is available to power the phone from a mains power outlet. The adapter requires a suitable local main supply cable.

8.6 Installation

8.6.1 Installation Summary

This section provides a summary of the installation process for Vantage phones with IP Office.

Installation Summary:

	Process	See...
1.	Before going to the customer site, pre-upgrade the phone firmware if possible (see Pre-Upgrading the Phone Firmware ^[83]). This avoids performing the 2 hour phone upgrade process on site or at the end-user's desk.	See the additional process outline below.
2.	Configure the IP Office system for SIP extension support as per the generic installation process.	Generic Installation Process ^[24]
3.	Create user and extension entries in the IP Office configuration: <ul style="list-style-type: none">• For Vantage Basic users: Create a user record and SIP extension record for the user.	SIP User Settings ^[31] SIP Extension Settings ^[32]
4.	Download and unpack the Vantage firmware set.	Downloading the Vantage Software ^[83]
5.	Check and configure the settings files.	Configuring the Settings Files ^[85]
6.	Upload the unpacked firmware set to the separate 3rd-party HTTP file server.	–
7.	Set the IP Office system's HTTP Server IP Address to the address of the separate server.	System File Server Settings ^[39]
8.	Proceed with initial phone startup.	Initial Phone Startup ^[88]

8.6.1.1 Pre-Upgrading the Phone Firmware

This process can be used prior to site installation to pre-upgrade a set of phones. It doesn't set or install the dialer application and doesn't require a user login.

	Process	See...
1.	Download and unpack the Vantage firmware onto an HTTP file server. This must be the same version of firmware that will also be used at the customer site.	Downloading the Vantage Software 83
2.	Edit the <i>K1xxSupgrade.txt</i> file to either remove the GET 46xxsetting.txt line or comment it out with ## .	–
3.	If you are able, configure a DHCP server to provide the file server address, that removes the following steps.	–
4.	Unbox each Vantage phone and using a PoE connection, connect the phone to the same network as the HTTP file server.	–
5.	Once the phone has stated with its pre-installed factory firmware (approximately 20-minutes), change the file server address to be the HTTP file server.	Changing the File Server Address 94
6.	After downloading the <i>k1xxSupgrade.txt</i> file from the file server, the phone will eventually begin upgrading its firmware.	–
7.	When completed, check the phone's software version.	Checking the Firmware Version 96
8.	Power off and re-box the phone.	–

8.6.2 Downloading the Vantage Software

The Vantage software (firmware and application files) is not included as part of the IP Office administration software and are not automatically installed on the IP Office system. Vantage software can be downloaded from the Avaya support website (<http://support.avaya.com>).

- Ensure that the version of Vantage software that you download is listed as supported by the release of IP Office with which you intend to use it.
- In some cases, the application *.apk* files can be downloaded separately. You must ensure that any separately downloaded application file is listed as compatible with both the Vantage firmware version and the IP Office release.

Loading the Vantage Files onto a File Server

8.6.2.1 Loading Vantage Files onto the File Server

The method of copying the Vantage files onto the 3rd-party file server will depend on that server. Refer to the appropriate documentation for the file server being used.

There are some additional considerations regarding the file server for Vantage phones:

- **File Location**

If using the IP Office systems auto-generated K1xxSupgrade.txt file, the Vantage files need to be located in the root directory of the file server. For example on an IIS server, in the wwwroot folder. It is possible to use a sub-folder, however that requires you to switch to [using a static K1xxSupgrade.txt file](#)^[85]. That then allows you to add the necessary sub-folder path to the file names that the phone's will be instructed to request.

- **MIME Types**

The file extensions used by the Vantage files are not supported as standard by some file servers. If that is the case, you need to [add additional MIME types](#)^[44] to the file server configuration.

8.6.2.2 Adding Additional MIME File Types

Most HTTP/HTTPS file servers are already configured by default to serve common file types such as .txt, .zip and .tar files. However, there may be additional configuration required in order for the server to correctly respond to requests for newer file types such as .apk, .sig and .sig256 files.

The method used on most file servers is to add additional MIME types to the server's configuration (also called media or content types). The MIME type tells both the file server and the requesting device how to handle the particular file. In most cases, MIME types are configured based on file extensions. The exact method depends on the 3rd-party file server being used.

Example MIME Types:

File Extension	MIME Type
.apk	application/vnd.android.package-archive or application/octet-stream
.sig	file/download
.sig256	file/download

- The required setting for .apk files can vary depending on the version of Android requesting the file, so testing using either option is necessary.

To add a MIME type to an IIS Server:

1. Open the **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, go to the site, application or directory for which you want to add a MIME type.
3. In the **Home** pane, double-click **MIME Types**.
4. In the **Actions** pane, click **Add...**
5. In the **Add MIME Type** menu, add the file name extension and MIME type required and then click **OK**.

To add a MIME type to an IIS Sever configuration file:

1. Locate the server's configuration file. For example C:\Windows\System32\inetsrv\config\applicationHost.config.
2. Add the additional MIME types required to the <staticContent> section. For example:

```
<staticContent>
  <mimeMap fileExtension=".apk" mimeType="application/vnd.android.package-archive" />
  <mimeMap fileExtension=".sig" mimeType="file/download" />
  <mimeMap fileExtension=".sig256" mimeType="file/download" />
</staticContent>
```

To add a MIME type to an Apache server:

MIME types can be added to the servers **httpd.conf** file. However, this requires the server to then be restarted for any changes to take effect. Alternatively, the new MIME types can be added to a **.htaccess** file placed in the same directory as the files. In either case, the MIME entries take the format:

```
AddType application/vnd.android.package-archive
AddType file/download .sig .sig256
```

8.6.3 Configuring the Settings Files

For Vantage phones, one of the settings files that the phone requests needs to specify which dialer application the phone should support and also the specific file name (and if necessary path) for the installation file for that dialer application. This is done using the following settings:

- **SET ACTIVE_CSDK_BASED_PHONE_APP**

The value defines the dialer application supported by the phone. The supported values is:

- **com.avaya.android.vantage.basic** - Used for Vantage Basic.

- **SET PUSH_APPLICATION**

This value sets the name of the .apk application file that the phone should load.

- If the specified file is not available when requested, the phone will not continue to use its existing copy. This means that the file server providing the .apk files to the phones must be permanently available.

Using the Auto-Generated K1xxSupgrade.txt File

The IP Office system can auto-generate a K1xxSupgrade.txt file. The contents of the auto-generated file will match the firmware and dialer application supported by the release of IP Office. To view the file, browser to <http://<IPOffice>/K1xxSupgrade.txt>. The file is displayed, for example:

```
## IPOFFICE/11.0.0.0 build 822 192.168.0.180 AUTOGENERATED
SET APPNAME K1xx_SIP-R1_1_0_1_3105.tar
GET 46xxsettings.txt
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"
SET PUSH_APPLICATION Com.avaya.android.vantage.basic_playstore_1.1.0.1.0001_200318_e82ab3e.apk
```

If the auto-generated K1xxSupgrade.txt file requires modification:

- **If the dialer version needs to be changed:**

This can be done using a NoUser source number to change the dialer application specified in the auto-generated K1xxSupgrade.txt file. Add **SET_VANTAGE_APK_VER=nnnn** where **nnnn** is the version suffix that should be added to **com.avaya.android.basic_playstore_nnnn.apk**.

- For example, use **SET_VANTAGE_APK_VER=1.1.0.1.0000_060318_99535a2** to change the auto-generated output to **SET PUSH_APPLICATION com.avaya.android.vantage.basic_playstore_1.1.0.1.0000_060318_99535a2.apk**.

- **If the firmware version needs to be changed:**

This can be done using a NoUser source number to change the firmware specified in the auto-generated K1xxSupgrade.txt file. Add **SET_VANTAGE_FW_VER=nnnn** where **nnnn** is the version suffix that should be added to the **K1xx_SIP-Rnnnn.tar** file name.

- For example, use **SET_VANTAGE_FW_VER=1_1_0_1_3119**. to change the auto-generated output to **SET APPNAME K1xx_SIP-R1_1_0_1_3119.tar**.

Using a Static K1xxSupgrade.txt File

If necessary a static K1xxSupgrade.txt file can be used. For example, when the Vantage files are located in a sub-folder on the file server rather than the file server's root folder.

To create a static file, the auto-generated file shown in the browser can be saved to the PC and used as a template for editing. The edited file is then [uploaded](#)^[4] back to the IP Office system. The static file is provided to phones rather than the auto-generated file.

For example, the following is a set of static K1xxSupgrade.txt for a scenario where the Vantage files have been placed in a */vantage* sub-folder on the file server. The file requests in this case are still redirected via the IP Office using its **HTTP Server IP Address** setting.

```
## Static K1xxSupgrade File
SET APPNAME vantage/K1xx_SIP-R1_1_0_1_3105.tar
GET 46xxsettings.txt
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"
SET PUSH_APPLICATION vantage/com.avaya.android.vantage.basic_playstore_1.1.0.1.0001_200318_e82ab3e.apk
```

Adding Additional Settings

Whilst configuring these settings, you should consider any [other settings](#)^[8] required, especially whether or not to set [emergency call](#)^[8] numbers. Additional settings can be added in several ways:

- Add them to a static 46xxspecials.txt file if using auto-generated K1xxSupgrade.txt and 46xxsettings.txt files. See [46xxspecials.txt](#)^[17].
- Add them to the 46xxsettings.txt file if a static file is being used. Note however that those may be overwritten by any similar setting in a 46xxspecials.txt file.
- Add them to the K1xxSupgrade.txt file if a static file is being used. This has the advantage of keeping Vantage specific settings in a Vantage specific. However it risks those settings be overwritten by any similar setting in the 46xxsettings.txt or 46xxspecials.txt files.

8.6.3.1 Other Settings

This section covers a small sample of the additional settings you may consider for Vantage installations. The *"Installing and Administering Avaya Vantage"* manual details the full range of *46xxsettings.txt* file settings supported and not supported by Vantage phones.

Studying the contents of the auto-generated *46xxsettings.txt* file shows the commands required for IP Office operation, including those that are automatically adjusted to match the IP Office system's configuration settings.

Additional settings can be added in several ways:

- Add them to a static *46xxspecials.txt* file if using auto-generated *K1xxSupgrade.txt* and *46xxsettings.txt* files. See [46xxspecials.txt](#)^[17].
- Add them to the *46xxsettings.txt* file if a static file is being used. Note however that those may be overwritten by any similar setting in a *46xxspecials.txt* file.
- Add them to the *K1xxSupgrade.txt* file if a static file is being used. This has the advantage of keeping Vantage specific settings in a Vantage specific. However it risks those settings be overwritten by any similar setting in the *46xxsettings.txt* or *46xxspecials.txt* files.

Commands are entered in the format **SET <NAME> <VALUE>**. For simple on/off commands, the values 0 (off) and 1 (on) are used. The default is the value used by Vantage phones is no setting is specified.

- **GROUP**
Set the group value used by the phone. The default is 0.
- **BRANDING_VOLUME**
Sets the volume level of the Avaya connection sound. The range is 1 (low) to 8 (loud). The default is 5.
- **CLICKS**
Sets whether the audio clicks function is on or off. The default is on (1).
- **USER_INSTALL_APPS_GOOGLE_PLAY_STORE**
Sets whether the user can install applications from the Google Play Store. The default is off (0).
- **PIN_APP**
Sets the name of the application locked on the screen. When an application is pinned, the user cannot switch to another application or the home or settings screens. See [Application Pinning](#)^[97]. To select the Avaya dialing application, use the same name as set for the **ACTIVE_CSDK_BASED_PHONE_APP** command.
- **UPGRADE_POLLING_PERIOD**
Sets the frequency in minutes, that the phone polls its file server. The range is 0 (off) to 10080 (weekly). Additional settings can also be used to control when the phone downloads new files and when it installs those files. The default is hourly (60).
- **BRANDING_FILE**
Specifies the URL of the branding image. When set, the image replace the Avaya log shown top-left of the dialer application screen. The image must be 142x56 pixels and in PNG, JPEG, GIF or BMP format. If using the IP Office as the file server this needs to be the full URL to the files location as this request is not redirected by the IP Office unless the file is uploaded to the IP Office.
- **ADMIN_PASSWORD**
Set the phone administrator password. If set, this overrides any password specified by the **PROCPSWD** command.
- **PHNEMERGNUM**
Set an emergency call number. Enter a number of up to 30 telephone dialing digits. If set, the phone's lock screen includes an **Emergency call** button. This number is the number auto-dialled from the emergency call screen. You must ensure that the number specified is correctly routed as an emergency number (using **Dial Emergency** short codes) by the IP Office system.
- **PHNMOREEMERGNUMS**
Sets a set of emergency call numbers. Multiple numbers, separated by , commas can be entered. These numbers can then be manually dialed from the emergency calls screen. If **PHNEMERGNUM** has not been specified, then the first number in the list is also used for that function. Dialing of numbers not in this list is blocked. You must ensure that the numbers specified are correctly routed as emergency numbers (using **Dial Emergency** short codes) by the IP Office system.
- **TIMEZONE**
Sets the phone's timezone for time and date operation. The value should be in [Olson name format](#), for example **SET TIMEZONE Europe/London, America/Chicago** or **Europe/Zurich**. If not specified, the phone defaults to GMT timezone (with no Daylight Saving). The default is GMT. When set, the user can still manually change the timezone (*Settings | Date & time | Select time zone*) using the phone menus. The setting specified by the settings file appears in the user menu under the name **Default**.
- **WIFISTAT**
Sets whether the phone user can configure WiFi settings or not. The default is on (1).

Example File

The following is an example of a 46xxspecials.txt file with a range of additional settings for the supported Vantage phones.

```
## Vantage settings
IF $MODEL4 SEQ K165 GOTO VANTAGE_COMMON
IF $MODEL4 SEQ K175 GOTO VANTAGE_COMMON
GOTO END_VANTAGE


# VANTAGE_COMMON
SET TIMEZONE Europe/London
SET CLICKS 0
SET PHNEMERGNUM 999
SET PHNMOREEMRGNUMS 911,112,9999, 9911, 99112
SET WIFISTAT 0
SET USER_INSTALL_APPS_GOOGLE_PLAY_STORE 0
SET BRANDING_FILE http://192.168.0.50/logo.png

# END_VANTAGE
```

8.6.4 Initial Phone Startup

The initial startup of a new or factory defaulted Vantage telephone varies depending on whether it receives a file server address via initial DHCP or not and whether the file server provides the required files.

Initial Startup:

1. After applying power to a new or defaulted phone, it will go through a startup process. This takes approximately between 4 to 20 minutes.
2. When completed, the phone displays the "Avaya Vantage" logo and time/date.
3. Wait a couple of minutes. This is important as the phone may still have further downloads to complete.
4. If the  icon appears in the status bar, the phone is downloading additional files. This may include downloading the configured phone dialer application and/or downloading updated firmware.



- **Dialer Application**

If a new dialer application is downloaded, the phone displays a message prompting you whether to install the application now or later.

1. Allow the application to be installed now. After installing it the phone will reboot.
2. After the reboot completes, again wait a couple of minutes and then check that there are no further downloads in progress. If there are further downloads in progress, it indicates that the phone is downloading updated firmware.

- **System Update**

An update of the phone's firmware can take up to 2 hours. Do not power off the phone during this process.

5. Once all application and firmware updates have been completed, you can continue with the initial phone startup. The screen background varies depending on whether the phone was able to obtain its configuration files
 - **[Red Background](#)** 
The phone has not obtained the settings file.
 - **[Blurred Office Workers Background](#)** 
The phone has obtained the settings file and installed the dialer application.

8.6.5 Blurred Office Workers Background

This section covers the initial configuration of a Vantage phone started in a scenario where it has automatically received a file server address and downloaded the required settings and application files from that file server address. This may occur happen in a number of ways:

- The network DHCP server has provided the file server address through Option 242. For example if the IP Office is the DHCP server.

To configure the phone:

1. No further manual configuration is required. Go to [logging in](#) .

8.6.6 Red Background

This section covers the initial configuration of a new Vantage phone started in a scenario where it has not received a file server address. This may occur for a number of reasons:

- The network DHCP server is not configured to support Option 242 to provide file server address.
- The file server address obtained by DHCP was not that of the server hosting the required files for the phone.
- The required files were not present on the file server.
- The phone is being powered from a 48V dc power supply unit without a network cable with the intention of connecting it to the network wirelessly.

For installed phones, the red background with a request for PIN code may also appear post installation, see [Red Screen/Enter PIN Code](#)^[98].

To configure the phone:

1. Swipe up on the screen. The Android setup menu **Welcome** screen is displayed.
2. If required, click on **English (United States)** and click on the language and country required.
3. Click on the arrow icon.
4. The phone searches for available wireless networks.
 - **If you don't want to connect via Wi-Fi:** Click on **Skip >** and then **SKIP ANYWAY**.
 - **If you want to use the device via Wi-Fi:**
 - a. Click on the wireless network that the phone should use.
 - b. Enter the network password and click **CONNECT**.
5. Enter the user's name and click **NEXT >**.
6. Enter details of the user's email account. This can be done later through the settings menus. Otherwise click **Not now**.
7. Scroll through the Google services, changing any settings if required and then click **NEXT >**.
8. The phone should now display the Android home screen. This is still a standard Android device with no Avaya dialer application and SIP telephone settings.
9. Access the phone's settings menu:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the ⚙ icon to display the quick settings menu.
 - d. Click on the ⚙ icon to display the settings menu.
10. Under **Wireless & Networks** select ... **More**.
11. If using group settings, click on **Group** and enter group number that the phone should use.
12. Click on **File Server**. The address to enter will depend on how you configured the [Vantage file server options](#)^[79]:
 - **Dual File Servers (IP Office and 3rd-Party File Server)**
If using *K1xxSupgrade.txt* and *46xxsettings.txt* files from the IP Office system, enter the system's address prefixed with **https://**. This method requires that system has a its **HTTP Server IP Address** set to the address of the 3rd-party HTTP file server that is hosting the other Vantage firmware files. Not prefixing the address with **https://** will cause the phone to not be able to obtain directory contacts (see [Error syncing IP Office Contacts](#)^[98]).
 - **Single File Server (3rd-Party File Server)**
If all the files for the Vantage phones are on the same server, enter the address of that server. This requires the *46xxsettings.txt* file on that server to be manually configured with setting that match the IP Office system's SIP configuration and set the IP Office as the SIP Proxy for the Vantage phones.
15. The phone may need to restart several times as it loads updated firmware files and then the Avaya dialer application.
16. When completed, the phone should restart with the blurred office workers background.
17. Continue by [logging in](#)^[90] and then, if necessary, [pairing the optional wireless handset](#)^[91].

8.6.7 Logging In


The method of logging in depends on the supported dialer application.

To login to the phone:

1. The method of logging in depends on the supported dialer application:
 - **Vantage Basic:**
 - a. Swipe the padlock icon up the screen.
 - b. Enter your extension number and user password.
 - c. The first time you login a software license screen is displayed. Click **ACCEPT**.
 - d. The Vantage Basic dial pad screen is displayed.





8.7 Bluetooth Handset Operation

The J2B1 wireless handset module provides the Vantage phone with a Bluetooth handset.




- The handset has integrated power, mute, volume up and volume down buttons.
- The nominal range is 10m in clear-air.
- The handset automatically powers off if out of range or unable to detect the Vantage phone for over 20 minutes.
- The handset charges using contactless charging when placed in its cradle.
- Full charging takes approximately 3 hours. When fully charged the handset has a talk time of 12 hours and a standby time of 60 hours.
- The handset cradle includes a magnetic hook switch that can be used to start, end and answer calls.
- The handset includes a [status lamp](#) .

8.7.1 Pairing the Bluetooth Handset

If the phone has been fitted with the wireless handset module, the Bluetooth handset needs to be paired with the Vantage phone.

- A  icon is shown in the status bar when the phone has Bluetooth enabled. This icon shows additional dots () when there are Bluetooth devices connected.
- A  icon is shown in the status bar when the phone detects it has a wireless handset module attached but no wireless handset connected.
- The icon above is replaced by a  icon when the wireless handset is connected. The icon also indicates the charge level of the handset.

To associate the Bluetooth handset:

1. Access the phone's settings menu:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the  icon to display the quick settings menu.
 - d. Click on the  icon to display the settings menu.
2. On the handset, press and hold the power button. Keep it pressed until the handset lamp flashes regularly. This indicates it is in pairing mode.
3. Select **Bluetooth**.
4. Change the setting to **On**. The phone scans for available Bluetooth devices.
5. When the handset is shown in the list of Bluetooth devices (**Avaya J100-02AE11** or similar), click on it and select **Connect**.
6. The  icon appears in the status bar, showing that the handset is connected and its charge level.

8.7.2 Handset Lamp

The handset includes a status lamp positioned between the power and mute buttons. During normal operation the lamp flashes twice every 5 seconds. However, the lamp is used for a range of other status indications as listed below.

Handset State	Lamp
Power on: Press the power button for 2.4 seconds.	4 flashes.
Power off: Press the power button for 3.2 seconds.	3 flashes.
Handset is in pairing mode: Press the power button for 10 seconds. The handset remains in pairing mode for 150 seconds.	Flash every 0.5 seconds.
Pairing successful:	10 rapid flashes.
Handset idle:	2 flashes every 5 seconds.
Handset in use (on a call):	3 flashes every 3 seconds.
Incoming call:	3 flashes every 7 seconds.
Handset muted:	Lamp on, flashes off 3 times every 4 seconds.
Handset try to reconnect to the phone:	Flash every 0.5 seconds.
Handset out of range of phone:	Flash every 5 seconds.

8.8 Additional Processes



This section includes additional configuration processes and options.

- [Switching to Wireless Connection](#) ⁹³
- [Rebooting a Phone](#) ⁹³
- [Changing the File Server Address](#) ⁹⁴
- [Changing the Phone's Group Setting](#) ⁹⁴
- [Clearing the User Data](#) ⁹⁵
- [Factory Defaulting a Phone](#) ⁹⁵
- [Checking the Firmware Version](#) ⁹⁶
- [Checking the Dialer Application Version](#) ⁹⁶
- [Starting an Immediate Upgrade](#) ⁹⁶
- [Application Pinning](#) ⁹⁷

8.8.1 Switching to Wireless Connection

The Vantage phone can be connected to the network using a wireless WiFi connection.




To switch to a wireless network connection:

1. Access the phone settings:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the  icon to display the quick settings menu.
 - d. Click on the  icon to display the settings menu.
2. Click **Network**.
3. Click **Network mode**.
4. Select **Wi-Fi**.
5. Click **Wi-Fi** once the option is no longer greyed out, this may take a couple of seconds.
6. Select the require wireless network.
7. Enter the network password and click **CONNECT**.

8.8.2 Rebooting a Vantage Phone

This method can be used to locally reboot a Vantage telephone without removing power.



To reboot a Vantage device:

1. Access the phone's settings menu:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the  icon to display the quick settings menu.
 - d. Click on the  icon to display the settings menu.
2. Select  **Backup & reset**.
3. Select **Reboot**.
4. Select **Yes**.
5. The phone will power off and then restart.

8.8.3 Changing the File Server Address

If necessary, the file server address can be changed manually.



To change the phone's file server address:

1. Access the phone settings:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the  icon to display the quick settings menu.
 - d. Click on the  icon to display the settings menu.
2. Under **Wireless & Networks** select ... **More**.
3. Click on **File Server** and enter file server address. This should be the server configured to provide *K1xxSupgrade.txt* and *46xxsettings.txt* files for the phone. In most scenarios that will be the IP Office.
4. Click **OK**.
5. Exit the settings. The new value is used the next time the phone polls for software or is [rebooted](#) ⁹³.

8.8.4 Changing the Phone's Group Setting

In some scenarios, the group ID value is used with the *46xxsettings.txt* files to control which files and settings are used by different phones. If the Vantage phone needs to use a group value use the following process to set the value.






To change the phone's group setting:

1. Access the phone settings:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the  icon to display the quick settings menu.
 - d. Click on the  icon to display the settings menu.
2. Under **Wireless & Networks** select ... **More**.
3. Click on **Group** and enter group number that the phone should use.
4. Click **OK**.
5. Exit the settings.
6. The new value is used the next time the phone polls for software or is [rebooted](#) ⁹³.

8.8.5 Clearing the User Data


This process removes all user data, user settings and any user installed applications.

To clear the existing user:

1. Access the phone's settings menu:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the  icon to display the quick settings menu.
 - d. Click on the  icon to display the settings menu.
2. Select  **Backup & reset**.
3. Select **Clear user data**.
 - If the option is not visible then you need to login as the administrator:
 - a. Click on the  icon shown top-right.
 - b. Click on **Admin login**.
 - c. Enter the [administrator password](#)  and click **OK**. The default password is *Avaya@1234*.
4. Select **Yes**.






8.8.6 Factory Defaulting the Phone

This process returns the phone similar state to an new out-of-the box device. It removes all user data and settings. It also removes any applications and certificates not loaded as part of phone firmware. However, it does not return the phone to its original firmware.

If you just want to clear the existing user data and applications select [Clear user data](#)  instead.

This process takes approximately 20 minutes to complete.

To factory reset a Vantage device:

1. Access the phone's settings menu:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the  icon to display the quick settings menu.
 - d. Click on the  icon to display the settings menu.
2. Select  **Backup & reset**.
3. Select **Factory data reset**.
 - If the option is not visible then you need to login as the administrator:
 - a. Click on the  icon shown top-right.
 - b. Click on **Admin login**.
 - c. Enter the [administrator password](#)  and click **OK**. The default password is *Avaya@1234*.
4. Select **RESET DEVICE**.
5. Select **ERASE EVERYTHING**.
6. The phone will power off and then restart.

8.8.7 Checking the Firmware Version

To check the firmware version:

1. Access the phone's settings menu:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the ⏮ icon to display the quick settings menu.
 - d. Click on the ⚙ icon to display the settings menu.
2. Scroll down to the **System** section.
3. Select **About Avaya Vantage**.
4. The information displayed includes the software version and build number.

8.8.8 Checking the Dialer Application Version

To check the dialer application version:

1. Within the application, click on the user name and extension number.
2. Select **Support** and then **About**.
3. Details of the dialer application version are displayed.

8.8.9 Starting an Immediate Upgrade

Through the *46xxsettings.txt* file, you can configure when the phone polls for updated files and when the phone will install new files. If required, you can check if the phone has detected updated firmware and, if so, trigger an immediate update.

- **! Important**

A firmware upgrade can take up to 2 hours. During that time the phone should not be switched off.

To check for and start a firmware upgrade:

1. Access the phone's settings menu:
 - a. If the status bar is currently not visible, swipe down from the top of the display to show it.
 - b. Swipe down to display the **Lock/Logout** menu.
 - c. Click on the ⏮ icon to display the quick settings menu.
 - d. Click on the ⚙ icon to display the settings menu.
2. Scroll down to the **System** section.
3. Select **About Avaya Vantage**.
4. Select **Software information**.
5. The information under **Update now** will show when the phone last checked for updated firmware.
6. If updated firmware is available, the **Update now** option can be clicked to start an immediate upgrade.

8.8.10 Application Pinning

You can pin the dialer application to the phone screen. When this is done, the user cannot access any other applications, the home screen or the settings menus.

You can turn application pinning on or off through the dialer applications own settings using the Vantage administrator password. The settings command **SET PIN_APP** can also be used to pin the application by default. See [Other Settings](#)^[86].

To manually switch pinning on or off:

1. Within the dialer application, click on the user name/number drop-down shown at the top-right of the screen.
2. Select **User Settings**.
3. Select **Application**.
4. The current pinning setting is shown by the **Application Pinning Mode**.
5. To change the setting, click on **Application Pinning Mode**.
6. Enter the administrator password. The default password is *Avaya@1234*.

8.9 Error Messages

8.9.1 The Configured Phone Application Was Not Found...

Likely causes of this error message are:

- A mismatch between the name of the `.apk` file specified in the `46xxsettings.txt` file and the `.apk` file on the file server. See [Setting the Dialer Application](#)^[85].
- The specified file is not on the file server.
- The file server is not reachable.
- An error, such as a loop in the settings file, has caused the phone to timeout.

8.9.2 Please note Vantage Basic is not functional ...

The error message *"Please note Vantage is not functional as it is not configured as the active phone application"* indicates whilst the phone has Vantage Basic installed, it has not been instructed to use Vantage Basic as its dialer application.

Check that the settings files loaded by the phone (`K1xxSupgrade.txt`, `46xxsettings.txt`, `46xxspecials.txt`) include the command `SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"`. See [Configuring the Settings Files](#)^[86].

Following any correction to the settings file [reboot the phone](#)^[93].

8.9.3 BT Handset is Not Paired

See [Pairing the Bluetooth Handset](#)^[91]. Likely causes of this error message are:

- A new or defaulted Vantage phone starts with Bluetooth support switched off.
- If the handset has not been able to detect its paired phone for over 20 minutes, it switches itself off.
- Bluetooth has been switched off.

8.9.4 Red Screen/Enter PIN Code

The red background with minimal controls may appear for a number of reasons.

- For new/defaulted Vantage phones see [Red Background](#)^[87].
- For existing Vantage phones that have been working, the most likely cause is an error in the current settings files making the installed dialer application invalid. Login using the user's IP Office password. Then refer to [Please note Vantage Basic is not functional ...](#)^[92].

8.9.5 Error syncing IP Office Contacts

By default, to obtain contacts from the IP Office the Vantage phone should use https. This is done by prefixing the IP Office address with **https://**. If the phone has been installed without using a `https://` prefix, either:

- Add **https://** to the IP Office address and restart the phone.
- Enable the **HTTP Directory Read** and **HTTP Directory Write** options in the IP Office security settings.

8.9.6 IP office contacts directory not available

See [Error syncing IP Office Contacts](#)^[98].

Chapter 9.

Avaya Equinox Installation Notes

9. Avaya Equinox Installation Notes

Avaya Equinox is a unified communication application that works on a wide range of operating systems; Windows, Android, macOS and iOS (see [Operating System Support](#)^[100]). It is supported with IP Office 11.0 and higher.

- Note that Avaya Equinox on Vantage phones is currently not supported with IP Office.

There are currently two installation models supported:

- **Basic Avaya Equinox Installation**

This model of installation has the Equinox clients initially registered directly to the IP Office system. This provides the client with support for telephony functions only. It does not support access to Instant Messaging, Presence and other Zang Spaces features.

- **Equinox with Zang Spaces Installation**

This model of installation has the Avaya Equinox clients initially registered to Zang Spaces which then links them to the IP Office system.

- Using the free Basic accounts this provides the Avaya Equinox clients with support for Instant Messaging and presences.
- Using the other paid-for levels of Zang accounts provides the Avaya Equinox clients with support other Zang Spaces features such as Meetings Online online.

9.1 Operating System Support

Avaya Equinox can be installed on the following operation systems:

OS	Supported Versions
iOS	iOS 10, iOS 11.
Android	4.4 (Kit Kat), 6.X (Marshmallow), 7.X (Nougat), 8.0 (Oreo).
Windows	Windows 7, Windows 8.1, Windows 10. <ul style="list-style-type: none">• Windows 7 support is only on Professional, Enterprise and Ultimate versions. Windows 8.1 and 10 support is only Pro and Enterprise.
macOS	10.11 (El Capitan), 10.12 (Sierra), 10.13 (High Sierra).

9.2 Standalone/Simultaneous Mode

Avaya Equinox can operate in either of the following modes. The mode used depends on the user licensing.

- **Standalone Mode**

In this mode, Avaya Equinox is the user's sole telephony device whilst they are logged into it. Logging into Avaya Equinox will log them off any other extension. Similarly logging on at another phone will log them out of Avaya Equinox.

- **Simultaneous Mode**

In this mode, the user can be logged in on both a physical desk phone and a softphone client such as Avaya Equinox at the same time. They can choose to make and answer calls on each extension

- Softphone clients includes Avaya Equinox clients, Communicator clients, one-X Mobile clients, IP Office Web Client and IPOCC Agent Web Client.
- Simultaneous client usage was previously only supported if the softphone client registered to IP Office on which the user was configured. For R11.0, the softphone client can be registered to any IP Office in the network.

9.3 User Licensing

Use of Avaya Equinox is subject to the following license requirements.

IP500 V2 User Support

On IP500 V2 systems, Avaya Equinox is supported for the following users:

User Profile	System Licenses	User Licenses	Mode	OS
Basic User	Essential Edition	Avaya Softphone License	Standalone	macOS, Windows
Mobile User	Essential Edition + Preferred Edition	Mobile Worker + Avaya Softphone License	Standalone	macOS, Windows
Teleworker User	Essential Edition + Preferred Edition	Teleworker	Simultaneous	macOS, Windows
Office Worker User	Essential Edition + Preferred Edition	Office Worker	Simultaneous	macOS, Windows
Power User	Essential Edition + Preferred Edition	Power User	Simultaneous	Android, iOS, macOS, Windows

IP Office Server Edition/IP Office Select User Support

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

User Profile	System Licenses	User Licenses	Mode	OS
Office Worker User	IP Office Server Edition or IP Office Select	Office Worker	Simultaneous	macOS, Windows
Power User	IP Office Server Edition or IP Office Select	Power User	Simultaneous	Android, iOS, macOS, Windows

9.4 Codec Support

The supported audio codecs depend on the type of Avaya Equinox client and the type of IP Office system.

Codec	iOS/Android	macOS/Windows	IP Office
Opus	Yes	Yes	No
G.722	Yes	Yes	Yes
G.711 A-law	Yes	Yes	Yes
G.711 U-Law	Yes	Yes	Yes
G.726	Yes	Yes	No
G.729A	Yes	Yes	Yes
G.729B	Yes	No	Yes ^[1]

1. Supported on IP500 V2 only.

9.5 IP Office Configuration

This section covers the general IP Office configuration to support Avaya Equinox clients. This part of installation is similar for installations using or not using Zang.

9.5.1 System SIP Configuration


The IP Office system needs to be configured for SIP extension operation as shown in the [Generic Installation Process](#) ^[24].

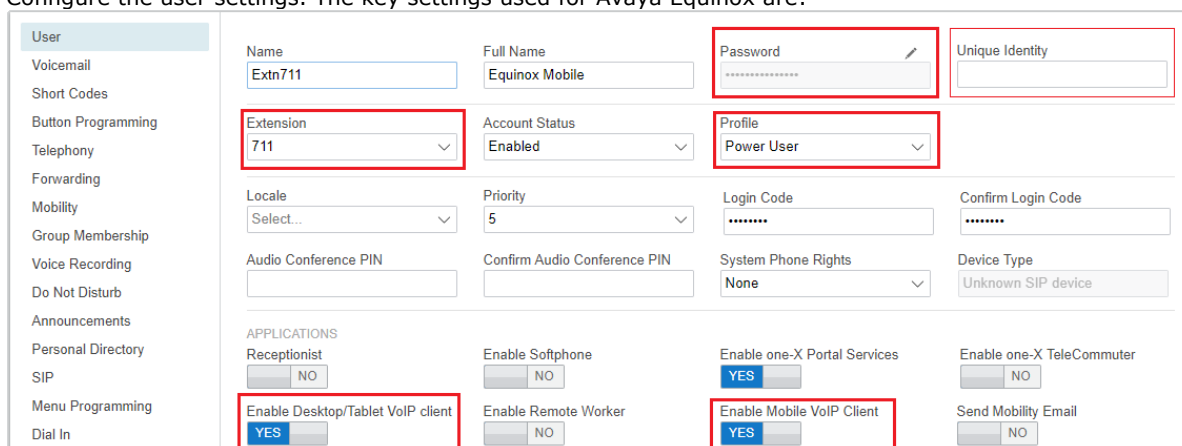
9.5.2 User Configuration

The following process creates a new Avaya Equinox user who will use Avaya Equinox in [standalone mode](#) ^[100]. 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 Equinox in [simultaneous mode](#) ^[100], alter the configuration settings of the existing user. No adjustments to their associated extension record are required.

To create an Avaya Equinox user:

- Using either IP Office Manager or IP Office Web Manager, load the system configuration.
 - If using IP Office Manager:**
 - To edit an existing user, select the existing user record.
 - To add a new user, select the system on which the user record should be created and then select **User**.
 - If using IP Office Web Manager:**
 - Select **Call Management | Users**.
 - To edit an existing user, click the  pencil icon next to the user.
 - To add a new user, click **+Add User** and select the system on which the user record should be created.
- Configure the user settings. The key settings used for Avaya Equinox are:



- Password**
Enter and confirm the user's password. This password is used for Avaya Equinox login.
 - Extension**
Enter an extension number for the user. This value is also used for the Avaya Equinox client login.
 - Unique Identity**
For Avaya Equinox users who will use Zang, enter their domain email address. This is the address that must also be entered for the user in the [Zang user configuration](#) ^[107].
 - Profile:**
Avaya Equinox is supported for any user profile other than **Non-licensed User**. The **Basic User** and **Mobile User** profiles require a Avaya Softphone License in addition to the necessary licenses for the user profiles.
 - Enable Mobile VoIP client**
Select this option to allow the user to use Avaya Equinox on Android and iOS devices.
 - Enable Desktop/Tablet VoIP client**
Select this option to allow the user to use Avaya Equinox on macOS and Windows devices.
- Depending on the license profile selected, the configuration tool may indicate that various other settings must be complete.

4. When creating a new user, after clicking **OK** or **Create**, you are prompted whether to also automatically create a new extension. If Avaya Equinox will be the user's only telephony device, select **None**. The user does not need an associated extension to use Avaya Equinox as a standalone client.

9.6 Zang Configuration

The following processes are used to configure a company (domain) within Zang. This process requires you to have configured a Zang account for the companies domain and to have access to the configuration of that domain's DNS server.

In summary:

1. [Complete the IP Office and IP Office user configuration](#) ^[102]
This is the same for installations using or not using Zang.
2. [Add a company and verify the company domain](#) ^[104]
3. [Add an app that details the connection address for the IP Office system](#) ^[106].
4. [Add the Avaya Equinox users](#) ^[107].

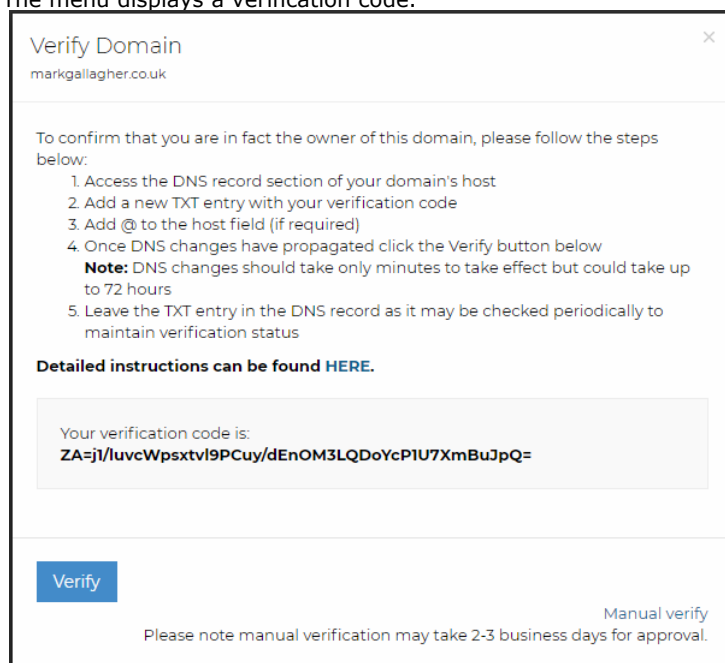
9.6.1 Verify the Company Domain

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

- Details of the customer domain. This must match the email address domain that the Avaya Equinox user's will use for their Avaya Equinox login.
- Access to the DNS server settings for the domain.

To verify the company domain address:

1. Login to Zang at <https://accounts.zang.io>.
2. If not already done so, click on your user name top-right and select **Add Company**.
3. Otherwise, click on **Manage Companies**. and click on the existing company name (or use **Add New Company** to add another company).
4. Select the **Domains** tab.
5. Select **Add Domain**.
6. Enter the domain address and click **OK**.
7. Click on the **Verify** button shown next to the domain name.
8. The menu displays a verification code.



Verify Domain ✕

markgallagher.co.uk

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

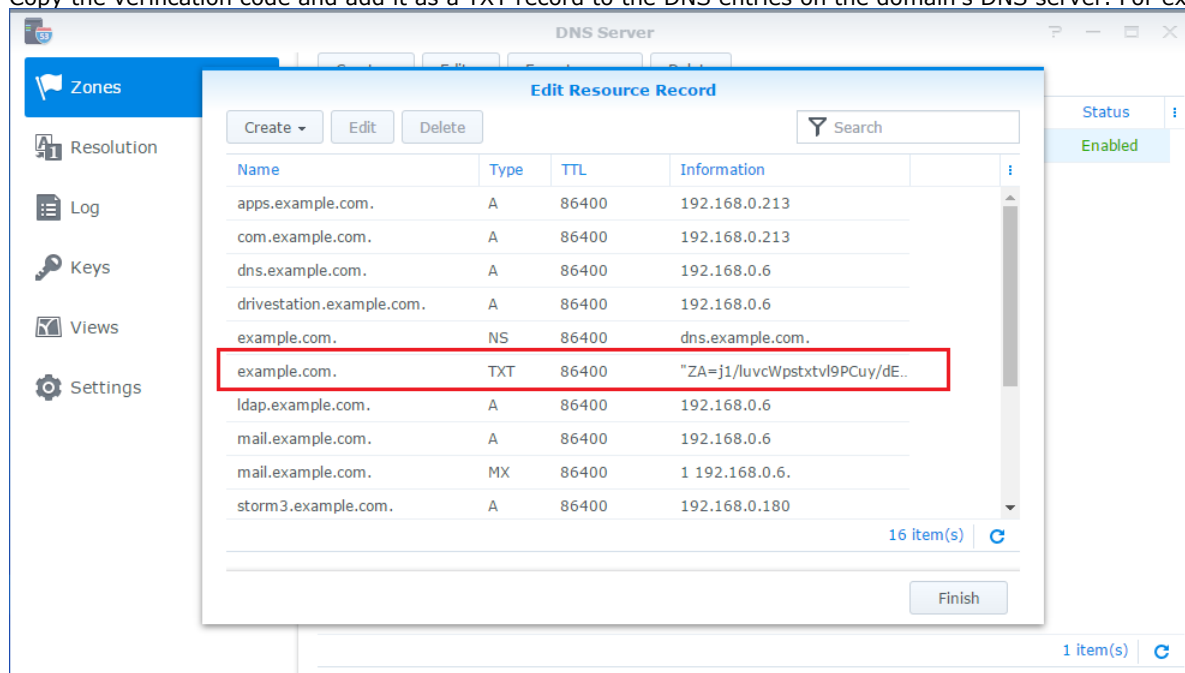
Detailed instructions can be found [HERE](#).

Your verification code is:
ZA=j1/lucWpsxtvl9PCuy/dEnOM3LQDoYcPIU7XmBuJpQ=

Verify Manual verify

Please note manual verification may take 2-3 business days for approval.

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



10. Click **Verify**.

9.6.2 Add IP Office Details

Once you have created a company within Zang, you need to configure details of the IP Office system to which the Avaya Equinox users should be connected when they login.

This process can be performed whilst waiting for the company domain to be verified.

To add the IP Office system details:

1. Login to Zang at <https://accounts.zang.io>.
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 IP Office system:

```
{
  "Client_Settings_File_Address": [
    {
      "Profile_Name": "Configuration for production users",
      "Client_Settings_File_Url": "http://ipoffice.example.com/46xxsettings.txt"
    }
  ]
}
```

The screenshot shows the Zang Cloud interface. On the left is a sidebar with 'Zang Cloud' and 'Manage Companies'. The main area has tabs for 'General', 'Domains', 'Manage Users', 'Licenses', 'Apps', and 'API Key'. The 'Apps' tab is selected, showing 'Equinox Cloud Client Application Settings'. A green message bar says 'App settings saved successfully'. Below this is a 'General' tab. The 'Product' is 'Equinox Cloud Client'. There are two main sections: 'Settings' and 'Public Settings'. The 'Settings' section has a description and an example JSON object. The 'Public Settings' section has a description and a JSON array of objects, each with 'Profile_Name' and 'Client_Settings_File_Url'.

Settings
This is an optional JSON setting object accessible only to authenticated users of this company.

EXAMPLE:

```
{ "theme-style": "dark", "example": "example value" }
```

Public Settings
This is an optional JSON setting object that does not require authentication to access.

EXAMPLE:

```
{ "theme-style": "dark", "example": "example value" }
```

The JSON array in the 'Public Settings' field is:

```
[
  {
    "Profile_Name": "Configuration for production users",
    "Client_Settings_File_Url": "http://example.com/46xxsettings.com"
  }
]
```

7. Click **Save**.

9.6.3 Add Avaya Equinox Users

For each user configured for Avaya Equinox operation on IP Office, their domain email address needs to be added to the company settings in Zang.

This process can only be performed once the domain has been verified.

To add the IP Office users:

1. Login to Zang at <https://accounts.zang.io>.
2. Click on **Manage Companies** and click on the existing company name.
3. Select the **Manage Users** tab.
4. Create an entry for each Avaya Equinox user configured on the IP Office system. Each entry must use an email address within the verified domain and which matches the user's **Unique Identity** in the IP Office configuration.

9.7 Client Installation

9.7.1 Windows Client

- **Communicator for Windows**

Installing Avaya Equinox on a PC which already has Communicator for Windows installed will automatically remove Communicator for Windows.

Prerequisites:

- **Windows 7:** Microsoft .NET Framework 3.5 or a later version.
- **Windows 8.1, Windows 10:** Microsoft .NET Framework 4.5.2 or a later version.
- **Exchange Server/Outlook Integration:**
 - Exchange Server 2010 SP1 and later.
 - Microsoft Outlook add-in for web mail is supported on Exchange Server 2013 and later.
 - Exchange Web Services must be enabled for the Avaya Equinox Outlook Add-in. Internet access must also be available because portions of the add-in are hosted on the Internet.

Downloading the Software:

The install package for the Windows Avaya Equinox client can be downloaded from the IP Office support pages on support.avaya.com.

Installing the Software (No DSCP):

This process covers simple single user installation without DSCP or IM support. For advanced installation options see [Advanced Installation](#)^[108].

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**.
11. Proceed to [initial configuration](#)^[112].

9.7.1.1 Advanced Installation

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

Command options can be combined, for example using "Avaya Equinox Setup.msi" /qn NOQOS=1 IMPROVIDER=1

- **Silent installation:** "Avaya Equinox Setup.msi" /qn
- **Automatic configuration enabled:** "Avaya Equinox Setup.msi" AUTOCONFIG=""
This option is not supported for Zang installations.
- **Silent uninstall:** msixexec /qn /x "Avaya Equinox Setup.msi"
- **Installer help:** Msiexec /?
- **Create install log:** msixexec /i <path_to_ACW_installer> /L*v <path_for_logs>
- **Create uninstall log:** msixexec /x <path_to_ACW_installer> /L*v <path_for_logs>
- **Enable IM Provider (disabled by default):** "Avaya Equinox Setup.msi" IMPROVIDER=1
- **Enable DSCP driver installation (disabled by default):** "Avaya Equinox Setup.msi" NOQOS=0
- **Disable Outlook plug-in install:** "Avaya Equinox Setup.msi" OP=0

- **Disable browser plug-in install:** "Avaya Equinox Setup.msi" BP=0

9.7.1.2 Installation Using a Group Policy

Use this procedure to deploy Avaya Equinox from a Windows server using Group Policy. This can be used to automatically install the Avaya Equinox client when a user login on the network.

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 Equinox 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 Equinox installer.
8. In the **Script Parameters** field, add the [command line parameters](#) ⁽¹⁰⁸⁾ required. For example, for a silent installation add the /qn parameter and click **Ok**.

9.7.2 macOS Client

Downloading the Software:

The install package for the macOS Avaya Equinox client can be downloaded from the IP Office support pages on support.avaya.com.

Installing the Software:

This process covers simple single user installation. For advanced installation options see [Advanced Installation](#) ¹¹⁰.

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**.
10. Proceed to [initial configuration](#) ¹¹².


9.7.2.1 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`

9.7.3 iOS Client



To install Avaya Equinox on an iOS device:

1. Open the App Store and search for Avaya Equinox.
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 Equinox to make emergency calls.
6. Proceed to [initial configuration](#) .

9.7.4 Android Client

The Avaya Equinox client can be installed from the Google Play Store.

To install Avaya Equinox on an Android device:

1. On the Android device, access the Google Play Store.
2. Search for *Avaya Equinox* by *Avaya Incorporated*.
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.
7. 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 Equinox will not work.
8. Allow the application to restart.
9. When the end user license agreement is displayed click **Accept**.
10. Proceed to [initial configuration](#) .

9.7.5 Initial Configuration

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

- [Login with Zang](#) ¹¹²
This login uses the users domain email address as configured in the Zang settings. Those settings then connect with the IP Office system.
- [Login without Zang](#) ¹¹³
This login uses the direct address of the settings file on the IP Office system and then the IP Office user's extension number and password.

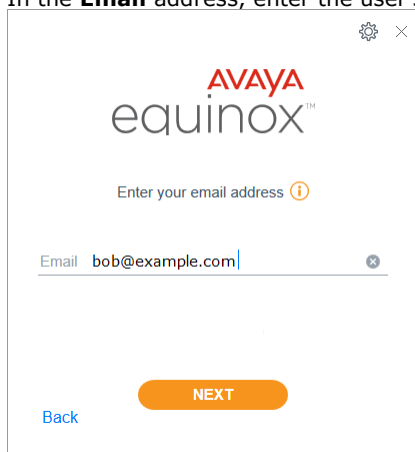
9.7.5.1 Zang Connection

Use this process for installations where Zang is being used. In this scenario, the Avaya Equinox users register with Zang using their domain email address. The Zang 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.

To configure the client:

1. Start the Avaya Equinox application.
2. In the **Email** address, enter the user's domain email address and click **NEXT**.



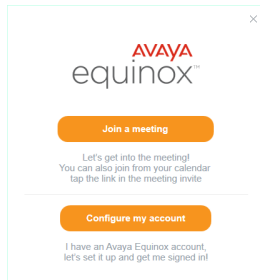
3. Follow the prompts as presented.

9.7.5.2 Direct IP Office Connection (Non-Zang)

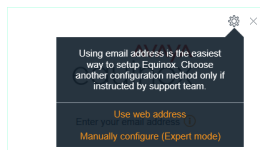
Use this process for installations where Zang is not being used. In this scenario, the Avaya Equinox users register direct with the IP Office system. If the Zang has been configured, see [Zang Connection](#) ^[112].


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.

To configure the client:



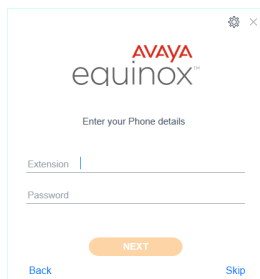
1. Start the Avaya Equinox application.
2. Select **Configure my account**.



3. Click on the  settings icon and select **Use web address**.



4. Enter the address of the IP Office system settings file in the form **http://<server>/acxsettings.txt**. The server address can be either the fully-qualified domain name or IP address.
5. Click **NEXT**.



6. Enter the user's extension number and their user password and click **SIGN IN**.
7. The application displays a set of tutorial screens.

9.7.6 Calendar Integration

Avaya Equinox can display meetings from the user's calendar on its Top of Mind and My Meetings pages. The meetings can be drawn from the following sources:

- **Local calendar**

For Avaya Equinox on Android and iOS devices, copy meetings from the local calendar of the device on which Avaya Equinox is running.

- **Exchange server**

Copy meetings from the user's account on an Exchange server.

9.7.6.1 Enabling Exchange Calendar Support

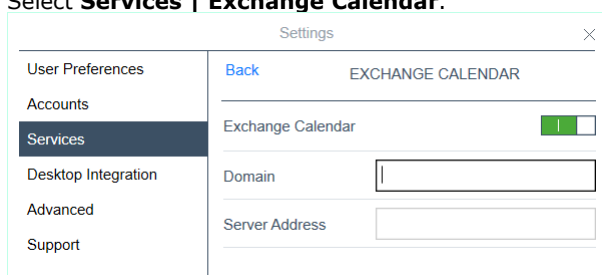
Before Exchange can be selected as a calendar source, details of the Exchange server and the user's email account on that server need to be entered in the Avaya Equinox settings.

- Exchange Server 2010 SP1 and later versions supported.

To setup Exchange server calendar integration:

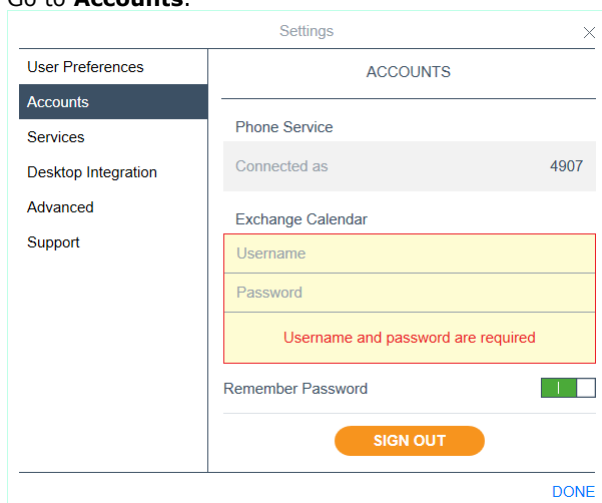
1. Depending on the operating system, click on the  settings icon or click on the  menu icon and then the  settings icon.

2. Select **Services | Exchange Calendar**.



The screenshot shows the 'Settings' dialog with the 'Services' tab selected. Under 'EXCHANGE CALENDAR', the 'Exchange Calendar' toggle is turned on. There are input fields for 'Domain' and 'Server Address'.

3. Enable **Exchange Calendar**.
4. Enter the Exchange server domain and server address details
5. Go to **Accounts**.




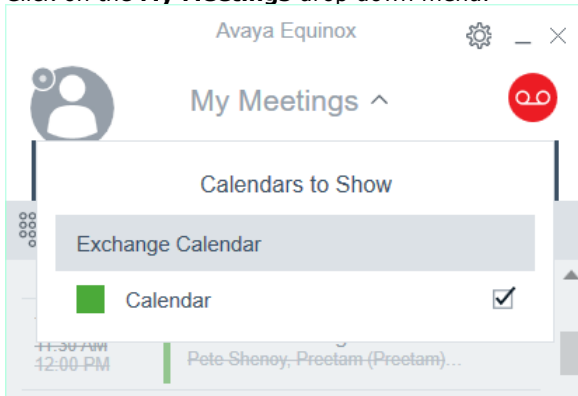
The screenshot shows the 'Settings' dialog with the 'Accounts' tab selected. Under 'Exchange Calendar', there are input fields for 'Username' and 'Password'. A red message box states 'Username and password are required'. There is a 'Remember Password' toggle and a 'SIGN OUT' button. A 'DONE' button is at the bottom right.

6. In the **Exchange Calendar** section, enter your email account details.
7. Click **Done**. The application will restart.
8. Following the restart you can [select Exchange as your calendar source](#) ¹¹⁵.

9.7.6.2 Calendar Selection

To select the calendar to display:

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.

9.7.7 Contact Integration

When you initially logged in to Avaya Avaya Equinox, you did not configure access to local contacts.

To enable contacts:

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**.





9.8 Troubleshooting

The Avaya Equinox client can send a collection of log files as an email.

9.8.1 Defaulting Equinox


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

To default the application settings:




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.
5. [Reconfigure the application](#) .

9.8.2 Emailing a Bug Report

The Avaya Equinox softphone can create an email with its application logs attached as a zipped file.

- On Android devices, to use this function you first need to [set an email address](#) .




To email a bug report:

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.

9.8.3 Setting the Email Address

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

To configure the email address for bug reports:

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.

Chapter 10.

Other Avaya SIP Phones

10. Other Avaya SIP Phones

This section provides notes for specific Avaya SIP phones where their installation differs from the [generic installation process](#)^[24]. The sections may also detail differences in operation when registered with an IP Office system rather than other Avaya systems.

10.1 1010, 1040 Telephones

The 1000 Series phones are high-quality SIP video phone devices. The 1010 and 1040 phones are supported. Each consists of a main module to which a range of video camera and microphone/speaker devices can be attached. The main module provides outputs for display of video on HD video compatible devices.

10.2 1100/1200 Series

IP Office supports the 1120E, 1140E, 1220 and 1230 telephones.

In most cases these phones are redeployed from previous Nortel BCM or SIP system and need migration from their existing firmware to Avaya IP Office SIP firmware.

The additional steps for the firmware migration options are detailed in the separate *"IP Office 1100/1200 Series Phone Installation"* manual. See [additional documentation](#)^[24].








10.3 B100 Series (B179)

IP Office supports the B179, a high-quality SIP conference phone.

The additional steps required for configuration of this type of phone to work with IP Office are covered in the separate *"Installing and Administering the IP Office B179 SIP Conference Phone"* manual. See [additional documentation](#)^[24].

To set the conference codes:

The B100 Series phones need to be configured with a number of conference codes. The main conference code required is one to conference the phone with any held calls it has. This should match a conference short code on the IP Office system. The default IP Office system short code is ***47**. The analog B149/B159 also need to be configured with codes to send a hook flash to the system to hold/unhold calls.

1. Press the  **Menu** button.
2. Scroll to **CONF GUIDE** and press **OK**.
3. Scroll to **SETTINGS** and press **OK**.
4. At the **ENQUIRY** prompt enter **F** and **OK**. Enter **F** by pressing the  key. Backspace by pressing  .
5. At the **CONFERENCE** prompt enter **F** and the IP Office conference short code, for example **F*47**. Press **OK**.
6. At the **RETURN** prompt enter **F** and press **OK**.
7. To exit the menus, press  **Menu** again, to exit the current menu option press  .

10.4 D100 Series (D160)

These DECT handsets use a base station that connects to the IP Office system using a SIP trunk and appear on the IP Office as SIP extensions. Their installation process requires creation of a SIP DECT line.

The additional steps required for configuration of this type of phone to work with IP Office are covered in the separate *"Installing and Administering IP Office D100 SIP Wireless Terminal"* manual. See [additional documentation](#)^[24].

10.5 E100 Series (E129, E159, E169)

IP Office supports the E129, E159 and E169 telephones.

The additional steps required for configuration of these type of phone to work with IP Office are covered in the separate "Installing and Maintaining Avaya E129 SIP Deskphone" and "Administering Avaya E129 SIP Deskphone" manuals. See [additional documentation](#).

10.5.1 E129

Following configuration of the system to [support SIP extension](#), there are a number of methods that can be used for individual E129 configuration. The method to use depends on whether the network has a DHCP server and whether that DHCP server has been configured to provide the file and SIP server information.

	Method	Description
1.	Full DHCP	Use this method to connect an E129 telephone if the network has a DHCP sever configured to provide the phone with IP address details plus file and server settings. This is the method to use if using the IP Office system as the DHCP server.
2.	Normal DHCP	Use this method to connect an E129 telephone if the network has a DHCP sever to provide the phone with an IP address, but that DHCP server is not configured to provide the phone with file and SIP server settings.
3.	Normal DHCP to Static IP	Use this method to connect an E129 telephone with a static IP address if the network has a DHCP sever. That server provides the phone with an initial IP address which is then changed to a static IP address during initial configuration.
4.	Static IP Method 1	Use this method if there is no DHCP server on the network but you have browser access to the network.
5.	Static IP Method 2	Use this method if there is no DHCP server on the network and no browser access to the network.

10.5.1.1 Full DHCP

Use this method to connect an E129 telephone if the network has a DHCP sever configured to provide the phone with IP address details plus file and server settings. This is the method to use if using the IP Office system as the DHCP server.

- To perform this process you need the extension number and login code of the [user created on the IP Office system](#) for the phone.

To connect an E129 telephone using full DHCP:


1. Connect the LAN cable from the network to the LAN port on the telephone.
2. If the cable provides PoE power, the phone will start booting. Otherwise, connect the phone's power supply to the DC 5V socket and switch on power to the telephone.
3. The phone will display various messages as it starts.
4. The phone may appear to repeat the booting process more than once. This is normal if the phone has downloaded a new firmware file.
5. When the phone displays **Username**, enter the extension number of the IP Office user added for the phone and press **OK**.
6. When the phone displays **Password**, enter the Login Code set in the IP Office configuration for that user and press **OK**.
7. The phone displays **Processing login...**
 - If the details are not recognized, the phone displays **Login failed** and then returns to displaying **Username**. Check the details required against those set in the IP Office configuration.
 - If the details are correct, the phone displays the normal idle display with **NextScr** and **Headset** buttons.
8. Make a test call to another extension.
9. Repeat the process for any other E129 telephone being installed.

10.5.1.2 Normal DHCP

Use this method to connect an E129 telephone if the network has a DHCP sever to provide the phone with an IP address, but that DHCP server is not configured to provide the phone with file and SIP server settings.

- To perform this process you need the extension number and login code of the [user created on the IP Office system](#) ⁽³⁾ for the phone.
- This method requires a web browser on the same network.

To connect an E129 telephone using partial DHCP:


1. Connect the LAN cable from the network to the LAN port on the telephone.
2. If the cable provides PoE power, the phone will start booting. Otherwise, connect the phone's power supply to the DC 5V socket and switch on power to the telephone.
3. The phone will display various messages as it starts.
4. When the phone displays **Username**, do not enter anything. Attempting to enter the user details at this stage will result in a brief **Server Unavailable** message before returning to the **Username** request.
5. Press the  conference button. The phone briefly displays the IP address it is currently using.
6. Enter that IP address in the web browser.
7. When the login menu appears, enter the administration password. The default password is **admin**.
 - a. Select **Accounts | Account 1 | General Settings**.
 - i. In the **SIP Server** field enter the IP address of the IP Office system LAN interface on which you want SIP phones supported.
 - ii. In the **SIP User ID** field enter the extension number of the IP Office user added for the phone.
 - iii. In the **Authenticate Password** field enter the Login Code set in the IP Office configuration for that user.
 - iv. Click **Save and Apply**.
 - b. Select **Maintenance | Upgrade and Provisioning**.
 - i. Set the **Firmware Server Path** to the IP address of the IP Office system.
 - ii. Set the **Config Server Path** to the IP address of the IP Office system.
 - iii. Click **Save and Apply**.
8. The phone displays various messages as it restarts. The phone may appear to repeat the booting process more than once. This is normal as the phone downloads a new firmware file.
9. Make a test call to another extension.
10. Repeat the process for any other E129 telephone being installed.

10.5.1.3 DHCP to Static IP

Use this method to connect an E129 telephone with a static IP address if the network has a DHCP sever. That server provides the phone with an initial IP address which is then changed to a static IP address during initial configuration.

- To perform this process you need the extension number and login code of the [user created on the IP Office system](#) ⁽³⁾ for the phone.
- You also need the static IP address settings for the phone (IP address, subnet mask and gateway address), the file server IP address and the SIP server address (IP Office LAN1 or LAN2).
- This method requires a web browser on the same network.

To connect an E129 telephone using static IP:


1. Connect the LAN cable from the network to the LAN port on the telephone.
2. If the cable provides PoE power, the phone will start booting. Otherwise, connect the phone's power supply to the DC 5V socket and switch on power to the telephone.
3. The phone will display various messages as it starts.
4. When the phone displays **Username**, do not enter anything. Attempting to enter the user details at this stage will result in a brief **Server Unavailable** message before returning to the **Username** request.
5. Press the  conference button. The phone briefly displays the IP address it is currently using.
6. Enter that IP address in the web browser.
7. When the login menu appears, enter the administration password. The default password is **admin**.
 - a. Select **Accounts | Account 1 | General Settings**.
 - i. In the **SIP Server** field enter the IP address of the IP Office system LAN interface on which you want SIP phones supported.
 - ii. In the **SIP User ID** field enter the extension number of the IP Office user added for the phone.
 - iii. In the **Authenticate Password** field enter the Login Code set in the IP Office configuration for that user.
 - iv. Click **Save and Apply**.
 - b. Select **Maintenance | Upgrade and Provisioning**.
 - i. Set the **Firmware Server Path** to the IP address of the IP Office system.
 - ii. Set the **Config Server Path** to the IP address of the IP Office system.
 - iii. Click **Save and Apply**.
 - a. Select **Network | Basic Settings**.
 - i. Click **Statically configured as**.
 - ii. In the **IPv4 Address**, **Subnet Mask** and **Gateway** fields enter the IP address details that the phone should use.
 - iii. Click **Save and Apply**.
 - d. Click **Reboot** (top-right). When prompted click **OK**. Close the browser.
8. The phone displays various messages as it restarts. The phone may appear to repeat the booting process more than once. This is normal as the phone downloads a new firmware file.
9. Make a test call to another extension.
10. Repeat the process for any other E129 telephone being installed.

10.5.1.4 Static IP Method 1

Use this method if there is no DHCP server on the network but you have browser access to the network.

- To perform this process you need the extension number and login code of the [user created on the IP Office system](#) ³ for the phone.
- You also need the static IP address settings for the phone (IP address, subnet mask and gateway address), the file server IP address and the SIP server address (IP Office LAN1 or LAN2).
- This method requires a web browser on the same network.

To connect an E129 telephone using no DHCP:

1. Connect the LAN cable from the network to the LAN port on the telephone.
2. If the cable provides PoE power, the phone will start booting. Otherwise, connect the phone's power supply to the DC 5V socket and switch on power to the telephone.
3. The phone will display various messages as it starts.
 - a. The phone eventually displays **NETWORK DOWN**. Press the ● button.
 - b. Scroll down to **Network Config** and press ●.
 - c. Scroll down to **IP Setting** and press ●.
 - d. Scroll down to **Static IP** and press ●. The phone is now set to use a static IP address. To set that address:
 - e. Scroll down to **IP** and press ●. Enter the IP address for the phone. Use the * key to enter dots. Press **OK**.
 - f. Scroll down to **Netmask** and press ●. Enter the subnet mask for the phone and press **OK**.
 - g. Scroll down to **Gateway** and press ●. Enter the networks default gateway (router) address and press **OK**.
 - h. Scroll down to **Back** and press ●.
 - i. The phone prompts you for a reboot. Press **Reboot**.
4. When the phone displays **Username**, do not enter anything. Attempting to enter the user details at this stage will result in a brief **Server Unavailable** message before returning to the **Username** request.
5. Press the  conference button. The phone briefly displays the IP address it is currently using.
6. Enter that IP address in the web browser.
7. When the login menu appears, enter the administration password. The default password is **admin**.
 - a. Select **Accounts | Account 1 | General Settings**.
 - i. In the **SIP Server** field enter the IP address of the IP Office system LAN interface on which you want SIP phones supported.
 - ii. In the **SIP User ID** field enter the extension number of the IP Office user added for the phone.
 - iii. In the **Authenticate Password** field enter the Login Code set in the IP Office configuration for that user.
 - iv. Click **Save and Apply**.
 - b. Select **Maintenance | Upgrade and Provisioning**.
 - i. Set the **Firmware Server Path** to the IP address of the IP Office system.
 - ii. Set the **Config Server Path** to the IP address of the IP Office system.
 - iii. Click **Save and Apply**.
8. The phone displays various messages as it restarts. The phone may appear to repeat the booting process more than once. This is normal as the phone downloads a new firmware file.
9. Make a test call to another extension.
10. Repeat the process for any other E129 telephone being installed.

10.5.1.5 Static IP Method 2

Use this method if there is no DHCP server on the network and no browser access to the network.

- To perform this process you need the extension number and login code of the [user created on the IP Office system](#) ¹³⁷ for the phone.
- You also need the static IP address settings for the phone (IP address, subnet mask and gateway address), the file server IP address and the SIP server address (IP Office LAN1 or LAN2).


To connect an E129 telephone using no DHCP:

1. Connect the LAN cable from the network to the LAN port on the telephone.
2. If the cable provides PoE power, the phone will start booting. Otherwise, connect the phone's power supply to the DC 5V socket and switch on power to the telephone.
3. The phone will display various messages as it starts.
4. The phone eventually displays **NETWORK DOWN**. Press the **●** button.
5. Scroll to **Network Config** and press **●**.
 - a. Scroll to **IP Setting** and press **●**.
 - b. Scroll to **Static IP** and press **●**. The phone is now set to use a static IP address. To set that address:
 - c. Scroll to **IP** and press **●**. Enter the IP address for the phone. Use the * key to enter dots. Press **OK**.
 - d. Scroll to **Netmask** and press **●**. Enter the subnet mask for the phone and press **OK**.
 - e. Scroll to **Gateway** and press **●**. Enter the networks default gateway (router) address and press **OK**.
 - f. Scroll to **Back** and press **●**.
 - g. The phone prompts you for a reboot. Press **No**. If you do select **Reboot**, continue as from Step 7 of the [DHCP to Static IP connection](#) ¹²⁷ process.
6. Scroll to **Config** and press **●**.
 - a. Scroll to **SIP Proxy** and press **●**. Enter the IP address of the IP Office system LAN interface on which you want SIP phones supported and press **OK**.
 - b. Scroll to **SIP User ID** and press **●**. Enter the extension number of the IP Office user added for the phone and press **OK**.
 - c. Scroll to **SIP Password** and press **●**. Enter the Login Code set in the IP Office configuration for that user and press **OK**.
 - d. Scroll to **Save** and press **●**.
7. Scroll to **Upgrade** and press **●**.
 - a. Scroll to **Firmware Server** and press **●**. Enter the IP address of the IP Office system and press **OK**.
 - b. The phone prompts you for a reboot. Press **No**. If you do select **Reboot**, continue as from Step 7 of the [DHCP to Static IP connection](#) ¹²⁷ process.
 - c. Scroll to **Config Server** and press **●**. Enter the IP address of the IP Office system and press **OK**.
 - d. The phone prompts you for a reboot. Press **Reboot**.
8. The phone displays various messages as it restarts. The phone may appear to repeat the booting process more than once. This is normal as the phone downloads a new firmware file.
9. Make a test call to another extension.
10. Repeat the process for any other E129 telephone being installed.

10.5.1.6 Troubleshooting Telephone Connection

Username Keeps Reappearing

If the **Username** option keeps appearing after entering the user details, that indicates that either the telephone is not configured with the correct address of the SIP server or that the IP Office does not support the SIP extension registration.

During this state, you can press the  conference button to display the phone's current IP address if set.

1. Check that the IP Office system is configured to support SIP extensions. If not, [correct the system configuration](#) ^[25] and then restart the telephone connection process.
2. Check that the IP Office system has available Avaya IP Endpoint licenses. This can be done using the IP Office System Status Application. If no licenses are available, correct the [license availability](#) ^[10] and then restart the telephone connection process.
3. If using a third-party DHCP server configure with the additional options for providing file and SIP server details, check that the SIP server address is correctly set to the IP Office address (LAN1 or LAN2) on which SIP extensions are being supported. If the DHCP server needs reconfiguring, do so and then restart the telephone connection process.
4. If using a DHCP server that is not configured to provide file and SIP server addresses, use the [DHCP to Static IP](#) ^[121] connection process.
5. If not using DHCP, user [Static IP Method 1](#) ^[122] process from step 4.

Server Unavailable

This message appears briefly if the SIP server setting is not correctly set. See Username above.

Network Down

The **Network Down** message appears briefly during startup of the telephone. This is normal and does not indicate a problem. If the message remains displayed after the phone starts, it indicates that either there is no physical network connection or that the phone does not have any IP address.

Having checked the network cable connection, the latter problem will occur if there is has been no response from a DHCP server to provide the telephone with an IP address. If using DHCP, check the DHCP server connection and then restart the phone. If not using DHCP, see [Static IP Method 1](#) ^[122] to set the phone to a static IP address.

Login Failed

The **Login Failed** message indicates that the user name and password details were not recognized by the SIP server (IP Office). Check that the values being entered match the user and extension configured in the IP Office system configuration.

Phone reboots more than once when restarting

This is normal behaviour if the phone has downloaded new firmware. The default setting is for the phone to always check for and download the firmware whenever it is restarted.

10.5.1.7 Obtaining the Phone's IP Address

Regardless of whether installed using DHCP or with a static address, the phone can display its current IP address. This address can then be used for browser access to the phone.

To obtain the phone's IP address:

1. With the phone idle, press **NextScr**. The telephone displays its current IP address.
2. Press **NextScr** again. The telephone displays its account name. This matches the user's IP Office user name.
3. Press **NextScr** again to return the telephone back to idle.

10.5.1.8 Changing the Web Access Passwords

There are two levels of browser access to the telephone, user access and full administrator access.

To change the phone's browser access passwords:

1. Access the telephone's web configuration menus:
 - a. In a web browser, enter the phone's IP address. The default address uses http://, however https:// access can be configured if required.
 - b. When the SIP Deskphone login menu is displayed, enter the phone's current password for full administration access. The default password for this is **admin** for full administration access.
2. Click **Maintenance** and select **Web Access**.
3. In the menu enter and confirm the new passwords that the phone should use.
4. Click **Save and Apply**.

10.5.1.9 Hiding the Phone Configuration Menus

The menus on the phone display that relate to phone configuration can be hidden.

To restrict reconfiguration via the phone's menus:

1. Access the telephone's web configuration menus:
 - a. In a web browser, enter the phone's IP address. The default address uses http://, however https:// access can be configured if required.
 - b. When the SIP Deskphone login menu is displayed, enter the phone's current password for full administration access. The default password for this is **admin** for full administration access.
2. Click **Maintenance** and select **Security**.
3. Select the level of configuration access that should be allowed from the phone:
 - **Unrestricted**
If this mode is selected, all the phone menus are accessible.
 - **Basic settings only**
If this mode is selected, the **CONFIG** menu on the phone is not accessible.
 - **Constraint Mode**
If this mode is selected, the **CONFIG** and **FACTORY FUNCTIONS** menus on the phone are not accessible.
4. Click **Save and Apply**.

10.5.1.10 Reset an E129

To reset an E129:

1. Press the **●** button.
2. Scroll to **Config** and press **●**.
3. Scroll to **Factory Rest** and press **●**.
4. Press **OK** twice.

10.5.2 E159, E169

The E159 and E169 media stations are supported for IP Office Release 9.03 and 9.1 onwards.

Restrictions/Limitations

Consider the following limitations when administering the media station on IP Office:

- With IP Office Version 9.0.3, the firmware files for these phone are not part of the IP Office software.
- These phones do not support TLS or SRTP.
- These phones do not support the system directory.
- These phone are not supported in centralized branch deployments.
- These phones are not supported for IP Office resilience.

10.6 H100 Series (H715)

IP Office supports the H175 video collaboration telephone from IP Office Release 10.0 onwards.

The additional steps required for configuration of this type of phone to work with IP Office are covered in the separate *"Installing and Maintaining Avaya H100-Series Video Collaboration Stations"* and *"Administering Avaya H100-Series Video Collaboration Stations"* manuals. See [additional documentation](#)^[2].

Chapter 11.

3rd-Party SIP Phones

11. 3rd-Party SIP Phones

Through the its Solutions & Interoperability Lab, Avaya issues a range of application notes. These include application notes for particular models of third-part SIP telephones. Application notes can be downloaded from the Avaya DevConnect web site (http://www.devconnectprogram.com/site/global/compliance_testing/application_notes/index.gsp).

Brand	Model	Brand	Model
Algo	8028 SIP Door Phone	Grandstream	GXV3240
	8036 SIP Multimedia Intercom		GXV3275
	8128 SIP Strobe Light	LiveSentinel	SIP Video Door Intercom
	8180 SIP Audio Alerter	Polycom	SoundStation Duo
	8188 SIP Ceiling Speaker	QSC	Q-Sys SIP Softphone
	8301 SIP Paging Adapter	Revolabs	FLX UC 1000
	3226 Trunk Port FXO Doorphone	Valcom	One-Way IP Speakers PagePro IP
Ascom	i62 VoWiFi handset i75 VoWiFi Handset Myco Wireless Smartphones	Yealink	T-18 SIP Phones T-20 SIP Phones T-28 SIP Phones T-26 SIP Phones T-22 SIP Phones VP530 SIP Video Phone
Interquartz	Endurance 10CS		
Cetis	3300IP Series SIP Telephones 9600IP Series SIP Telephones		
G-Tek	AQ-10x		
	ASP-8210-SMK		
	ASP-6210-S		
	AAX-4100	Teledex	SIP ND2000 Series SIP NDC2000 Series SIP LD4200 Series

11.1 General Notes

- **Multiple Line SIP Devices**

Some SIP devices can support multiple lines or user accounts, each configured separately. If used with an IP Office each SIP line requires a separate IP Office SIP extension, user and license. Note this refers to a SIP device that can handle multiple simultaneous calls itself and not one that is handling multiple calls by holding them on the IP Office/receiving call waiting indication for waiting calls on the IP Office. For the later, the IP Office limits 3rd-party SIP devices to a maximum of 6 concurrent calls.

- **The IP Office is the SIP Registrar and SIP Proxy**

In most cases, a SIP extension device is configured with settings for a SIP registrar and a SIP proxy. For SIP devices connecting to an IP Office, the LAN1 or LAN2 IP address on which the SIP registrar is enabled is used for both roles.

- **SIP Codec Selection**

Unlike H323 IP devices which always support at least one G711 codec, SIP devices do not support a single common audio codec. Therefore, it is important to ensure that any SIP device is configured to match at least one system codec configured on the system.

- **G.723/G.729b**

These codecs are not available on Linux based IP Office systems. They are supported on IP500 V2 systems with VCM channels.

- **Simultaneous Calls**

3rd-Party SIP extensions are limited by default to 6 simultaneous calls. However this can be changed if required by associating additional 3rd-party endpoint licenses with the extension. See [Simultaneous Calls](#)^[13].

3rd-Party SIP Telephone Features

- Beyond basic call handling via the IP Office (see the features listed below), the features available will vary between SIP devices and Avaya cannot make any commitments as to which features will or will not work or how features are configured.

- | | | | |
|------------------------|---------------------------------|------------------------------|--------------------------|
| • Answer calls. | • Hold. | • Voicemail Collect. | • Hear Page Calls |
| • Make calls. | • Unsupervised Transfer. | • Set Forwarding/DND. | |
| • Hang Up. | • Supervised Transfer. | • Park/Unpark. | |

11.2 Simultaneous Calls

3rd-Party SIP extensions are limited by default to 6 simultaneous calls. However, a user Source Number can be used to allow a 3rd-party SIP extension to consume multiple 3rd-party endpoint licenses. Each additional license enables another 6 simultaneous calls, up to a maximum of 30 calls in total (4 additional licenses).

The user Source Number is **ULI=N** where **N** is the number of additional license from 1 to 4. Note that changes to the user Source Number require a system restart to take effect.

Chapter 12.

Appendix

12. Appendix

12.1 Example 46xxsettings.txt File

Below is an example auto-generated 46xxsettings.txt file from a IP Office R11.0 system.

The sections labeled ...AUTOGENERATEDSETTINGS are used to contain settings that have values that have been automatically adjusted to match the IP Office system's configuration settings. The sections after the NONAUTOGENERATEDSETTINGS label contain settings which for IP Office operation have set values.

If you need to add or change settings it is recommended that you do this using a separate 46xxspecials.txt file. The presence of a 46xxspecials.txt file on a system will automatically add the line `GET 46xxspecials.txt` to the end of the auto-generated 46xxsettings.txt file. Settings in the 46xxspecials.txt file will override any matching setting in the 46xxsettings.txt file.

Example 46xxsettings.txt File

Note this is just an example file with settings specific to the system from which it was copied.

```

## IPOFFICE/11.0.0.0.0 build 822 192.168.0.180 AUTOGENERATED
IF $MODEL4 SEQ 1603 GOTO 16XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 1608 GOTO 16XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 1616 GOTO 16XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9620 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9630 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9640 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9650 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9608 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9611 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9621 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9641 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J129 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J139 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J169 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J179 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K175 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K165 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K155 GOTO SIPXAUTOGENERATEDSETTINGS
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 4000
SET TLSSRVRID 0
SET ENABLE_G711U 1
SET ENABLE_G711A 1
SET ENABLE_G729 1
SET ENABLE_G722 0
SET ENABLE_G726 0
SET ENABLE_OPUS 0
SET DTMF_PAYLOAD_TYPE 101
SET SIPDOMAIN example.com
SET ENFORCE_SIPS_URI 0
SET DSCPAUD 46
SET DSCPSIG 34
SET TLSSRVR 192.168.0.180
SET TLSPT 443
SET HTTPPORT 80
SET TRUSTCERTS WebRootCA.pem
SET COUNTRY USA
SET ISO_SYSTEM_LANGUAGE en_US
IF $MODEL4 SEQ J129 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J139 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J169 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J179 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K175 GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K165 GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K155 GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aca GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aci GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acm GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acw GOTO K1EXAUTOGENERATEDSETTINGS
# J1X9AUTOGENERATEDSETTINGS
SET RTCPMON 192.168.0.180
SET RTCPMONPORT 5005
IF $MODEL4 SEQ J129 GOTO J129AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J139 GOTO STIMULUSPHONECOMMONSETTINGS
IF $MODEL4 SEQ J169 GOTO STIMULUSPHONECOMMONSETTINGS
IF $MODEL4 SEQ J179 GOTO STIMULUSPHONECOMMONSETTINGS
GOTO NONAUTOGENERATEDSETTINGS
# J129AUTOGENERATEDSETTINGS
SET USER_STORE_URI "https://192.168.0.180:443/user"
SET MWISRV "192.168.0.180"
SET SIP_CONTROLLER_LIST 192.168.0.180:5060;transport=tcp
SET FQDN_IP_MAP "storm1.example.com=192.168.0.180"
SET AUTH 0
SET ENCRYPT_SRTCP 0
SET GMTOFFSET +1:00
SET SNTPSRVR ""
SET DSTOFFSET 0
SET PHNMOREEMERGNMS "911"
SET PHNEMERGNM "911"

```

```

SET LANGUAGES Mlf_J129_LatinAmericanSpanish.xml,Mlf_J129_CanadianFrench.xml,Mlf_J129_BrazilianPortugu
SET SYSTEM_LANGUAGE Mlf_J129_English.xml
SET MEDIAENCRYPTION 9
GOTO NONAUTOGENERATEDSETTINGS
# STIMULUSPHONECOMMONSETTINGS
SET SIP_CONTROLLER_LIST 192.168.0.180:5060;transport=tcp
SET FQDN_IP_MAP "storm1.example.com=192.168.0.180,storm5.example.com=192.168.0.182"
SET AUTH 0
SET MEDIA_PRESERVATION 1
SET PRESERVED_CONNECTION_DURATION 120
SET MEDIAENCRYPTION 9
SET LANGUAGES Mlf_J169_J179_LatinAmericanSpanish.xml,Mlf_J169_J179_CanadianFrench.xml,Mlf_J169_J179_P
SET SYSTEM_LANGUAGE Mlf_J169_J179_English.xml
GOTO NONAUTOGENERATEDSETTINGS
# K1EXAUTOGENERATEDSETTINGS
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 1
SET SIP_CONTROLLER_LIST storm1.example.com:5060;transport=tcp
SET CONFERENCE_FACTORY_URI "ConfServer@example.com"
SET PSTN_VM_NUM "VM.user@example.com"
SET SETTINGS_FILE_URL "https://storm1.example.com:443/46xxsettings.txt"
SET FQDN_IP_MAP "storm1.example.com=192.168.0.180"
SET MEDIAENCRYPTION 9
SET ENCRYPT_SRTCP 0
SET DSCPVID 46
IF $MODEL4 SEQ K175 GOTO K1XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K165 GOTO K1XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K155 GOTO K1XXAUTOGENERATEDSETTINGS
GOTO NONAUTOGENERATEDSETTINGS
# K1XXAUTOGENERATEDSETTINGS
SET USER_STORE_URI "https://192.168.0.180:443"
SET SNTPSRVR "192.168.0.180"
SET INTER_DIGIT_TIMEOUT 4
SET NO_DIGITS_TIMEOUT 30
GOTO NONAUTOGENERATEDSETTINGS
# 16XXAUTOGENERATEDSETTINGS
SET LANG1FILE "mlf_Sage_v502_spanish_latin.txt"
SET LANG2FILE "mlf_Sage_v502_french_can.txt"
SET LANG3FILE "mlf_Sage_v502_portuguese.txt"
SET LANG4FILE "mlf_Sage_v502_italian.txt"
SET BRURI "http://192.168.0.180:80/user/backuprestore/"
SET HTTPPORT "80"
GOTO NONAUTOGENERATEDSETTINGS
# 96XXAUTOGENERATEDSETTINGS
IF $SIG SEQ 2 GOTO NONAUTOGENERATEDSETTINGS
SET SCREENSAVERON 240
SET SCREENSAVER 96xxscr.jpg
SET LANG1FILE "mlf_S31_v76_spanish_latin.txt"
SET LANG2FILE "mlf_S31_v76_french_can.txt"
SET LANG3FILE "mlf_S31_v76_portuguese.txt"
SET LANG4FILE "mlf_S31_v76_italian.txt"
SET BRURI "http://192.168.0.180:80/user/backuprestore/"
SET HTTPPORT "80"
GOTO NONAUTOGENERATEDSETTINGS
# 96X1AUTOGENERATEDSETTINGS
SET TRUSTCERTS "Root-CA-02062813.pem"
SET TLSSRRVRFYID 1
IF $SIG SEQ 2 GOTO NONAUTOGENERATEDSETTINGS
SET BRURI "https://192.168.0.180:443/user/backuprestore/"
SET HTTPPORT "80"
SET SCREENSAVERON 240
IF $MODEL4 SEQ 9608 GOTO BRANDINGSCR9608
SET SCREENSAVER 96xxscr.jpg
GOTO BRANDINGSCREND
# BRANDINGSCR9608
SET SCREENSAVER 9608scr.jpg
GOTO BRANDINGSCREND
# BRANDINGSCREND
SET LANG1FILE "mlf_96x1_v148_spanish_latin.txt"
SET LANG2FILE "mlf_96x1_v148_french_can.txt"
SET LANG3FILE "mlf_96x1_v148_portuguese.txt"
SET LANG4FILE "mlf_96x1_v148_italian.txt"
IF $MODEL4 SEQ 9608 GOTO NONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9611 GOTO NONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J169 GOTO NONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J179 GOTO NONAUTOGENERATEDSETTINGS
SET WEATHERAPP ""
SET WORLDCLOCKAPP ""

```



```

SET WMLHELPSTAT 0
GOTO NONAUTOGENERATEDSETTINGS
# NONAUTOGENERATEDSETTINGS
SET USBLOGINSTAT 0
SET ENHDIALSTAT 0
# PRODUCT_LINE_SETTINGS
IF $MODEL4 SEQ 1603 GOTO SETTINGS16XX
IF $MODEL4 SEQ 1608 GOTO SETTINGS16XX
IF $MODEL4 SEQ 1616 GOTO SETTINGS16XX
IF $MODEL4 SEQ 9620 GOTO SETTINGS96X0
IF $MODEL4 SEQ 9630 GOTO SETTINGS96X0
IF $MODEL4 SEQ 9640 GOTO SETTINGS96X0
IF $MODEL4 SEQ 9650 GOTO SETTINGS96X0
IF $MODEL4 SEQ 9608 GOTO SETTINGS96X1
IF $MODEL4 SEQ 9611 GOTO SETTINGS96X1
IF $MODEL4 SEQ 9621 GOTO SETTINGS96X1
IF $MODEL4 SEQ 9641 GOTO SETTINGS96X1
IF $MODEL4 SEQ J129 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ J139 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ J169 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ J179 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ K175 GOTO SETTINGSK1EX
IF $MODEL4 SEQ K165 GOTO SETTINGSK1EX
IF $MODEL4 SEQ K155 GOTO SETTINGSK1EX
IF $MODEL4 SEQ aca GOTO SETTINGSK1EX
IF $MODEL4 SEQ aci GOTO SETTINGSK1EX
IF $MODEL4 SEQ acm GOTO SETTINGSK1EX
IF $MODEL4 SEQ acw GOTO SETTINGSK1EX
GOTO PER_MODEL_SETTINGS
# SETTINGS96X1
SET UNNAMEDSTAT 0
IF $SIG_IN_USE SEQ H323 GOTO SETTINGS96X1H323
SET TLSSRVRID 0
SET SUBSCRIBE_SECURITY 0
SET ENFORCE_SIPS_URI 0
GOTO PER_MODEL_SETTINGS
# SETTINGS96X1H323
GOTO PER_MODEL_SETTINGS
# SETTINGS96X0
IF $SIG SEQ 2 GOTO SETTINGSSIP96xx
GOTO PER_MODEL_SETTINGS
# SETTINGSSIP96xx
SET TLSSRVRID 0
SET SUBSCRIBE_SECURITY 0
SET ENFORCE_SIPS_URI 0
GOTO PER_MODEL_SETTINGS
# SETTINGS16XX
GOTO PER_MODEL_SETTINGS
# SETTINGSJ1X9
IF $SIG_IN_USE SEQ H323 GOTO PER_MODEL_SETTINGS
SET SIMULTANEOUS_REGISTRATIONS 1
SET ENABLE_AVAYA_ENVIRONMENT 0
SET SIPREGPROXYPOLICY "alternate"
SET DISCOVER_AVAYA_ENVIRONMENT 0
SET FAILBACK_POLICY admin
SET SEND_DTMF_TYPE 2
SET SYMMETRIC_RTP 1
SET SIG_PORT_LOW 1024
SET SIG_PORT_RANGE 64511
SET TCP_KEEP_ALIVE_STATUS 1
SET ENABLE_PRESENCE 0
SET ENABLE_SHOW_EMERG_SK 0
SET ENABLE_SHOW_EMERG_SK_UNREG 0
SET TCP_KEEP_ALIVE_TIME 30
IF $MODEL4 SEQ J139 GOTO STIMULUSSETTINGS
IF $MODEL4 SEQ J169 GOTO STIMULUSSETTINGS
IF $MODEL4 SEQ J179 GOTO STIMULUSSETTINGS
GOTO PER_MODEL_SETTINGS
# STIMULUSSETTINGS
SET ENABLE_IPOFFICE 2
SET SDPCAPNEG 1
SET CONNECTION_REUSE 1
SET ENCRYPT_SRTP 0
SET SSH_ALLOWED 0
SET INGRESS_DTMF_VOL_LEVEL -1
GOTO PER_MODEL_SETTINGS
# SETTINGSK1EX

```

```

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 SUBSCRIBE_LIST_NON_AVAYA "reg,message-summary,avaya-ccs-profile"
SET SDPCAPNEG 1
SET SIPENABLED 1
IF $MODEL4 SEQ K175 GOTO SETTINGSK1XX
IF $MODEL4 SEQ K165 GOTO SETTINGSK1XX
IF $MODEL4 SEQ K155 GOTO SETTINGSK1XX
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 PER_MODEL_SETTINGS
# SETTINGSK1XX
SET UPGRADE_POLICY 0
SET REGISTERWAIT 300
SET CONNECTION_REUSE 1
SET ENABLE_PHONE_LOCK 0
SET POUND_KEY_AS_CALL_TRIGGER 0
GOTO END
# PER_MODEL_SETTINGS
IF $MODEL4 SEQ 1603 GOTO SETTINGS1603
IF $MODEL4 SEQ 1608 GOTO SETTINGS1608
IF $MODEL4 SEQ 1616 GOTO SETTINGS1616
IF $MODEL4 SEQ 9620 GOTO SETTINGS9620
IF $MODEL4 SEQ 9630 GOTO SETTINGS9630
IF $MODEL4 SEQ 9640 GOTO SETTINGS9640
IF $MODEL4 SEQ 9650 GOTO SETTINGS9650
IF $MODEL4 SEQ 9608 GOTO SETTINGS9608
IF $MODEL4 SEQ 9611 GOTO SETTINGS9611
IF $MODEL4 SEQ 9621 GOTO SETTINGS9621
IF $MODEL4 SEQ 9641 GOTO SETTINGS9641
IF $MODEL4 SEQ J129 GOTO SETTINGSJ129
IF $MODEL4 SEQ J169 GOTO SETTINGSJ169
IF $MODEL4 SEQ J179 GOTO SETTINGSJ179
GOTO END
# SETTINGSEQNX
SET SSOENABLED 0
SET SETTINGS_CHECK_INTERVAL 1
SET APPCAST_ENABLED 0
SET APPCAST_URL 0
SET APPCAST_CHECK_INTERVAL 0
SET ENABLE_BROWSER_EXTENSION 0
SET WINDOWS_IMPROVIDER 0
SET ENABLE_OUTLOOK_ADDON 1
SET OUTLOOK_CALL_CONTACT 1
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 1
SET OBSCURE_PREFERENCES "ESMENABLED,ESMSRVR,ESMPORT,ESMREFRESH,ESMUSERNAME,ESMPASSWORD,ACSENABLED,AC"
GOTO END
# SETTINGS1603
GOTO END
# SETTINGS1608
GOTO END
# SETTINGS1616
GOTO END
# SETTINGS9620
GOTO END
# SETTINGS9630
GOTO END
# SETTINGS9640
GOTO END
# SETTINGS9650
GOTO END
# SETTINGS9608
GOTO END
# SETTINGS9611
GOTO END
# SETTINGS9621

```

```
GOTO END
# SETTINGS9641
GOTO END
# SETTINGSJ129
SET CONFERENCE_TYPE 0
SET ENABLE_IPOFFICE 1
SET SUBSCRIBE_LIST_NON_AVAYA "reg,message-summary,avaya-ccs-profile"
SET MUTE_ON_REMOTE_OFF_HOOK 0
SET PSTN_VM_NUM "VM.user"
SET ENABLE_RECORDING 0
SET BLUETOOTHSTAT 1
SET INSTANT_MSG_ENABLED 0
SET SIPCONFERENCECONTINUE 0
SET ENABLE_CONTACTS 1
SET SUBSCRIBE_SECURITY 0
SET RTCPCONT 1
SET RTCP_XR 1
SET USE_QUAD_ZEROES_FOR_HOLD 0
SET ENABLE_EARLY_MEDIA 1
SET PHY1STAT 1
SET PHY2STAT 1
SET PHY2TAGS 0
SET DHCPSTD 0
SET ICMPDU 1
SET ICMPRED 0
SET AUDASYS 3
SET AUDIOENV 1
SET PHONE_LOCK_IDLETIME 0
SET LOCALLY_ENFORCE_PRIVACY_HEADER 0
SET PHNMUTEALERT_BLOCK 0
SET ENABLE_PHONE_LOCK 1
SET CONTROLLER_SEARCH_INTERVAL 4
SET FAST_RESPONSE_TIMEOUT 4
SET RINGTONES ""
SET RINGTONESTYLE 0
SET G726_PAYLOAD_TYPE 110
SET NO_DIGITS_TIMEOUT 50
SET INTER_DIGIT_TIMEOUT 5
SET DAYLIGHT_SAVING_SETTING_MODE 0
SET DSTOFFSET ""
SET SECURECALL 0
SET SSH_ALLOWED 2
SET SSH_BANNER_FILE ""
SET SSH_IDLE_TIMEOUT 10
SET LLDP_ENABLED 1
SET PLUS_ONE 1
SET INSTANT_MSG_ENABLED 0
SET ENABLE_MODIFY_CONTACTS 1
SET ENABLE_MULTIPLE_CONTACT_WARNING 0
SET ENABLE_REDIAL 1
SET ENABLE_REDIAL_LIST 1
SET ENABLE_CALL_LOG 1
SET PROVIDE_LOGOUT 0
SET SOFTKEY_CONFIGURATION 0,1,3
SET POE_CONS_SUPPORT 1
SET SUBSCRIBE_SECURITY 0
SET PHNNUMOFS 2
SET DATESEPARATOR /
SET DATETIMEFORMAT 0
SET DIALWAIT 5
SET RTCPMONPERIOD 5
SET APPSTAT 0
SET PROCSTAT 0
SET ENHDIALSTAT 0
SET PHNCC 1
SET PHNDPLENGTH 7
SET PHNIC 011
SET PHNLD 1
SET PHNLDLENGTH 10
SET PHNOL ""
SET QKLOGINSTAT 1
SET VLANTEST 60
GOTO END
# SETTINGSJ169
GOTO END
# SETTINGSJ179
GOTO END
```

END

12.2 Example 46xxspecials.txt File

To obtain an example of a complex structure, you can browse to <http://<IPOffice>/46xxspecials.txt> to obtain an auto-generated file. [Save and edit](#)^[18] that file before [uploading](#)^[41] it back to the system.

```
## IPOFFICE/11.0.0.0.0 build 821 192.168.0.1 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 K165 GOTO K1XXSPECIALS
IF $MODEL4 SEQ K175 GOTO K1XXSPECIALS
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
# 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
```

12.3 Document History

Date	Issue	Changes
23rd April 2018	03a	Update for IP Office Release 11.0. See What's New ^[10] .
1st May 2018	03b	<ul style="list-style-type: none"> Addition of notes for Zang with Equinox.
9th May 2018	03c	<ul style="list-style-type: none"> Addition of Vantage NoUser Source Number for firmware version.
10th May 2018	03d	<ul style="list-style-type: none"> Notes regarding HTTPS for directory display on Vantage phones. [IPOFFICE-137853] Hot-desking not supported on Vantage phones. Equinox not supported on macOS 10.10.
18th May 2018	03e	<ul style="list-style-type: none"> Note that J169/J179 phones are reported as 9611 phones when using the pre-R11.0 firmware. Minor correct to J100 Branch wording (unfinished sentence).

Index

1

1000 Series Phones 118
1100 Series Phones 118
1200 Series Phones 118
176 30

2

242 30, 50

3

3rd-Party IP Phones license 10

A

Account Code 19
Allow Direct Media 27
Allow Direct Media Path 32
Application Notes 21
Applications 11
Apply to Avaya IP Phones Only 29
Aura 20
Authorisation Code 19
Auto-answer 32
Auto-Creation
 Extensions 34
 Users 34
Auto-generation 14
Avaya IP Endpoints license 10

B

B100 Series Phones 118
Base Extension 32
Blacklisting 62
Branch 20

C

Calls
 Monitor 62
Centralized Branch 20
Certificates 52
Challenge Expiry Time 25
Codec 32
 Extension 32
 Lockdown 32
Codecs 27
Create identity certificates 56

D

D100 Series Phones 118
Data 11
DHCP 11, 12
 242 50
 Apply to Avaya IP Phones Only 29
 Mode 29
 Option 50
 Pools 29
 Settings 28
 SSON 30, 50
DHCP Server
 Alternate 48
Direct Media 27, 32
Disk 39
Documentations 21
Domain Name 25
Download
 Certificate 53
DTMF 27, 32

E

E100 Series Phones 119
Edit
 Extension 32
 Scope 50
 Settings 18
 SSON 69
 User 31
Extension
 Auto-creation 34
 Codec 32
 Register 35
 User 31

F

Failback 18
Failover 18
File Server 13, 38
 Certificate 58
 Upload files 41
Files
 Upload 41
Force Authorization 31
FQDN 25
Fully Qualified Domain Name 25

H

H100 Series Phones 126
Hold Music 32
Hot desking 19
HTTP
 Clients Only 39
 File Server Address 39
 Redirection 39

I

Identity Certificate
 File Server 58
Inband 32

J

J100 Series Phones 66

L

Layer 4 Protocol 25
Licenses 10
Local Hold Music 32
Log in 19
Log out 19
Login Code 31

M

Manuals 21
Media Security 32
Memory Card 39
Minimum Assessment Target 11
Monitor 62

N

Name
 User 31
network assessment 11

O

Option 50

P

Packet Loss 11
Phone
 Register 35

Phones

- 1100 Series 118
- 1200 Series 118
- 3rd-Party 130
- B100 118
- D100 118
- E100 Series 119
- H100 Series 126
- J100 Series 66

PoE 12

Pools 29

Power 12

Protocol 25

Provisioning Server 13, 38

Q

Quality 11

R

Register 35

- Blacklisting 62
- View 62

Registrar 25

Remote Extension

- Enable 25

Reserve License 32

Resilience 18

RFC2833 27, 32

RFC5373 32

S

Scope

- Activate 50
- Create 49

Security 52

Server

- DHCP 12
- File 13, 38
- Provisioning 13

Settings

- Auto-generation 14
- Editing the settings file 18

Silence Suppression 32

SIP 25

- Domain Name 25
- FQDN 25
- Registrar 25

SSON 30, 49, 50

- Change 69

Static addressing 68

System Default

- Codecs 27

System Monitor 62

T

TCP

- Port 25

TLS

- Port 25

U

UDP

- Port 25

Upload files 41

User

- Auto-creation 34
- Extension 31
- Login Code 31

Name 31

V

VCM 12

View 62

Voice Compression 12

VoIP 11

