IP Office™ Platform 10.0

SIP Telephone Installation Notes

- Issue 01c - (07 December 2016)

© 2016 AVAYA All Rights Reserved.

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 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, 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.

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.

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 Licensing 9
1.2 Network Assessment 10
1.3 Voice Compression Channels 11
1.4 Telephone Power Supply 11
1.5 DHCP Server Requirements 11
1.6 File (Provisioning) Server Requirements 12
1.7 File Auto-Generation 12
1.8 Config File Editing 13
1.9 Remote Workers 14
1.10 Resilience 14
1.11 Phone Operation Notes 14
1.12 Centralized Branch Extensions 14
1.13 Additional Documentation 15

2. Generic Installation Process

2.1 Enabling SIP Extension Support 19
2.2 System Default Codecs 21
2.3 DHCP Settings 22
2.3.1 System DHCP Support 23
2.3.2 System Site Specific Option Numbers 24
2.4 SIP User Settings 25
2.5 SIP Extension Settings 26
2.6 Allowing Extension/User Auto Creation 29
2.7 Attaching the Phones 30

3. File (Provisioning) Server Settings

3.1 System File Server Settings 33
3.2 Loading Files onto the System 34
3.2.1 Manually Copying Files 34
3.2.2 Using Manager to Upload Files 35
3.2.3 Using Web Manager to Upload Files 36
3.3 Loading Files onto a 3rd-Party Server 36

4. Alternate DHCP Server Setup

4.1 Checking for DHCP Server Support 38
4.2 Creating a Scope 39
4.3 Adding an Option 40
4.4 Activating the Scope 40

5. Security Certificates

5.1 Using the IP Office Certificate 42
5.1.1 Downloading the Linux Certificate 43
5.1.2 Downloading the IP500 V2 Certificate 44
5.2 IP Office Certification 45
5.2.1 Adding a Root CA Certificate to the IP Office TC 45
5.2.2 Create an Identity Certificate for the IP Office 46
5.2.3 Add the Identity Certificate to the IP Office 47
5.3 File Server Certification 48
5.3.1 Add the Certificates Snap-In 48
5.3.2 Add the Trusted Root CA Certificate to the Windows Certificate Store 48
5.3.3 Create an Identity Certificate for the File Server 49
5.3.4 Add the Identity Certificate to the File Server 50

6. Monitoring SIP Phones

6.1 Viewing SIP Phone Communications 52
6.2 Viewing Registrations 52
6.3 Registration Blacklisting 52

7. Avaya SIP Phone Installation Notes

7.1 1100/1200 Series 54
7.2 B100 Series (B179) 54
7.3 D100 Series (D160) 54
7.4 E100 Series (E129, E159, E169) 55
7.4.1 E129 55
7.4.2 E159, E169 62
7.5 H100 Series (H715) 62
7.6 J100 Series (J129) 63
7.6.1 Restrictions/Limitations 63
7.6.2 Known Problems 64
7.6.3 Files 64
7.6.4 Simple Installation 65
7.6.5 Static IP Address Configuration 65
7.6.6 SIP Settings Configuration 66
7.6.7 Changing the Phone SSON 66
7.6.8 Viewing the Phone Settings 66
7.6.9 Factory Reset 66

8. 3rd-Party Installation Examples

8.1 General Notes 69
8.2 AAstra 9133i SIP 70
8.3 Avaya A10 ATA 72
8.4 CounterPath eyeBeam/X-Lite 76
8.5 Grandstream 79
8.6 Innovaphone IP22, IP24, IP28 81
8.7 Nokia S60 v3 SIP Client 84
8.8 Patton Micro ATA 85
8.9 Polycom SoundPoint Phones 86

9. Document History

Index 89

Comments on this document? infodev@avaya.com

Chapter 1.
IP Office SIP Telephones

1. IP Office SIP Telephones

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

This document covers the general installation of SIP telephones with IP Office 10.0 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 begins with a generic installation process 18 which is suitable for most types of SIP telephone. Additional notes 54 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 15).

Supported Avaya SIP Telephones

The following Avaya SIP telephones are supported on IP Office Release 10.0 systems.

- **1000 Series:** 1010, 1040.
- **1100 Series** 54**:** 1120E, 1140E.
- **1200 Series** 54**:** 1220, 1230.
- **B100 Series** 54**:** B179.
- **D100 Series** 54**:** 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** 60**:** A simple SIP desk phone.
- **E159, E169** 62**:** SIP telephones that supports the docking of mobile devices.
- **H175** 62**:** SIP video telephone.
- **J129** 63**:** A simple SIP desk phone. Supported from IP Office Release 10.0 SP2.

When used as a branch system in a centralized Avaya Aura network 14, 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 15 issued by the Avaya Solution & Interoperability Test Lab.

1.1 Licensing

The type of license required for SIP telephones depend on whether the telephone is an Avaya SIP device or a 3rd-party SIP telephone. The former use **Avaya IP Endpoint** licenses, the later use **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.

1.2 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.

1.3 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 are 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.

1.4 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.

1.5 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** 22
  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** 38
  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.

1.6 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. 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 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 32. If using a third-party DHCP server, the file server address is set through the addition DHCP options.

1.7 File Auto-Generation

Avaya IP phones (SIP and H.323) request a number of files from the file server when the phone is restarted (phone configuration and firmware files).

When using the IP Office system as the file server, in response to a file request from a phone, the system auto-generates the necessary files if the actual file is not present in the memory. This feature is used for most of the file types except for actual firmware files.

If the appropriate file is uploaded to the system 34, then auto-generation of that particular file is overridden.

Testing 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>/J100Supgrade.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.

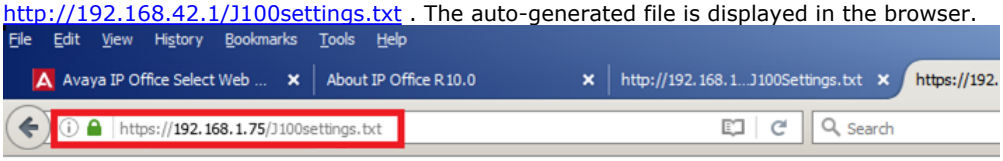
1.8 Config File Editing

Most Avaya IP phones download a settings file when restarted, This file contains a range of settings. This manual does not detail the set of individual settings.

- **Note:** It is strongly recommended where possible that you use the IP Office as the file server and also that you let it auto-generate the settings files for phones rather than using uploaded file. This helps as the sit automatically adjust the settings provided to phones to match changes made in the IP Office 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/J100settings.txt . The auto-generated file is displayed in the browser.




```
SET PHNDPLENGTH 7
SET PHNIC 011
SET PHNLD 1
SET PHNLDLENGTH 10
SET PHNOL ""
SET QKLOGINSTAT 1
SET VLANTEST 60
SET HTTPPORT 80
SET SIPDOMAIN 192.168.1.75
SET MWISRVR "192.168.1.75"

SET SIP_CONTROLLER_LIST 192.168.1.75:5061;transport=tls,192.168.1.56:5061;transport=tls

SET AUTH 1
SET ENFORCE_SIPS_URI 0
SET ENCRYPT_SRTCP 0
SET ENABLE_G711A 1
SET ENABLE_G711U 1
SET ENABLE_G729 1
```

   - **H175:** *H1xxsettings.txt*
   - **J129:** *J100settings.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 15.
4. When completed, upload the file to the file server being used by the telephones.
5. Restart the phone or phones in order for them to reload their files including downloading the edited settings file.

1.9 Remote Workers

For configuring the J129 for remote worker, there is no need for editing the auto generated settings files. First the phones should be provisioned locally in order to test operation and to obtain the proper root certificates. After this, when the phone is moved to remote location, the HTTP Server need to be configured with the public address route to the IP Office.

1.10 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 15.

1.11 Phone Operation Notes

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

- **IP Office Hot Desking *(Log In/Log Out)***
  SIP phone can use the IP Office user hot desking features, for example the *35 and *36 default short codes. However, when a different user is logged in using those functions, the user information stored on the phone (personal directory, call log, etc) is not changed. Additionally the phone continues to display the details of the user account used to register the phone with the system.
- **Account Code/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 #.
- **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.
- 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. However, for 3rd-party SIP phones, if supported by the phone the method used to signal an auto-answer call needs to be configured separately for each extension in the IP Office configuration.

1.12 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.

1.13 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	• *IP Office 1100/1200 Series Phone Installation*
1200 Series	1220, 1230	
B100 Series	B179	• *Installing and Administering the IP Office B179 SIP Conference Phone*
D100 Series	D160	• *Installing and Administering IP Office D100 SIP Wireless Terminal*
E100 Series	E129	• *Installing and Maintaining Avaya E129 SIP Deskphone* • *Administering Avaya E129 SIP Deskphone*
	E159, E169	• *Installing and Maintaining the Avaya E149 and E169 IP Media Stations*
H100 Series	H175	• *Installing and Maintaining Avaya H100-Series Video Collaboration Stations* • *Administering Avaya H100-Series Video Collaboration Stations*
J100 Series	J129	• *Installing and Administering J100 Series IP Deskphones SIP*
General		• *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.gsp).

Brand	Model
Algo	8028 SIP Door Phone 8036 SIP Multimedia Intercom 8128 SIP Strobe Light 8180 SIP Audio Alerter 8188 SIP Ceiling Speaker 8301 SIP Paging Adapter 3226 Trunk Port FXO Doorphone
Ascom	i62 VoWiFi handset i75 VoWiFi Handset Myco Wireless Smartphones
Interquartz	Endurance 10CS
Cetis	3300IP Series SIP Telephones 9600IP Series SIP Telephones
G-Tek	AQ-10x ASP-8210-SMK ASP-6210-S AAX-4100

Brand	Model
Grandstream	GXV3240 GXV3275
LiveSentinel	SIP Video Door Intercom
Polycom	SoundStation Duo
QSC	Q-Sys SIP Softphone
Revolabs	FLX UC 1000
Valcom	One-Way IP Speakers PagePro IP
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
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 38.
- **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 32.
- **TLS Certificate**
  If TLS is enabled, the IP Office system's own default identity certificate is used. For additional options see Server Certification 42.

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 9 to support both the SIP telephone extensions (Avaya and third-party) and the extension users.
2. **Enable SIP extension support** 19.
3. **Adjust the system Codecs** 21 *(Optional)*.
4. **Check the system DHCP settings** 22.
5. **Add SIP Users to the configuration** 25.
6. **Add SIP Extensions to the configuration** 26.
7. **Attach the phones** 30.

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 9 to support both the SIP telephone extensions (Avaya and third-party) and the extension users.
2. **Enable SIP extension support** 19.
3. **Adjust the system Codecs** 21 *(Optional)*.
4. **Check the system DHCP settings** 22.
5. **Enable Auto-Create Extn/User** 29.
6. **Attach the phones** 30.
7. **Modify the IP Office user and extension settings** 25.
8. **Disable Auto-Create Extn/User** 29.

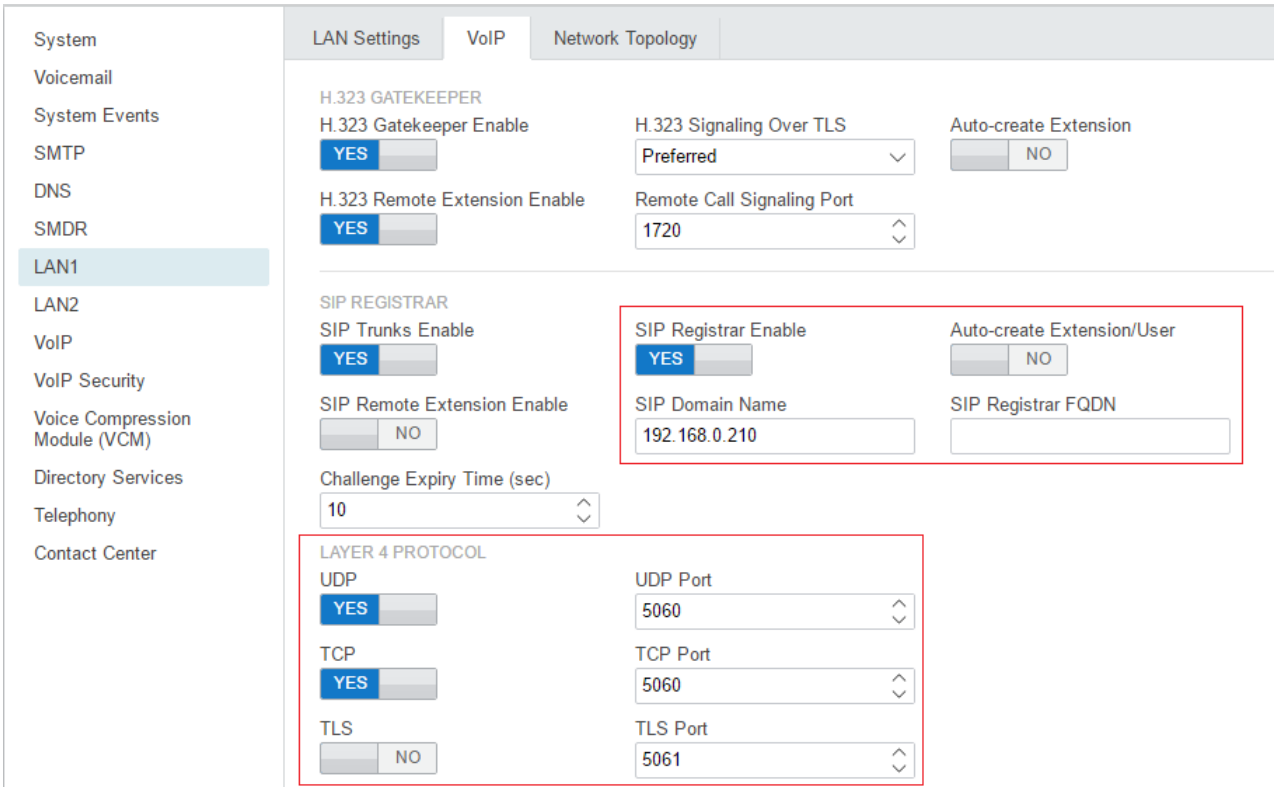
2.1 Enabling SIP Extension Support

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.



- **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.
- **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 devices.
- **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 devices in order to register with the IP Office. If you are using TLS, this value needs to included in the security certificates 42 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 extension devices.
    - **! 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 42 has been complete.
- **Challenge Expiry Time (sec):** *Default = 10*
  The challenge expiry time is used during SIP extension registration. When a device 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 devices 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***.

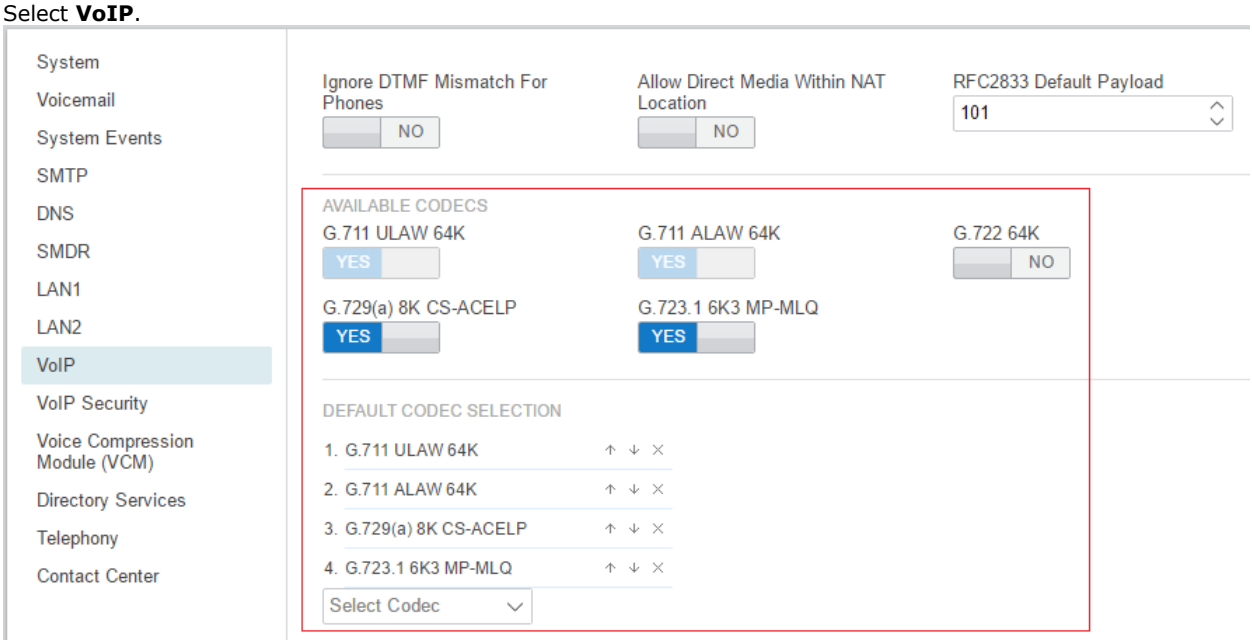
For most installations these settings do not need to be changed, however it is important to understand how the options are set and used by the system.

Similarly, 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.

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.

3. 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.
4. 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 38.
- 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

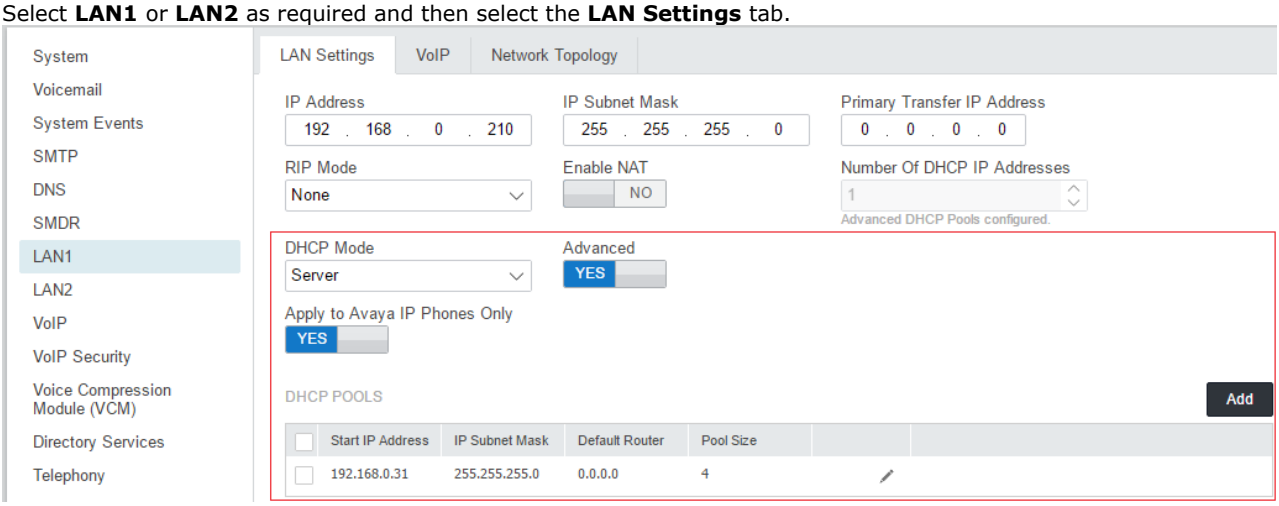
The following are the main steps for enabling the IP Office system to support DHCP operation for IP phones.

1. **Enable DHCP and Set the Number of Addresses** 23
2. **Check the Site Specific Option Numbers** 24
   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** 32
   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.



- **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.

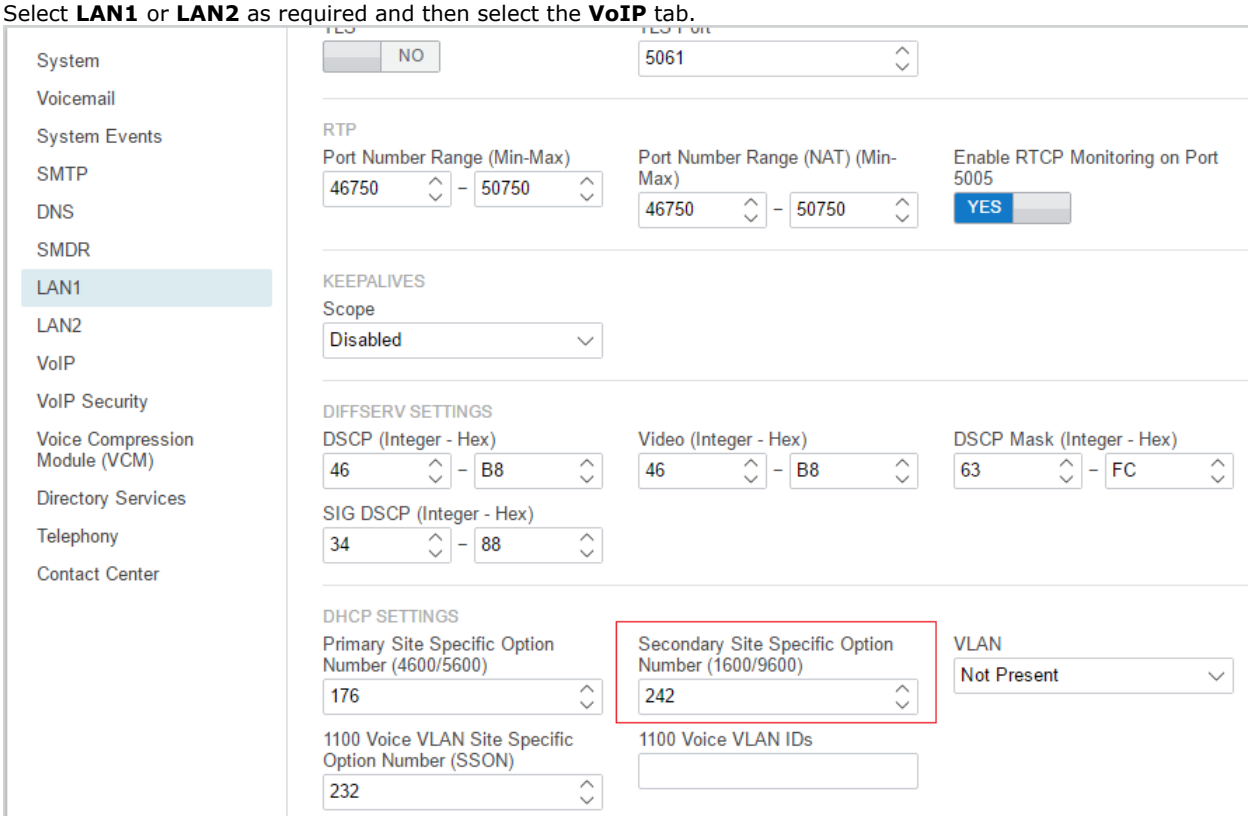
2.3.2 System Site Specific Option Numbers

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.



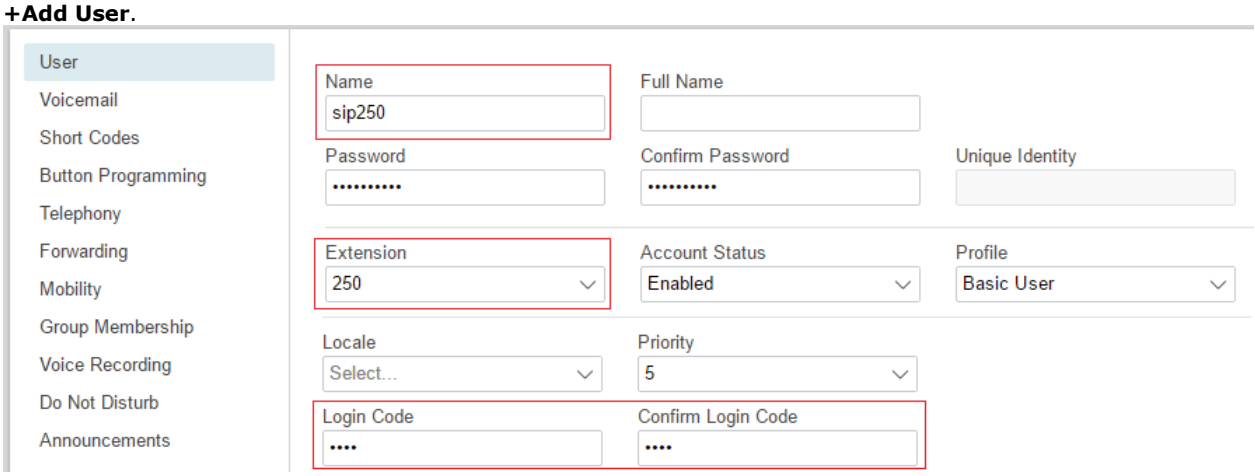
4. Check that the site specific option number settings match those required for the phones being supported. The default for most Avaya SIP phones is 242.
5. If this setting needs to be changed, save the configuration back to the system.

2.4 SIP User Settings

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

To configure a basic SIP user:

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **User** or **Call Management | User**. Select the user to edit or to create a new user, select | **User**. or **+Add User**.



3. The key settings used for SIP telephone registration are:

   - **Name**
     If the SIP extension is set to **Force Authorization** (the default), this field is used as the ***Authorization Name*** that must be set in the SIP device's configuration.
   - **Extension**
     This should match the SIP ID of the SIP device and the **Base Extension** setting of the SIP extension 26 in the IP Office configuration.
   - **Login Code**
     If the SIP extension is set to **Force Authorization** (the default), this field is used as the ***Authorization Password*** that must be set in the SIP device's configuration. If using IP Office Manager, this setting is on the **User | Telephony | Supervisor** settings tab.

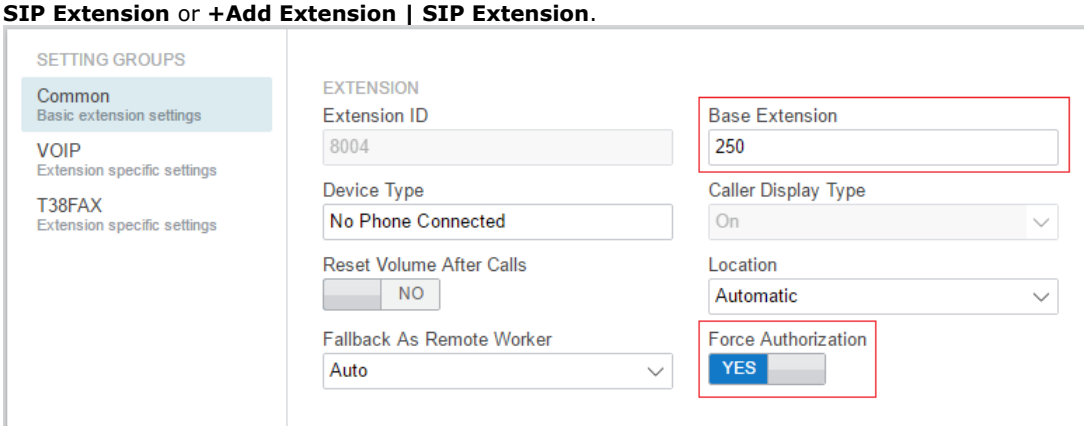
4. If creating a new user, after clicking **OK** or **Create**, you are prompted whether to also automatically create a new extension. If so, select **SIP Extension**.

2.5 SIP Extension Settings

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

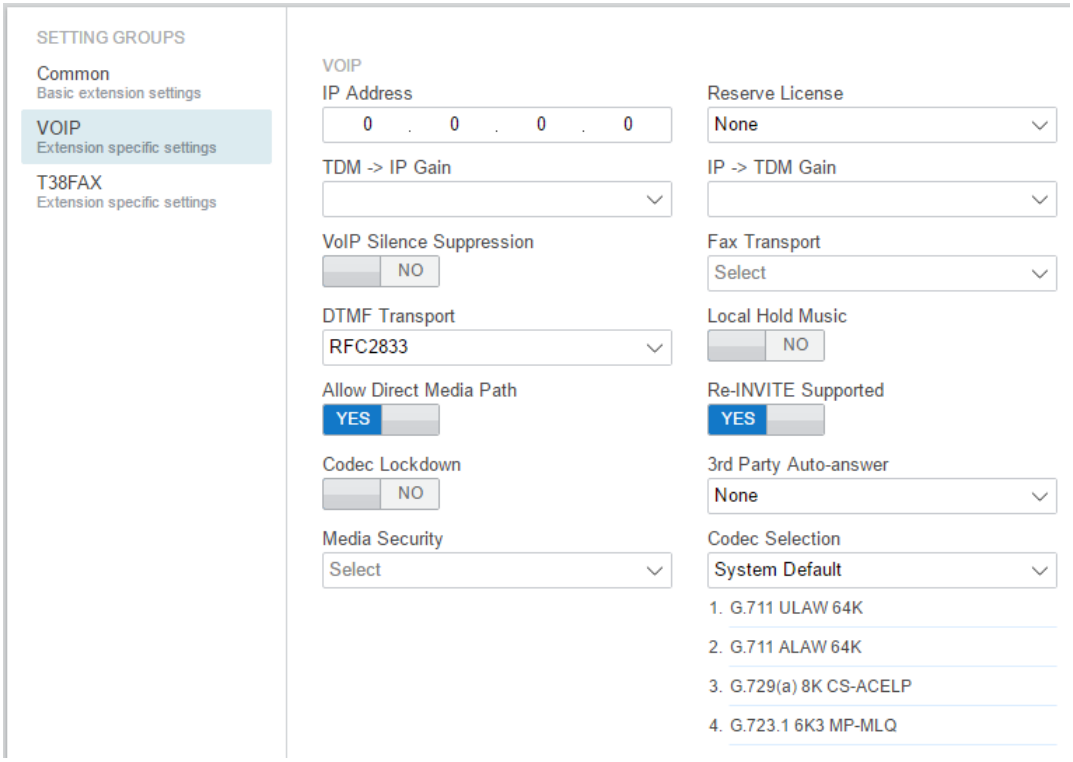
To configure a SIP extension:

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **User** or **Call Management | Extensions**. Select the extension to edit or to create a new user, select | **SIP Extension** or **+Add Extension | SIP Extension**.



- **Base Extension**
  This should match the **Extension** setting of the SIP user added to the IP Office configuration.
- **Force Authorization:** *Default = On*
  If enabled, SIP devices are required to register with the system using the **Name** and **Login Code** configured for the user within the system configuration.

3. 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 a device with that address.
- **Codec Selection**
  If the **Codec Selection** is left set to ***System Default***, the extension will use the system codec preferences 21. 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:**
  Each non-Avaya IP phones requires an **3rd Party IP Endpoint** license. Normally the available licenses are issued in the order that devices register. This option allows an extension to be pre-licensed before the device has registered by selecting the option **Reserve 3rd party IP endpoint licence**. 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 device. 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 devices 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 support auto answer using an RFC 5373 header added to the call invitation message.

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

  - **device auto answers**
    The IP Office system relies on the extension device auto answering calls.

- **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.

- **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.

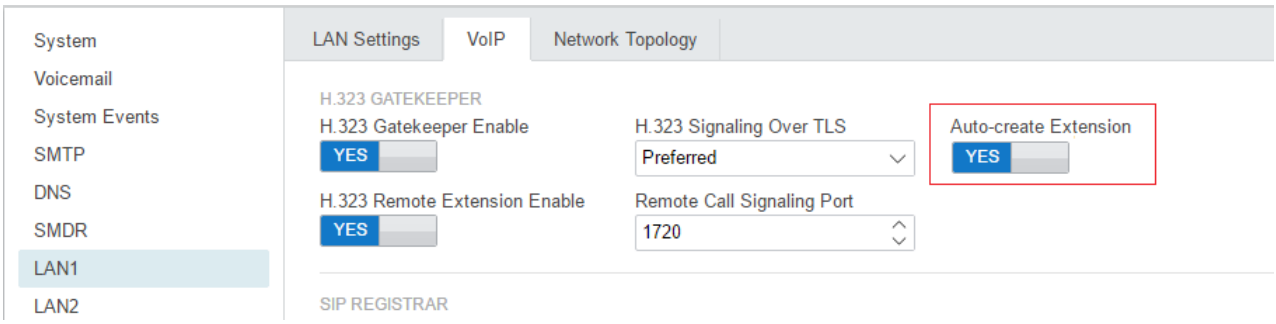
2.6 Allowing Extension/User Auto Creation

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

- **! 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.
- **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.



4. Change the **Auto-create Extn/User** settings to the state required.
5. 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 SSON 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 it.
    b. Using the upgrade file, it compares the details of the firmware it is already running and that which the firmware 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 IP Office user's **Login Code**.

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:

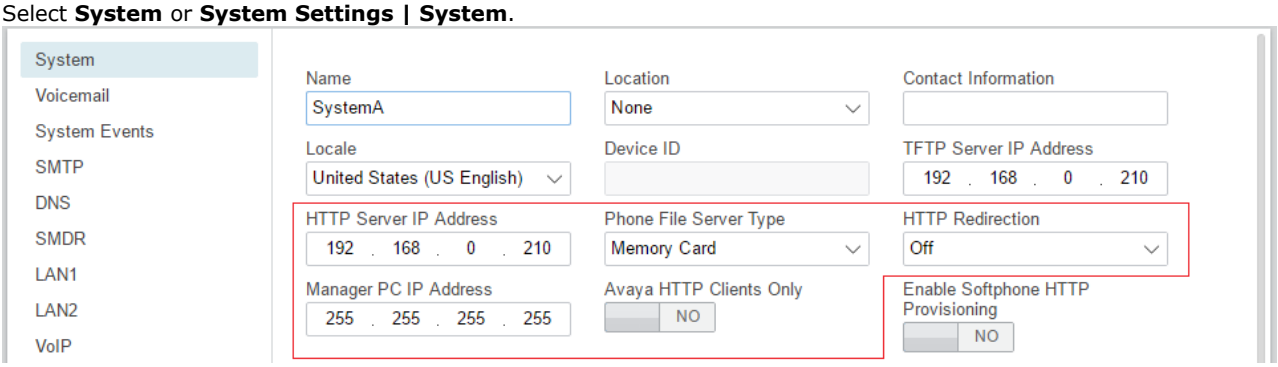
- For IP500 V2 systems, the IP Office system's own memory card can be used as the source for the files.
- For IP Office Server Edition systems, the system's own disk can be used as the source for the files used by the phones.
- When using either of the above, file auto-generation 12 is supported for settings and upgraded text files for supported Avaya SIP phones.
- If either of the options above are not acceptable, a 3rd party HTTP file server is required. The necessary phone firmware files then need to be loaded onto that server.

3.1 System File Server Settings

If the IP Office system is being used for DHCP support [22] 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:

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. 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 files 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***. The 0.0.0.0 default means no HTTP request.
   - **HTTP Redirection** *(Default = Off)*
     Supported for 96x1 H.323 and H175 SIP 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.
   - **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 [12] 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.

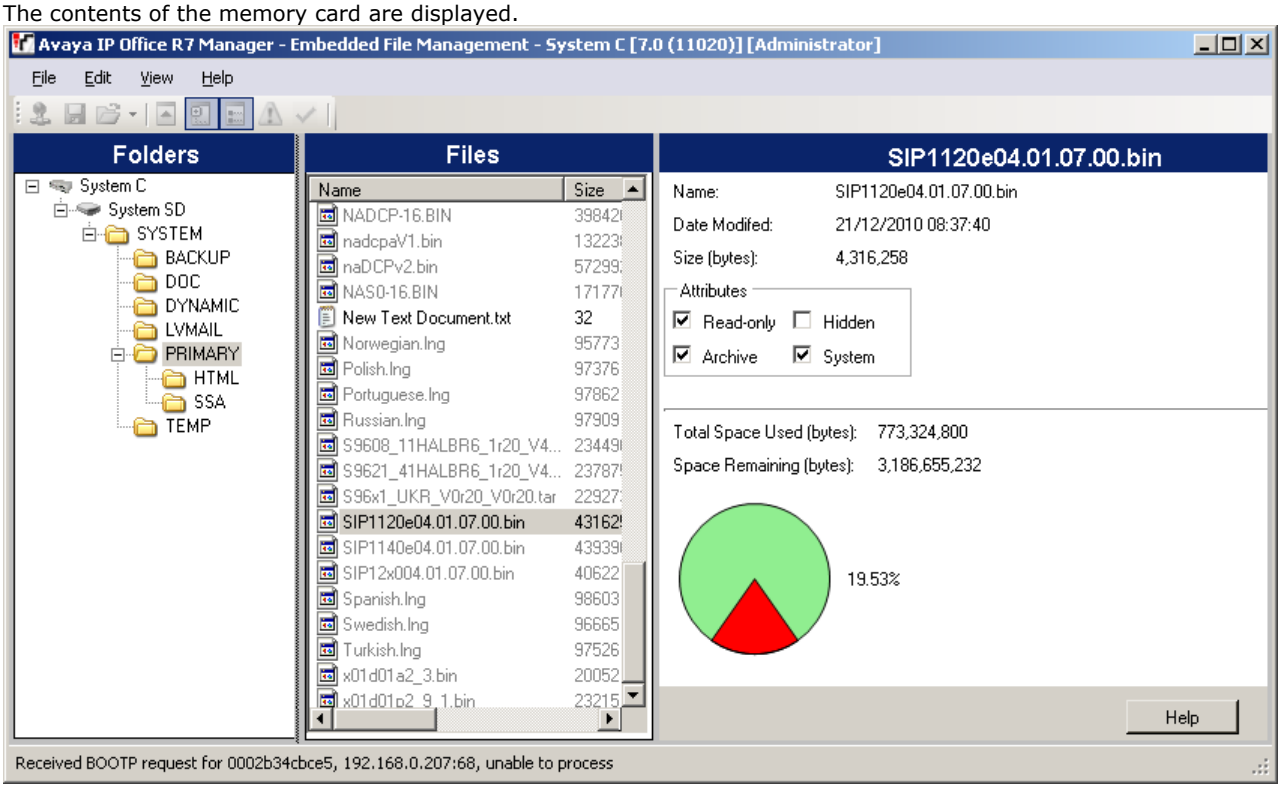
- **! WARNING**
  A memory card should never be removed from a running system without first being shutdown.IP Office Manager should be used to shutdown the memory card before it is removed from the system.

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 **Server 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.

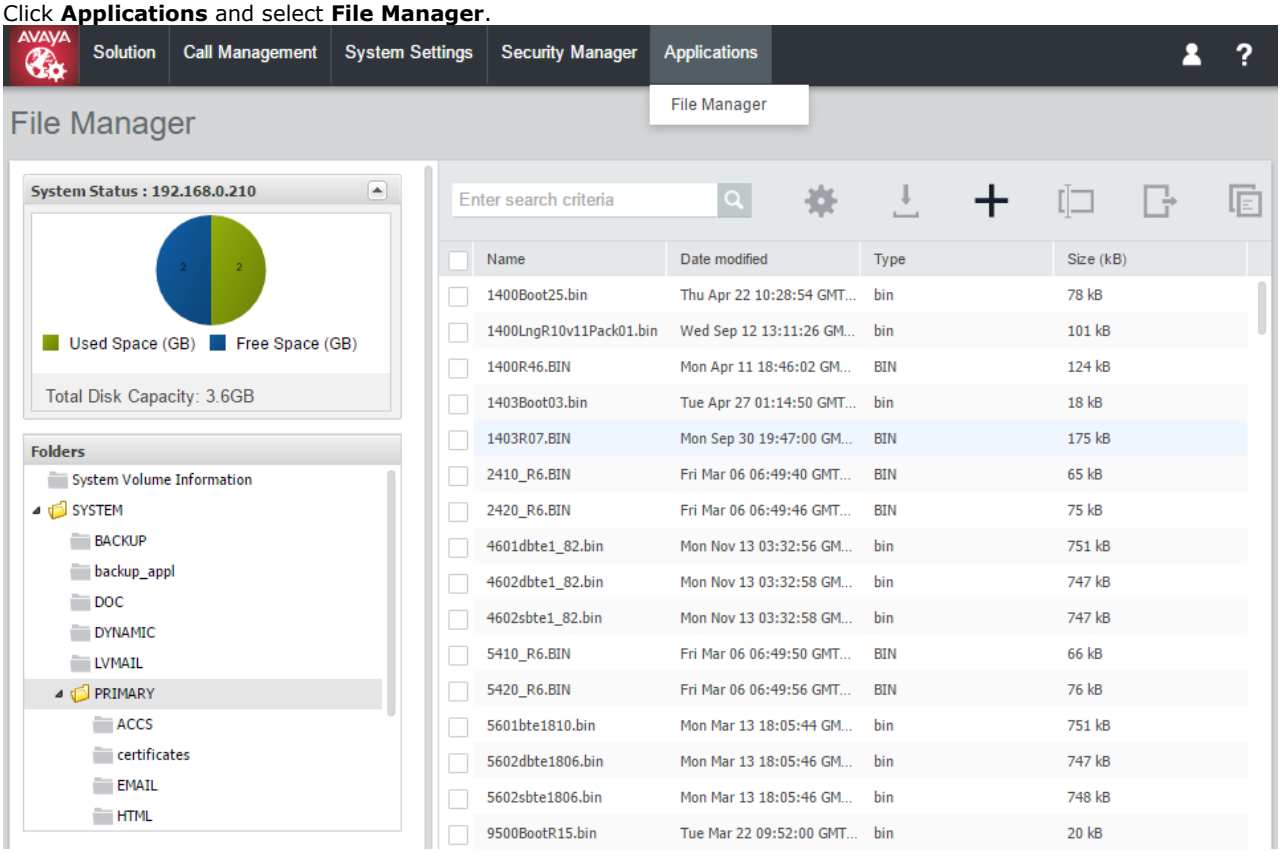


5. For an IP500 V2, use the folder tree to navigate to ***System SD*** **|** ***SYSTEM*** **|** ***PRIMARY***. For a IP Office Server Edition system, use the folder tree to navigate to ***system*** **|** ***primary***.
6. Individual files can be copied onto the card by using drag and drop or by selecting **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**.



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.

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 39 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 40 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=xxxx, 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.
   - ***TLSSRVR=*** 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 15.
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 40.

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 45.
- **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:

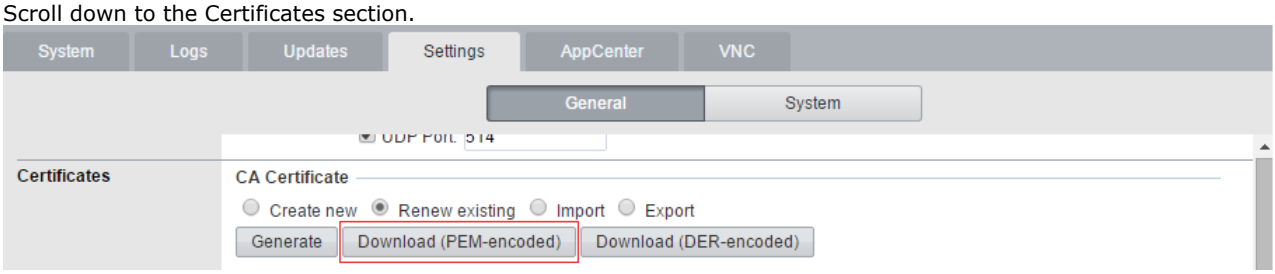
- **Downloading the IP Office certificate from an IP500 V2** 44
- **Downloading the IP Office certificate from a Linux based IP Office** 43

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 36 being used by the phones. .

5.1.2 Downloading the IP500 V2 Certificate

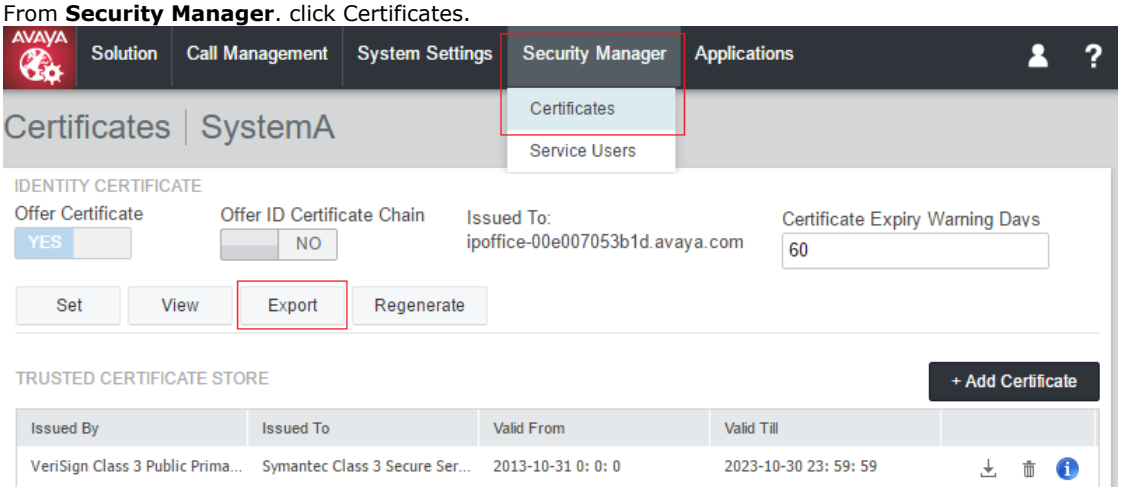
Use the following process to download the system's current identity certificate. The certificate file can then be renamed and uploaded to the file server being used by the IP Phones.

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 36 being used by the phones.

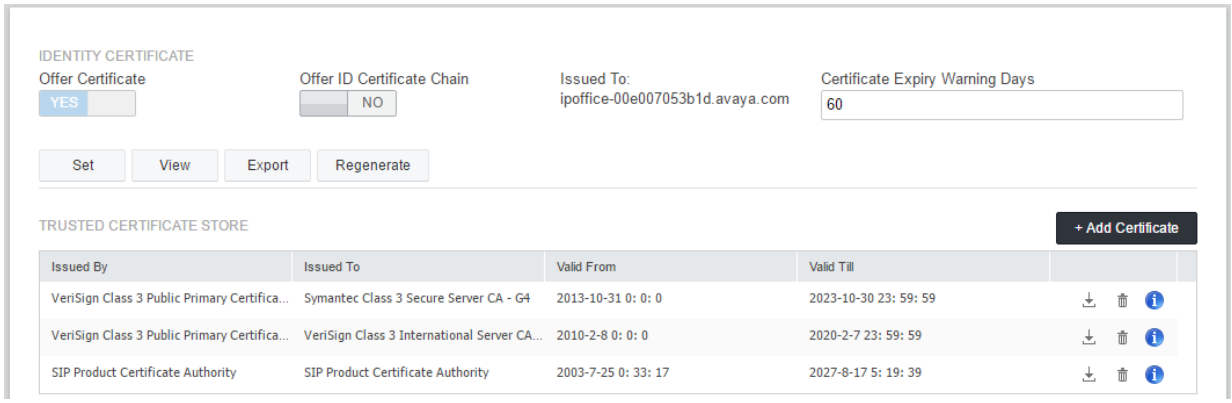
5.2 IP Office Certification

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:

1. 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 42.
   - **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.
2. 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.
   a. **IP Office Manager:** Access the system's security settings. Click **System** and select the **Certificates** tab.
   b. **IP Office Web Manager:** Click Security Manager and select Certificates.



   c. Click **Add** or **+Add Certificate** and select the root CA certificate.
3. 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.

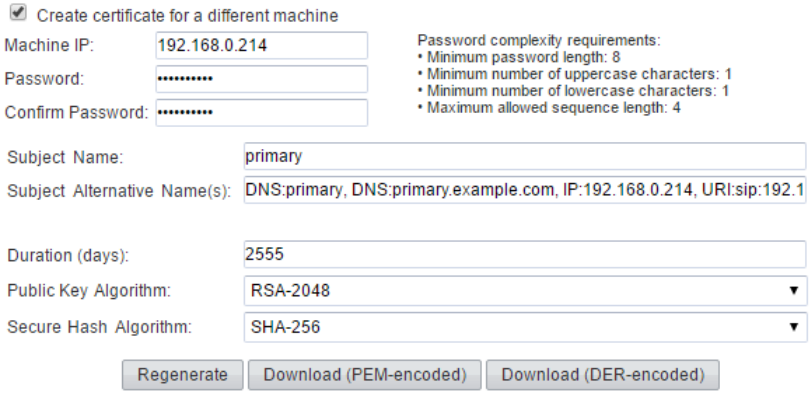
1. Using one of the methods for loading files onto the system 34, add the certificate to the ***/SYSTEM/PRIMARY/certificates/TCS/ADD*** folder.

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**.



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 **Generate** button.
6. Click on **Download (PEM-encoded)** to download the file.

5.2.3 Add the Identity Certificate to the IP Office

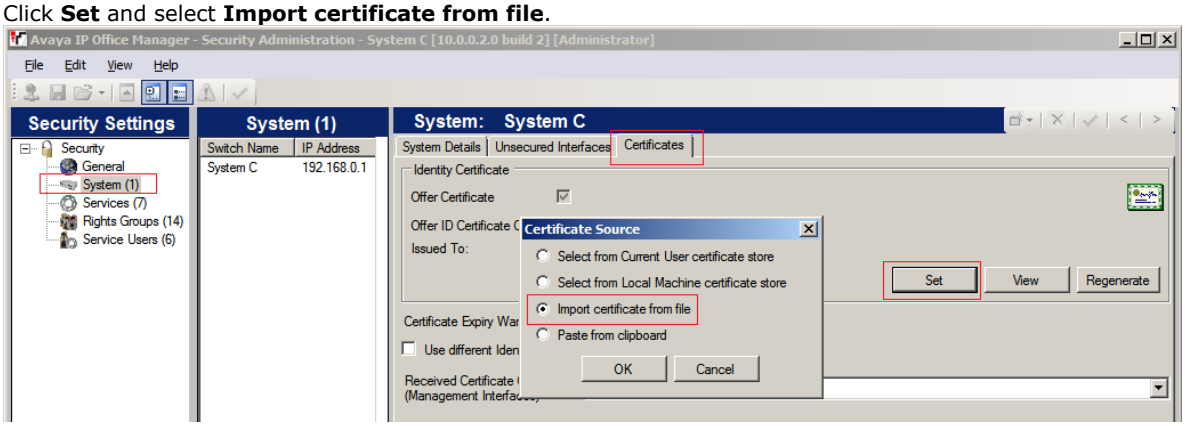
To add the identity certificate to the IP Office:

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

- **IP Office Manager:**

  a. Access the system's security settings. Click **System** and select the **Certificates** tab.

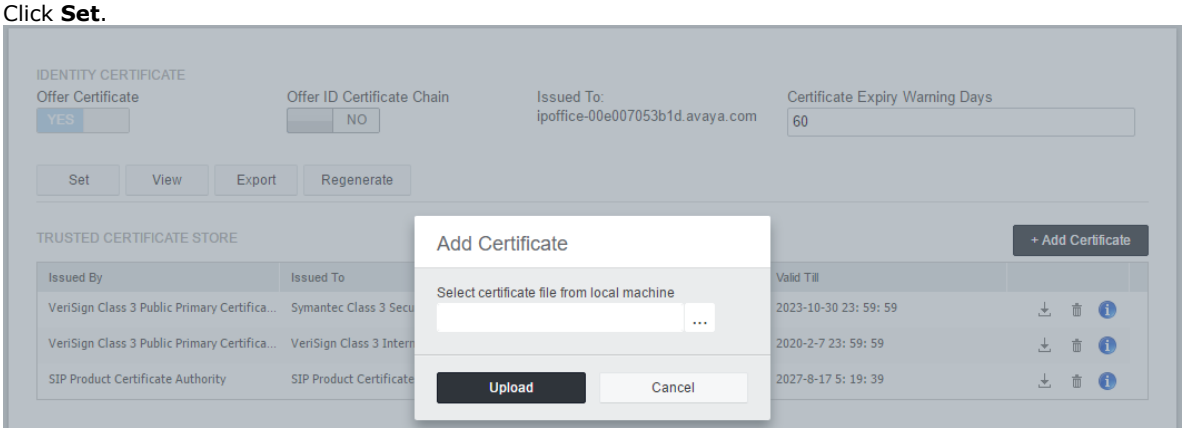
  b. Click **Set** and select **Import certificate from file**.



- **IP Office Web Manager:**

  a. Click **Security Manager** and select **Certificates**.

  b. Click **Set**.



2. Select the previously generated IP Office identity file 46 and load it.

3. 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 45 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).

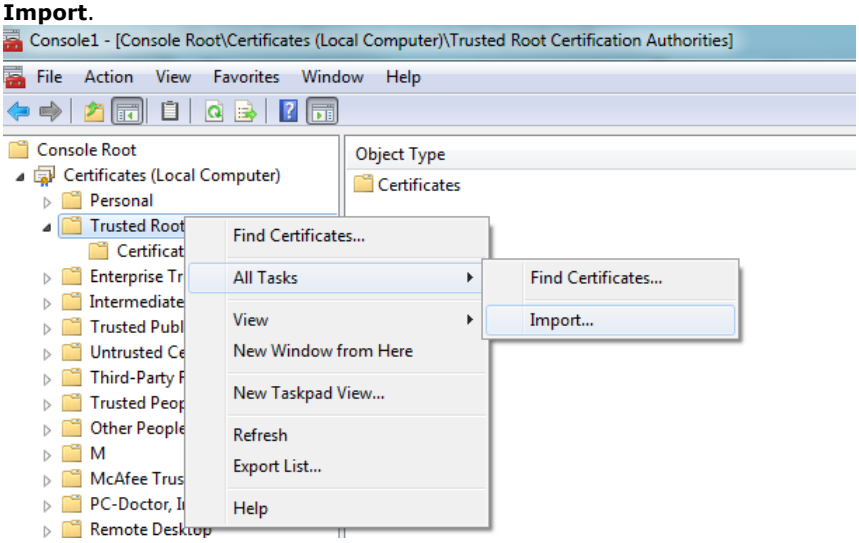
To enable the Certificates Snap-In:

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. You can now use the

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

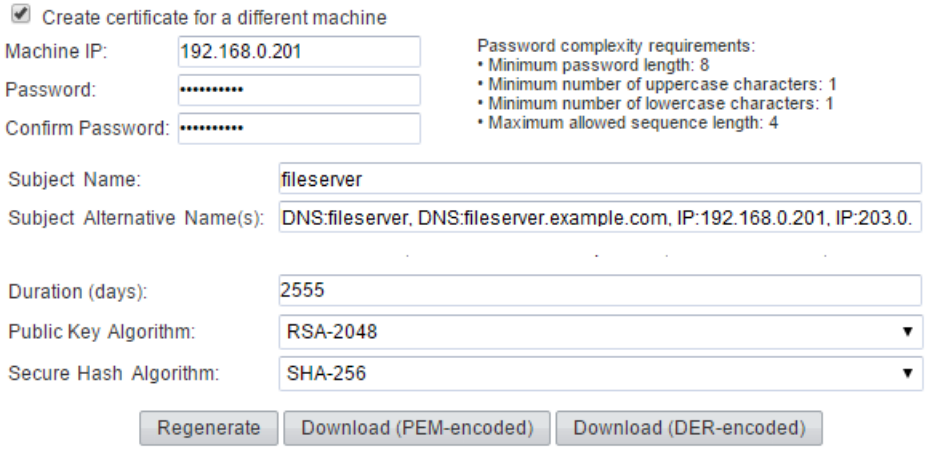
When the phone sends an HTTP request to the IP Office, it receives a 307 redirect message pointing to the HTTP server and resends the request to that server. But to open an HTTPS connection to the server, it needs to validate the server's identity by verifying the IIS server's identity certificate against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



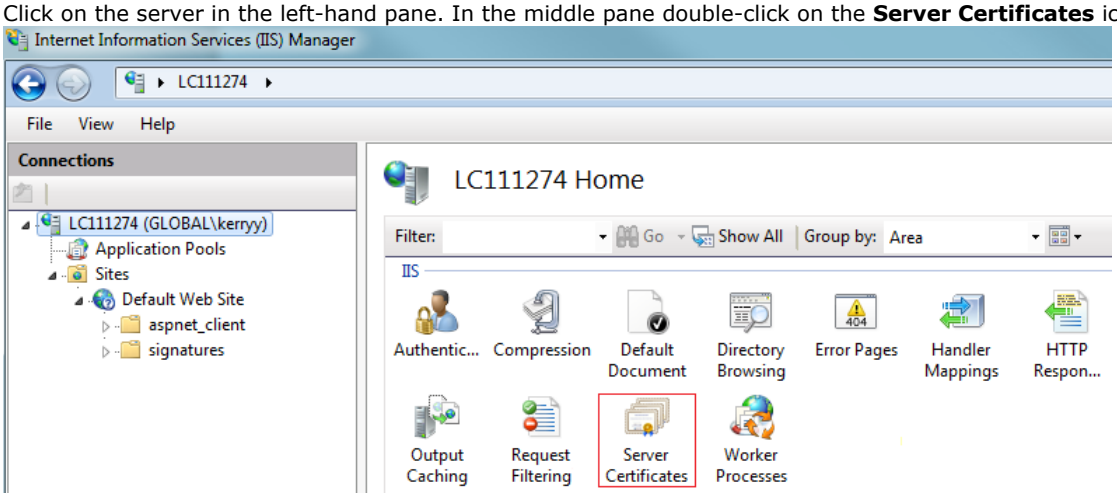
5. In the fields below that, enter the details for that PC. In this example, the computer hosting the IIS server has a single FQDN and numerous IP addresses. This information is all added to the Subject Alternative Names field: ***DNS: fileserver.example.com,IP:192.168.0.201, IP:203.0.100.30***
6. Click on the lower **Generate** button.
7. Click on **Download (PEM-encoded)** to download the file.
8. The identity certificate can now be added to the web server 48.

5.3.4 Add the Identity Certificate to the File Server

The identity certificate generated for the server 49 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.

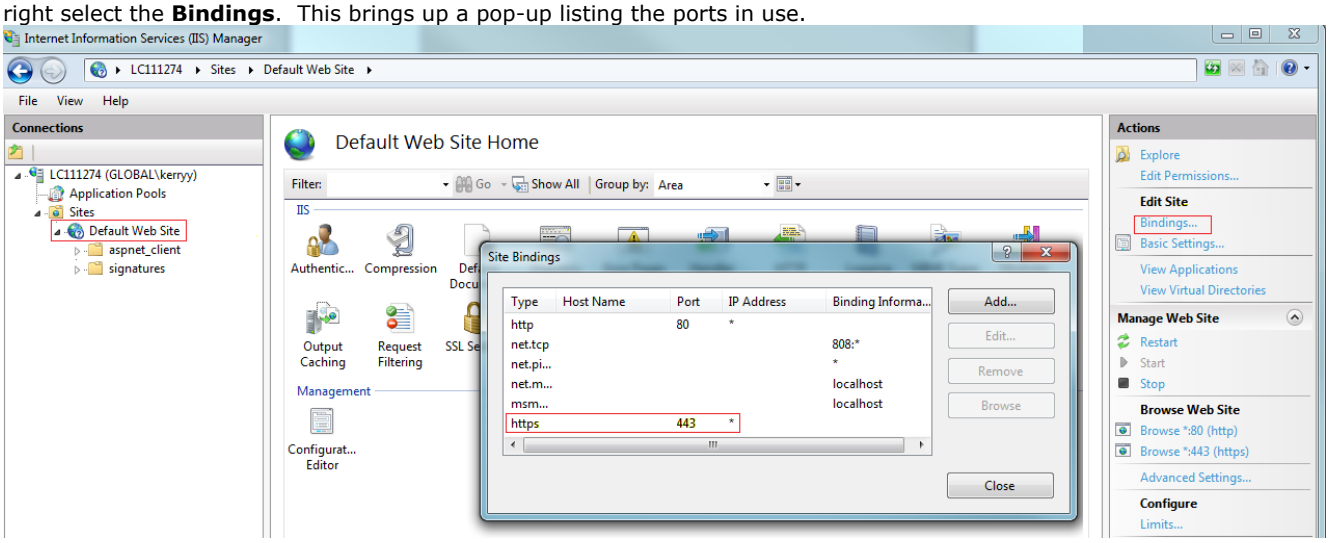


   a. On the far right of the window that appears click on **Import...**.

   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 46.

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

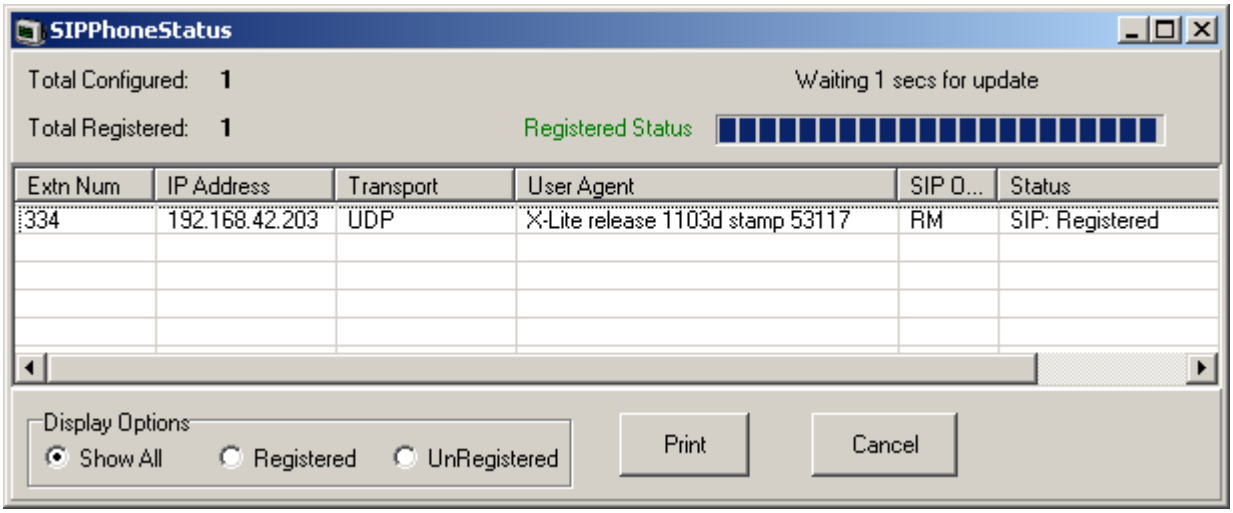
The System Monitor trace can be set to include SIP registration traffic, DHCP requests and HTTP file transfers.

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.



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**.

Chapter 7.

Avaya SIP Phone Installation Notes

7. Avaya SIP Phone Installation Notes

This section provides notes for specific Avaya SIP phones where their installation differs from the generic installation process 18. The sections may also detail differences in operation when registered with an IP Office system rather than other Avaya systems.

Specific installation processes are included for the following phones:

- **B179** 54
- **E129** 55
- **J129** 63

7.1 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 15.

7.2 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 15.

To set the conference codes:

The B100 Series phones needs 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 .

7.3 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. There 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 15.

7.4 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 15.

7.4.1 E129

Following configuration of the system to support SIP extension 19, 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** 55	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** 56	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** 57	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** 58	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** 59	Use this method if there is no DHCP server on the network and no browser access to the network.

7.4.1.1 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 25 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.

7.4.1.2 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 25 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.

7.4.1.3 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 25 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.

7.4.1.4 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 25 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.

7.4.1.5 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 25 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 57 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 57 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.

7.4.1.6 Troubleshooting Telephone Connection

Username Keeps Reappearing

If the **Username** option keeps appearing after entering the user details, that indicates that the 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 19 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 9 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 57 connection process.
5. If not using DHCP, user Static IP Method 1 58 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 58 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.

7.4.1.7 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.

7.4.1.8 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**.

7.4.1.9 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 **CONF**IG and **FACTORY FUNCTIONS** menus on the phone are not accessible.
4. Click **Save and Apply**.

7.4.1.10 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.

7.4.2 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.

7.5 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 15.

7.6 J100 Series (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 15.

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

- **J129 File Availability for SP2**
  Support for J129 phones is included in IP Office Release 10.0 SP2. However, the necessary files will not be included as part of the system software, apart from auto-generation of the settings file, until SP3. For SP2, the appropriate J129 firmware set needs to be obtained from the IP Office downloads section of the Avaya support (support.avaya.com) website and then be manually uploaded to the system 34. If using the IP Office as the file server, only the ***J100Supgrade.txt*** file, .BIN file and .XML language files need to be uploaded. Note that the ***J100Supgrade.txt*** files needs to be edited to refer to the ***J100settings.txt*** file rather than ***46xxsettings.txt***.

7.6.1 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**.

7.6.2 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 66 on the phone.

- **Changing IP Office Systems**
  To switch a phone between different IP Office systems requires a factory reset 66 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 66. 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 66 on the phone. This is needed since IP Office initially configures the phone to use HTTPS when TLS is configured.

7.6.3 Files

During a restart, J100 Series telephones requests a series of files, using HTTPS or HTTP, from the configured file server 32.

- **J129 File Availability for SP2**
  Support for J129 phones is included in IP Office Release 10.0 SP2. However, the necessary files will not be included as part of the system software, apart from auto-generation of the settings file, until SP3. For SP2, the appropriate J129 firmware set needs to be obtained from the IP Office downloads section of the Avaya support (support.avaya.com) website and then be manually uploaded to the system 34. If using the IP Office as the file server, only the ***J100Supgrade.txt*** file, .BIN file and .XML language files need to be uploaded. Note that the ***J100Supgrade.txt*** files needs to be edited to refer to the ***J100settings.txt*** file rather than ***46xxsettings.txt***.

The various files, in the order that the phone requests them, are:

- ***J100Supgrade.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 12 if not physically present.
  - * **Note:** The upgrade file provided for SP2 finishes with a line instructing the phone to request a ***46xxsettings.txt*** file. If using this file, edit this line to be a request for the ***J100settings.txt*** file.

- ***J100settings.txt***
  Details the phone settings including the SIP server settings. If using the IP Office system as the file server, the file is auto-generated 12 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 12 from the system settings if no file is physically present.

7.6.4 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. Edit the J100Supgrade.txt file to change the 46XXsettings.txt setting to J100settings.txt.
    d. Upload the files to the system's primary folder 34.
2. Enable SIP extension support on the system 19.
3. Create the SIP users 25 and SIP extensions 26.
4. Attach and register the phones 30.

7.6.5 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.

7.6.6 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 12, 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 13 to specify the SIP server settings.

7.6.7 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**.

7.6.8 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.

7.6.9 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**.

Chapter 8.

3rd-Party Installation Examples

8. 3rd-Party Installation Examples

This section gives examples of the installation settings used with a variety of SIP devices tested with IP Office. These are only the basic details for registration with an IP Office system. Full installation and configuration, for example assigning device IP addresses, is covered in the device or software manufacturer's own documentation.

The devices covered here are:

- **Astra 9133i** 70
- **Avaya A10 ATA** 72
- **CounterPath Eyebeam/X-Lite Softphones** 76
- **Grandstream GXP 2000, GXP 2020** 79
- **Innovaphone IP22, IP24, IP28** 81
- **Nokia S60 v3 SIP Client** 84
- **Patton Micro ATA** 85
- **Polycom Soundpoint** 86

Additional Documentation

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
Algo	8028 SIP Door Phone 8036 SIP Multimedia Intercom 8128 SIP Strobe Light 8180 SIP Audio Alerter 8188 SIP Ceiling Speaker 8301 SIP Paging Adapter 3226 Trunk Port FXO Doorphone
Ascom	i62 VoWiFi handset i75 VoWiFi Handset Myco Wireless Smartphones
Interquartz	Endurance 10CS
Cetis	3300IP Series SIP Telephones 9600IP Series SIP Telephones
G-Tek	AQ-10x ASP-8210-SMK ASP-6210-S AAX-4100

Brand	Model
Grandstream	GXV3240 GXV3275
LiveSentinel	SIP Video Door Intercom
Polycom	SoundStation Duo
QSC	Q-Sys SIP Softphone
Revolabs	FLX UC 1000
Valcom	One-Way IP Speakers PagePro IP
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
Teledex	SIP ND2000 Series SIP NDC2000 Series SIP LD4200 Series

8.1 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.
- **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.

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.

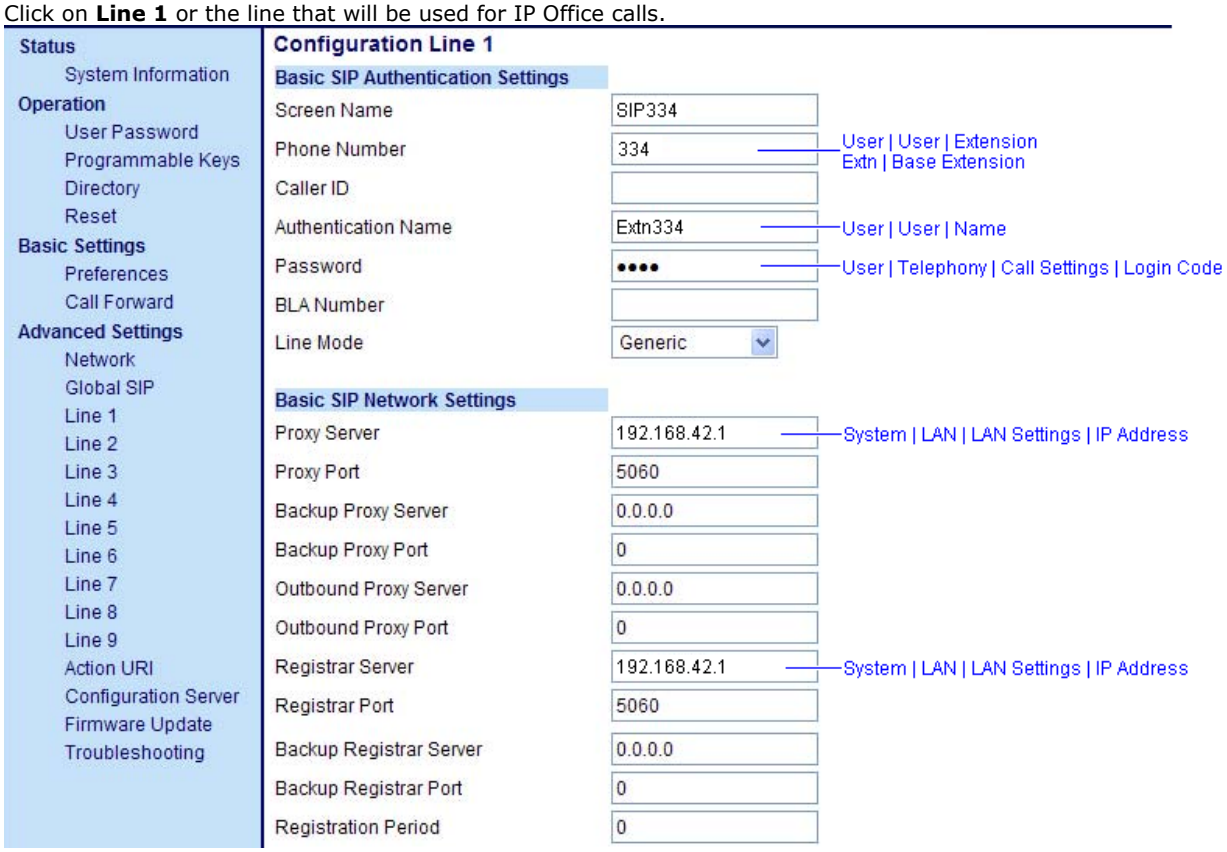
  - **Answer calls.**
  - **Make calls.**
  - **Hang Up.**
  - **Hold.**
  - **Unsupervised Transfer.**
  - **Supervised Transfer.**
  - **Voicemail Collect.**
  - **Set Forwarding/DND.**
  - **Park/Unpark.**
  - **Hear Page Calls**

8.2 AAstra 9133i SIP

AAstra produce a range of SIP phone devices. The example used here is a 9133i phone.

A. Either enable **Auto-Create Extn/User** or otherwise manually add SIP extensions and users to the IP Office configuration.

1. Browse to the IP address of the phone.
2. Login. The default user name and password are ***Admin*** and ***22222***.
3. Click on **Line 1** or the line that will be used for IP Office calls.



4. Enter the values to match the IP Office configuration settings as indicated above.

B. If installed using extension and user auto-creation, check the settings of the IP Office SIP extension and user created by the SIP devices registration.

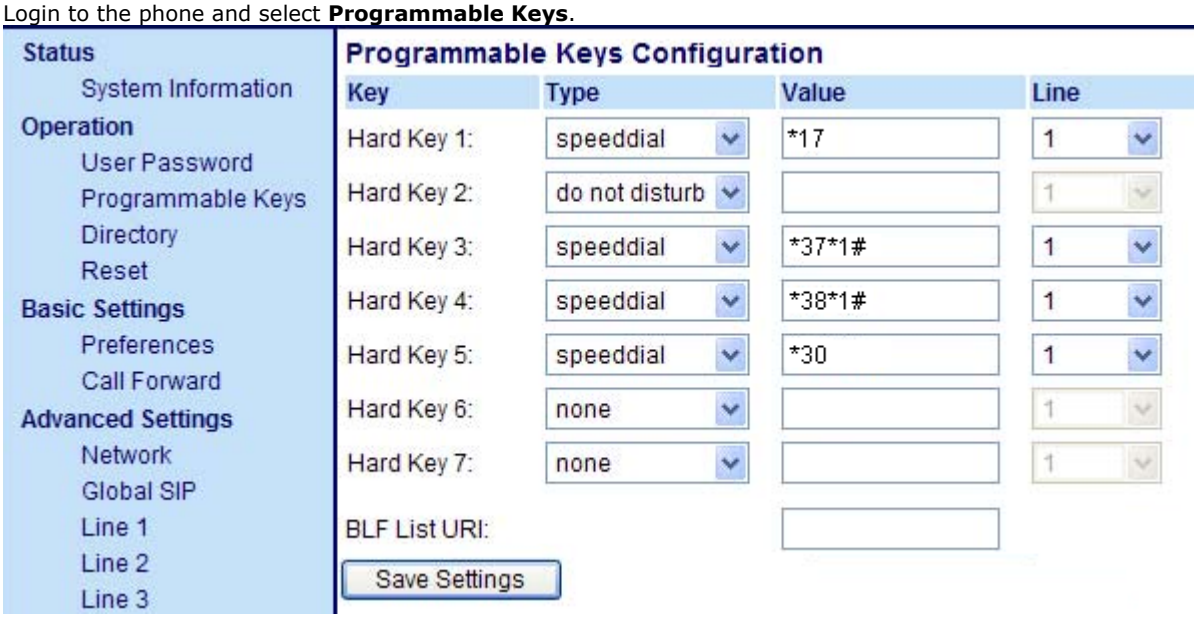
C. Make test calls from and to the SIP device.

D. If not installing any further SIP devices, **Disable Auto-Create Extn/User** if it is enabled.

Key Programming

The AAstra phones have a range of programmable keys that can be used to activate phone functions or to speed dial numbers. To use these to activate IP Office functions, the key must be configured to speed dial an IP Office short code.

1. Login to the phone and select **Programmable Keys**.



2. In the example above:
   - The first button on the side of the phone has been made a voicemail button by setting it to speed dial the default IP Office short code for voicemail access.
   - The second button is the phones own **Do Not Disturb** function. Therefore when used it will not be reflected in the users DND status on the IP Office system.
   - The third and fourth buttons are set to use the IP Office default short codes for parking and unparking a call from park slot 1 on the IP Office system. The phones own **Park** function does not work with IP Office systems.
   - The fifth button is set to the IP Office default short code for Call Pickup Any.

Notes

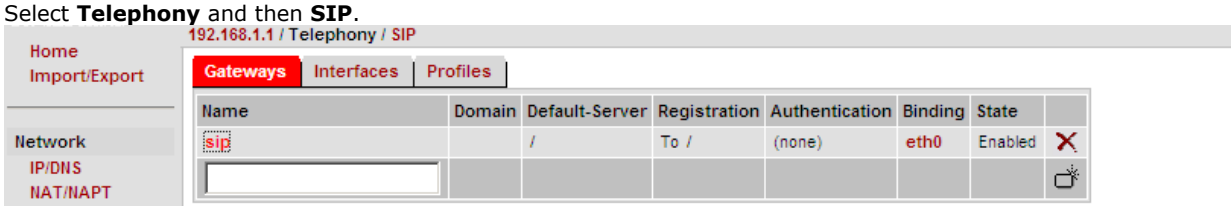
- Appearances L1-L3 do function and auto hold will work when switching lines
- Speaker button works but release is done thru the hang up button, you cannot end a speaker call by hitting speaker button again.
- To transfer use the **xfer** key. Press **xfer**, enter the transfer destination and press **xfer** again.
- To park a call, use the **xfer** key to transfer the call to the short code for parking a call. For example in this case transfer to *38*1#. To unpark, dial the short code created for that function.
- The **Conf** button can be used to conference calls. With the first party connected, press **Conf**, dial the second party and when answered press **Conf** again.

8.3 Avaya A10 ATA

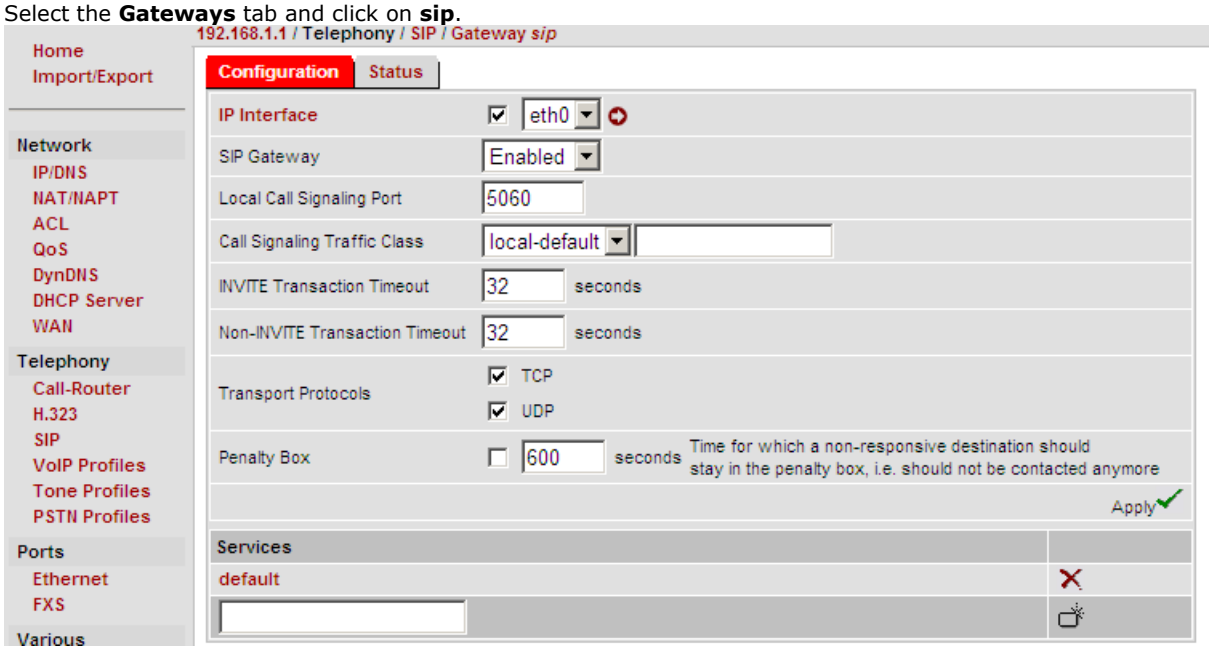
The Avaya A10 Analog Telephone Adapter provides 4 Phone/FXS ports on its rear plus a LAN port. It can be used to connect analog phone devices to the IP Office via the LAN, with the extensions appearing in the IP Office configuration as SIP extensions.

A. Either enable **Auto-Create Extn/User** or otherwise manually add SIP extensions and users to the IP Office configuration.

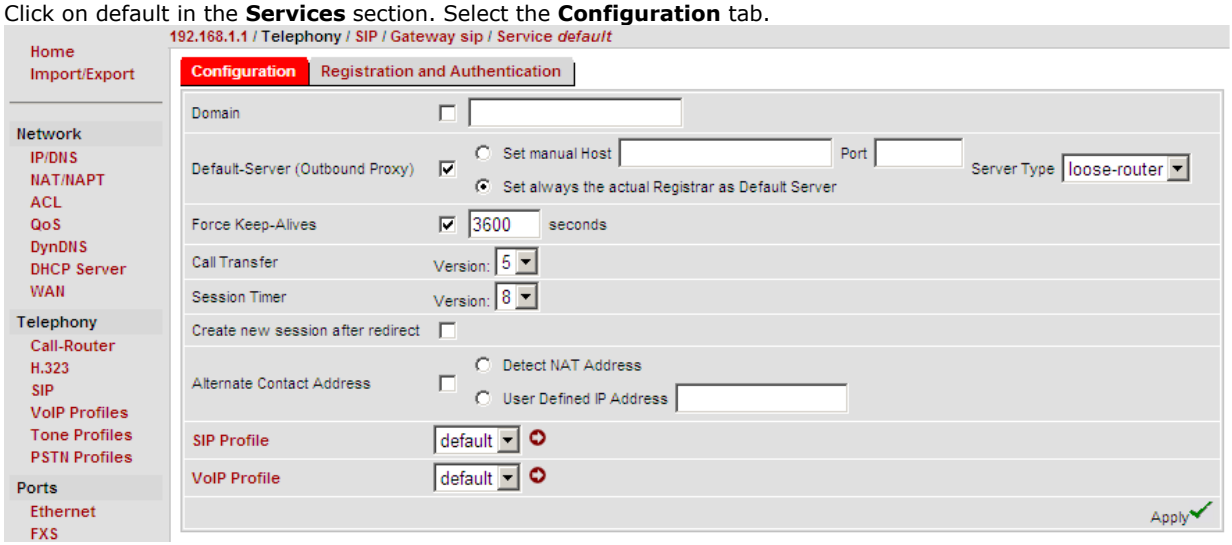
1. Browse to the IP address of the A10.
2. Enter the administrator name and password. The defaults are ***nimdbg*** and ***54321***.
3. Select **Telephony** and then **SIP**.



4. Select the **Gateways** tab and click on **sip**.

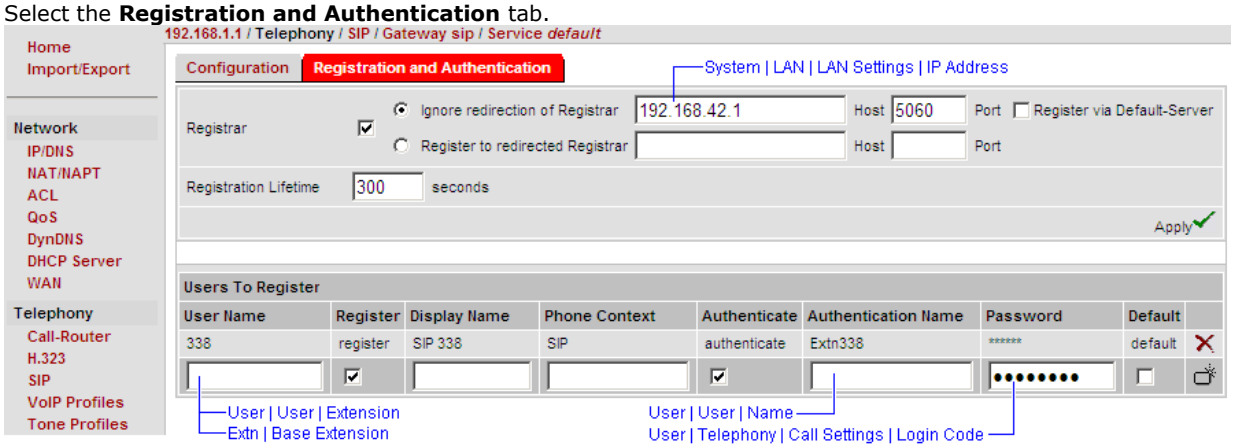


5. Click on default in the **Services** section. Select the **Configuration** tab.



- Ensure that the **Domain** field is empty and the check box not selected.
- Enable the check box for **Default-Server (Outbound Proxy)** and select **Set always the actual Registrar as Default Server**.
- Click **Apply**.

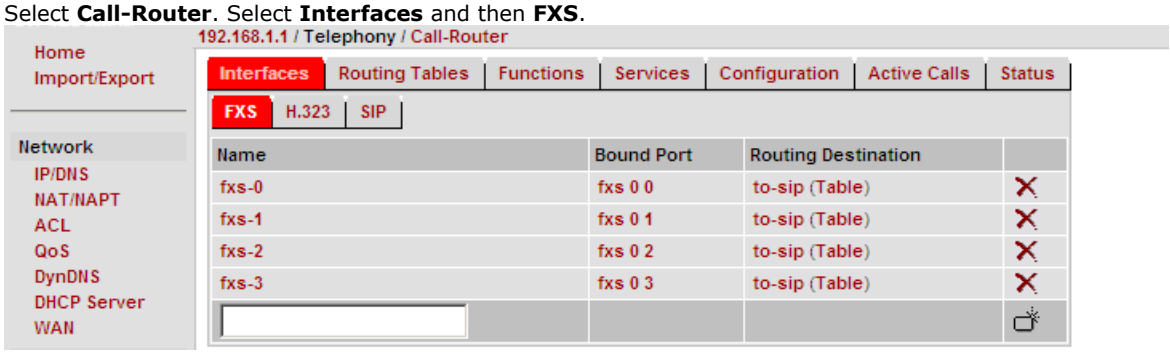
6. Select the **Registration and Authentication** tab.



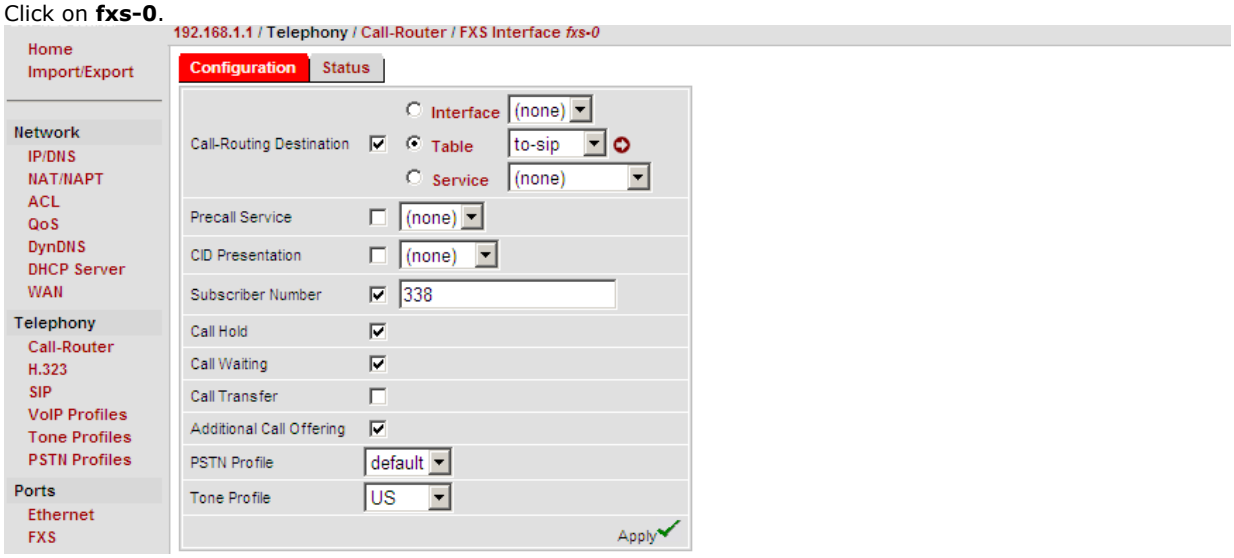
- Enable the Registrar checkbox. Select **Ignore redirection of Registrar** and enter the IP address and SIP port of the IP Office LAN on which the SIP registrar is enabled. Click **Apply**.

7. In the **Users To Register** section, create a user matching the IP Office SIP extension and user. Enter the settings and click on .

8. Select **Call-Router**. Select **Interfaces** and then **FXS**.

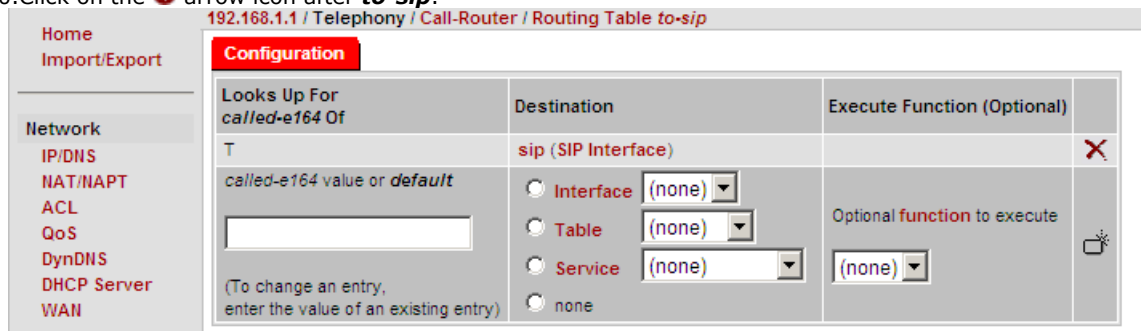


9. Click on **fxs-0**.



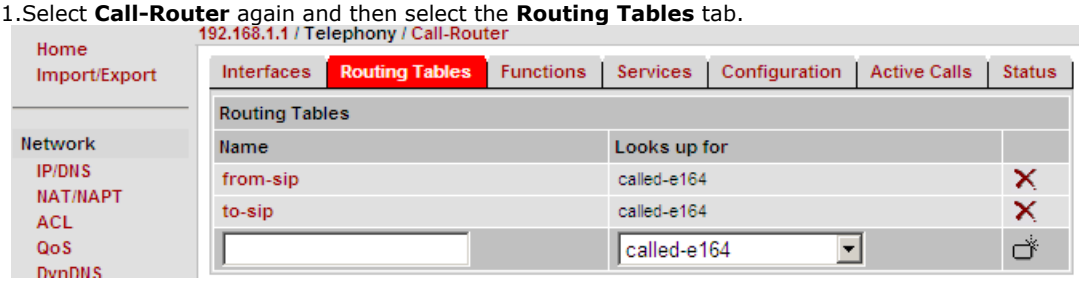
- Enable the **Call-Routing Destination** checkbox. Select **Table** and in the adjacent drop down list select ***to-sip***.
- Enable the **Subscriber Number** checkbox and enter the IP Office extension number for the SIP extension and user.
- Click **Apply**.

10. Click on the arrow icon after ***to-sip***.

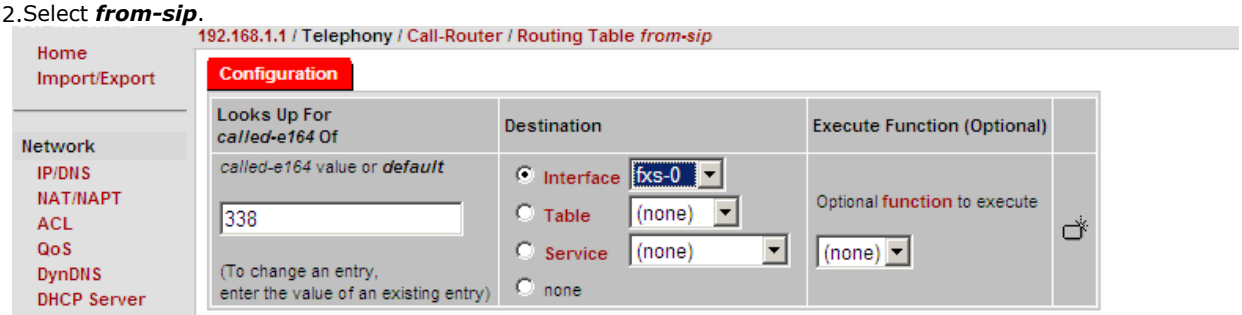


- Ensure that the table contains **T** with the destination **sip (SIP Interface)**.

11. Select **Call-Router** again and then select the **Routing Tables** tab.

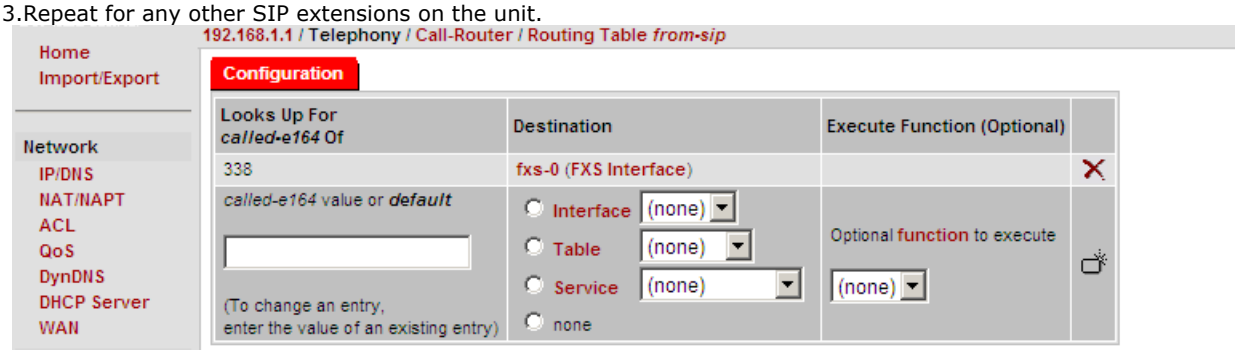


12. Select ***from-sip***.

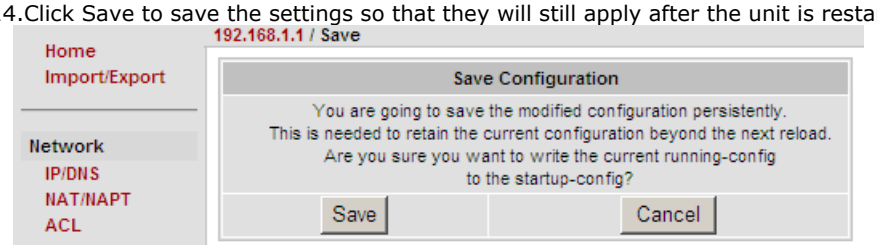


- Enter the IP Office SIP extension number.
- For the **Destination** select **Interface** and select the matching fxs port for that extension number.
- Click .

13. Repeat for any other SIP extensions on the unit.



14. Click Save to save the settings so that they will still apply after the unit is restarted.



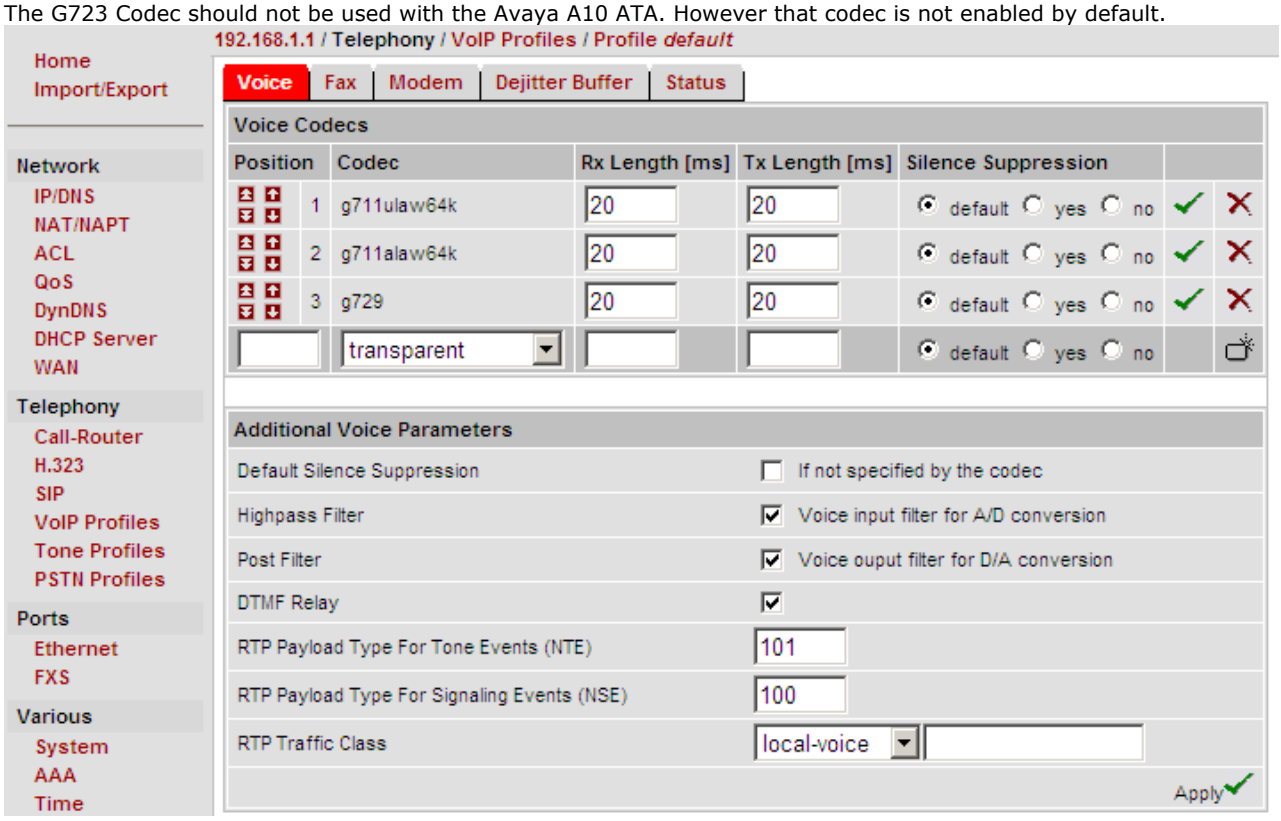
B. If installed using extension and user auto-creation, check the settings of the IP Office SIP extension and user created by the SIP devices registration.

C. Make test calls from and to the SIP device.

D. If not installing any further SIP devices, **Disable Auto-Create Extn/User** if it is enabled.

Notes

- When calling from an phone attached to an FXS port, there is a delay of approximately 5 seconds while the unit wait for dialing to be completed before it routes the dialed digits to the IP Office. To avoid this delay dial # after dialing the digits.
- The G723 Codec should not be used with the Avaya A10 ATA. However that codec is not enabled by default.

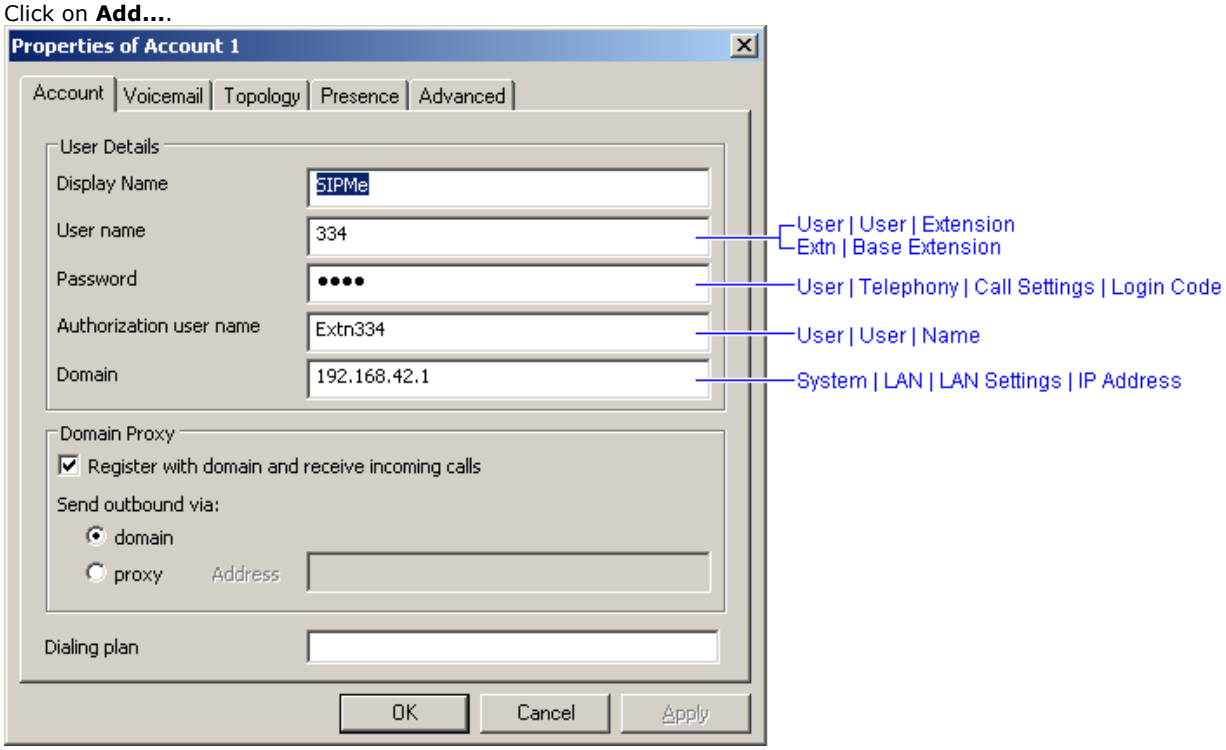


8.4 CounterPath eyeBeam/X-Lite

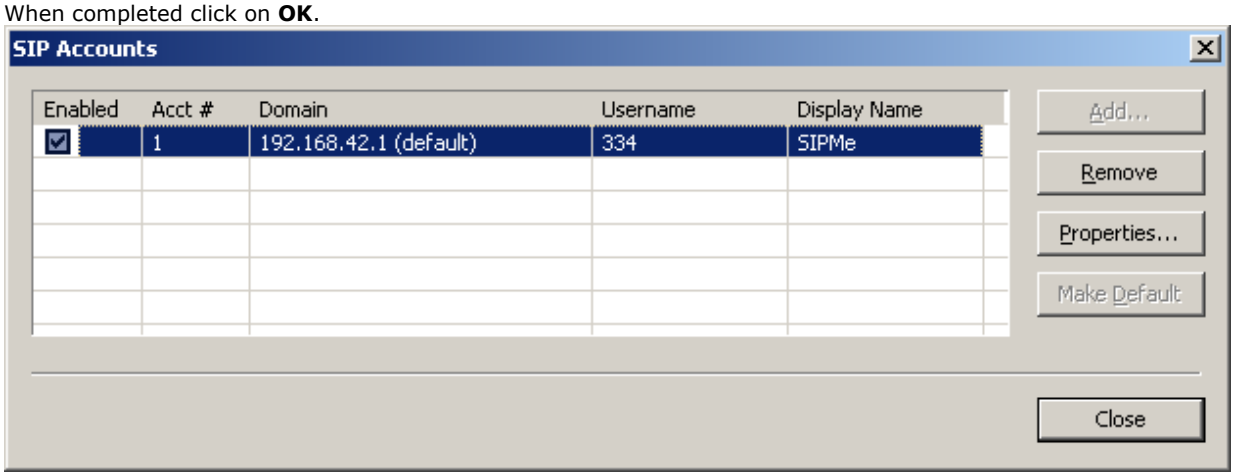
CounterPath produce a range of VoIP products. X-Lite is a simple SIP client application that can be used as a PC softphone test SIP operation. X-Lite can be downloaded from http://www.counterpath.com/.

A. Either enable **Auto-Create Extn/User** or otherwise manually add SIP extensions and users to the IP Office configuration.

1. Either enable the IP Office to allow automatic creation 29 based on SIP phone registration or manually add the SIP extension and user details to the IP Office configuration.
2. Start the X-Lite SIP client application.
3. Click on the down arrow icon and select **SIP Account Settings...**.
4. Click on **Add...**.

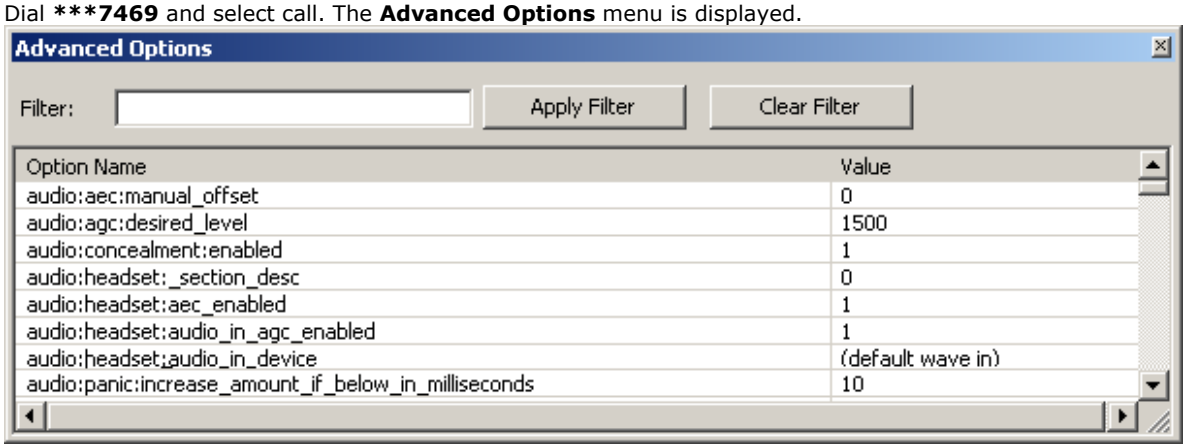


5. Set the fields to match the IP Office configuration settings are indicated above.
6. In the **Domain Proxy** section enable **Register with domain and receive incoming calls** and select **domain** .
7. When completed click on **OK**.

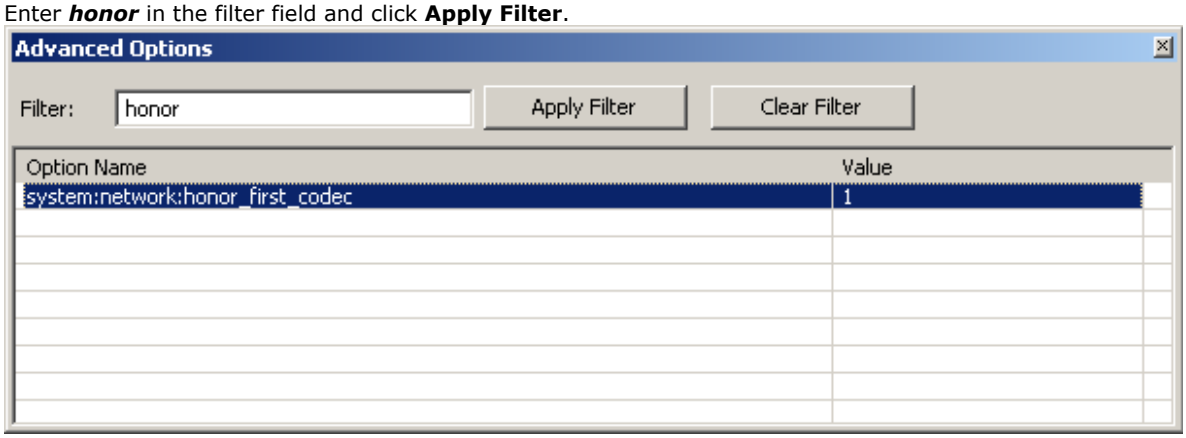


8. Ensure the the account is **Enabled**.
9. Click **Close**. The X-Lite client will now attempt to register with the IP Office. The success or failure of that process will be displayed by the client.
10. If left with its default configuration, then on calls from an IP Office DS extension to the X-Lite client, the speech from the client will not be heard. The solution is to either configure the client with a single audio codec 78 or to perform the following process.

a. Dial ***7469** and select call. The **Advanced Options** menu is displayed.

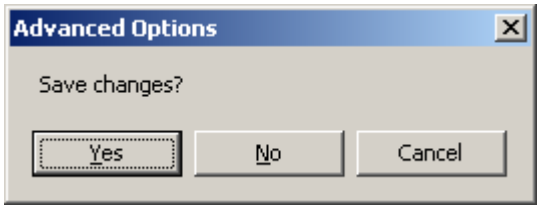


b. Enter ***honor*** in the filter field and click **Apply Filter**.



c. Set the value for **system:network:honor_first_codec** to ***1***.

d. Click on the **X** icon to close the menu.



e. Click on **Yes** to save the change.

B. If installed using extension and user auto-creation, check the settings of the IP Office SIP extension and user created by the SIP devices registration.

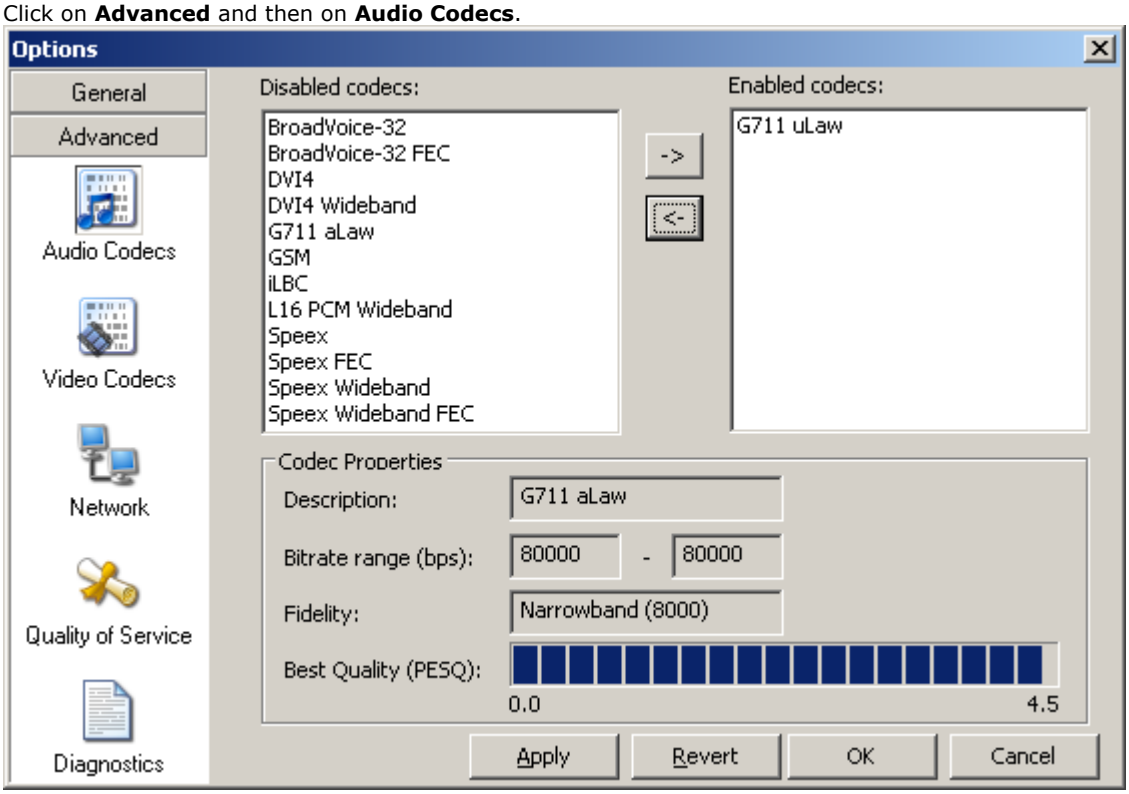
C. Make test calls from and to the SIP device.

D. If not installing any further SIP devices, **Disable Auto-Create Extn/User** if it is enabled.

Codec Selection

If the X-Lite client is left configured to support multiple audio codecs, then on calls to the extension there will be no return speech from the client. This can be resolved by configuring the client to only support a single audio codec, matching one of the codecs configured for the IP Office SIP extension.

1. Click on the down arrow icon and select **Options**.
2. Click on **Advanced** and then on **Audio Codecs**.



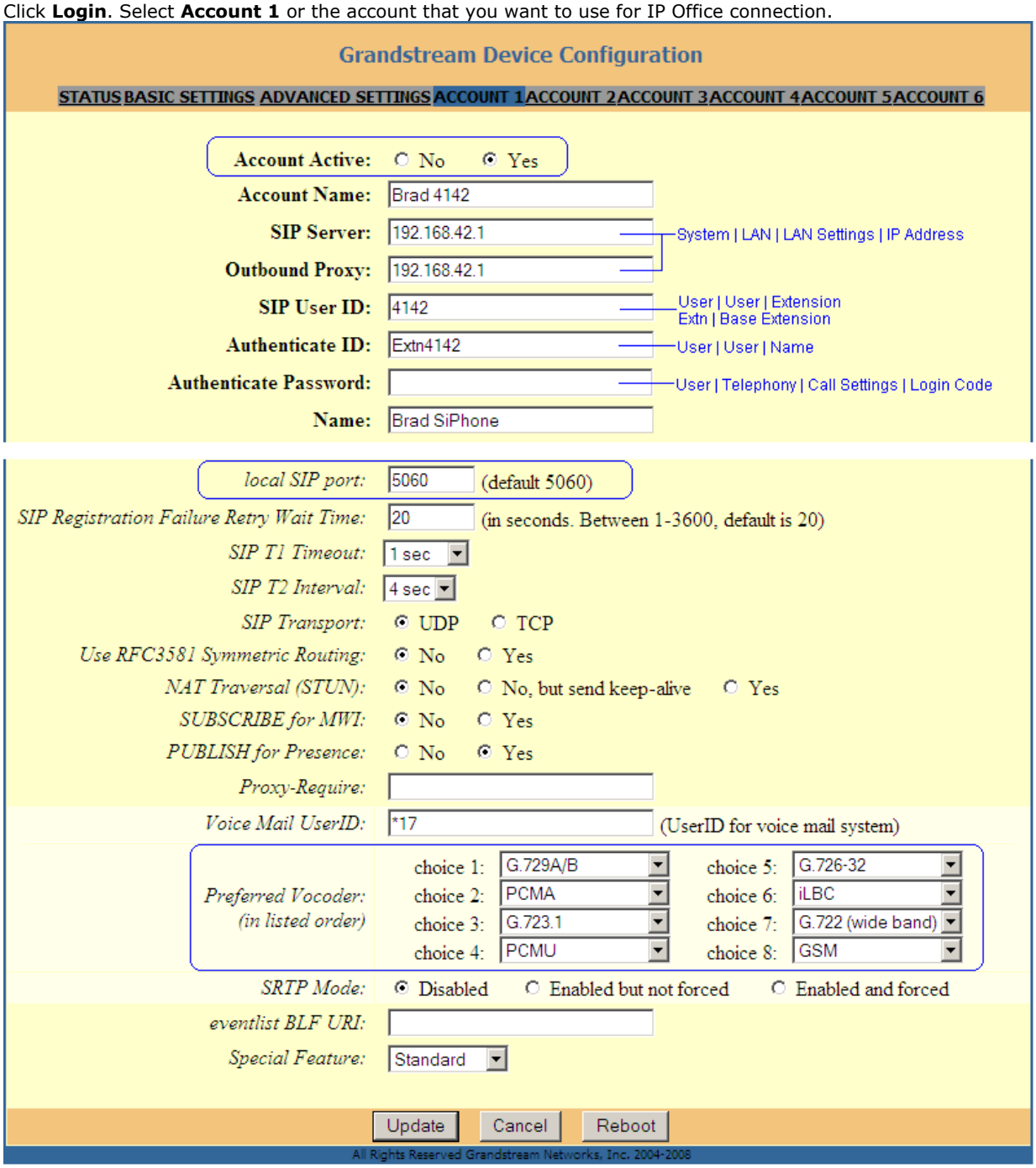
3. Ensure that the **Enabled codecs** column contains just a single codec. That codec must be one supported by the IP Office extension configuration for the SIP extension.
4. Click **OK**.

8.5 Grandstream

Grandstream devices can support multiple user accounts for the same or different SIP provider accounts. The configured accounts are displayed on the phone display and the user can select which account is used when making a call. For IP Office operation, each account can represent a different IP Office SIP extension and user.

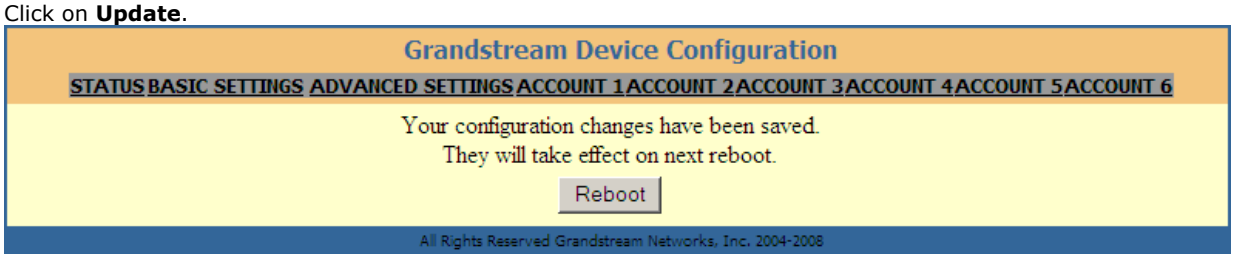
A. Either enable **Auto-Create Extn/User** or otherwise manually add SIP extensions and users to the IP Office configuration.

1. Browse to the IP address of the phone. By default the phone uses DHCP and displays its IP address on the display. Enter the password (the default is **admin**).
2. Click **Login**. Select **Account 1** or the account that you want to use for IP Office connection.

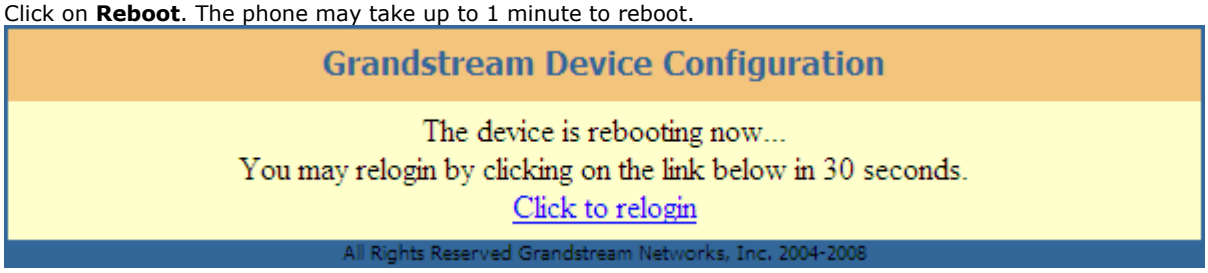


3. Set the fields indicated above to match those required for the IP Office system.

4. Click on **Update**.



5. Click on **Reboot**. The phone may take up to 1 minute to reboot.



B. If installed using extension and user auto-creation, check the settings of the IP Office SIP extension and user created by the SIP devices registration.

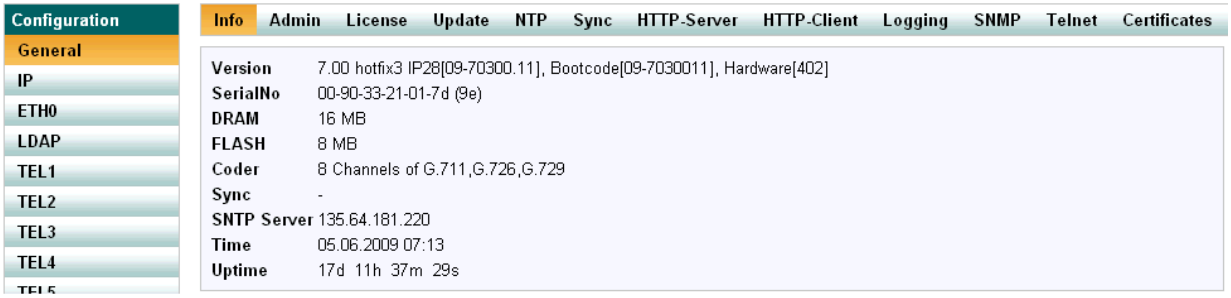
C. Make test calls from and to the SIP device.

D. If not installing any further SIP devices, **Disable Auto-Create Extn/User** if it is enabled.

8.6 Innovaphone IP22, IP24, IP28

A. Either enable **Auto-Create Extn/User** or otherwise manually add SIP extensions and users to the IP Office configuration.

1. Browse to the IP address of the unit.

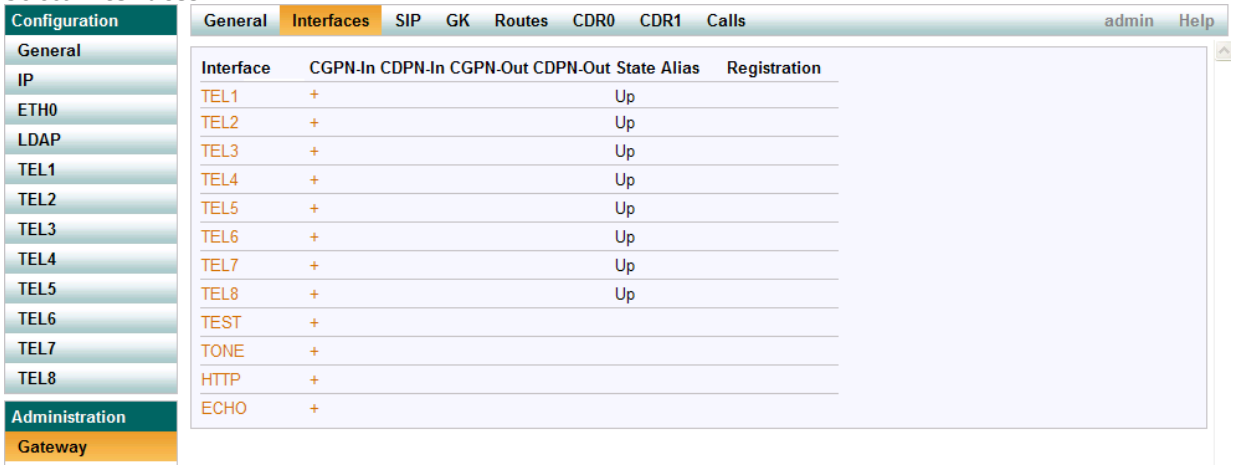


2. In the left hand column select **GATEWAY**.

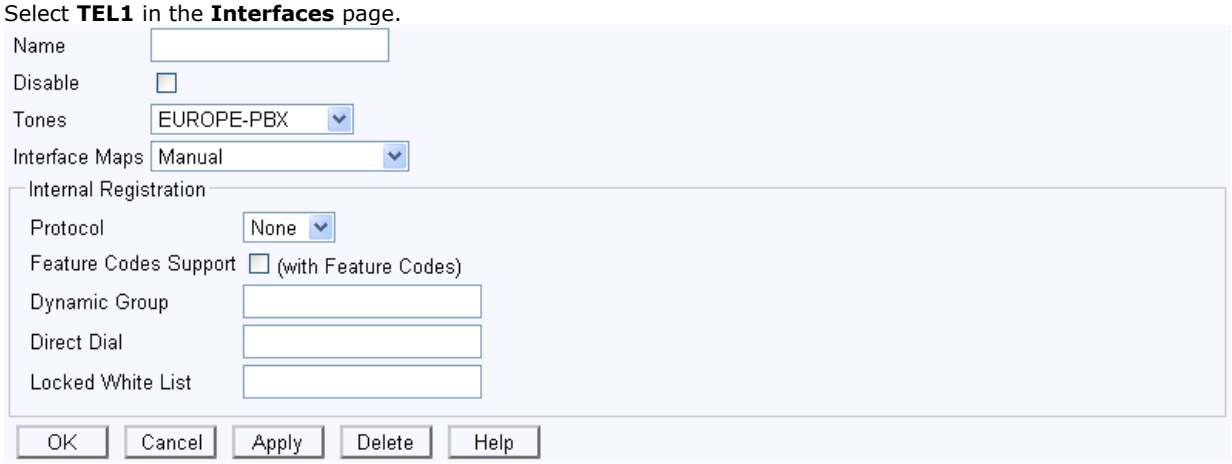
3. You will be prompted to login. The default user name is ***admin***. The default password is ***ip22***, ***ip24*** or ***ip28*** depending on the unit type.



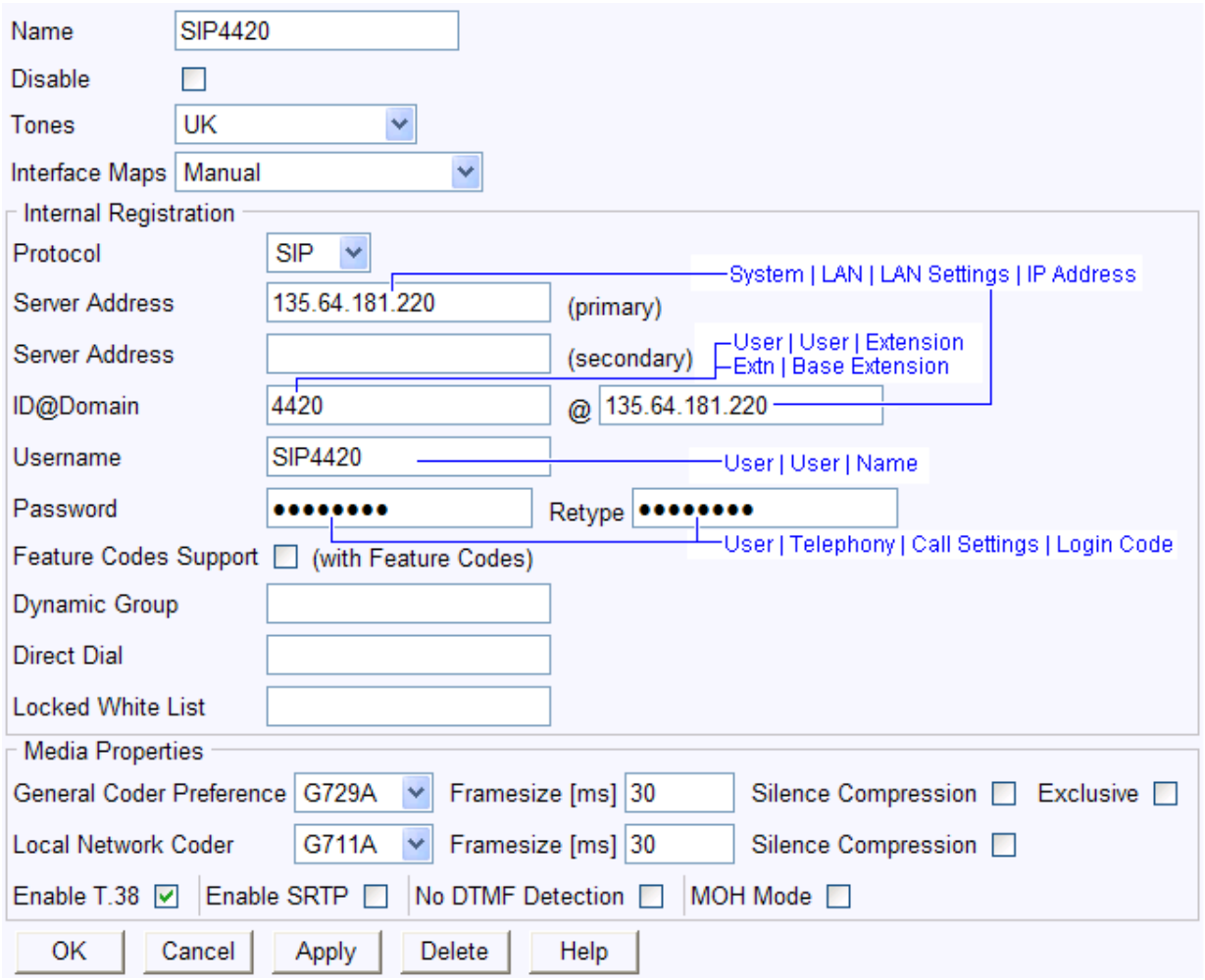
4. Select **Interfaces**.



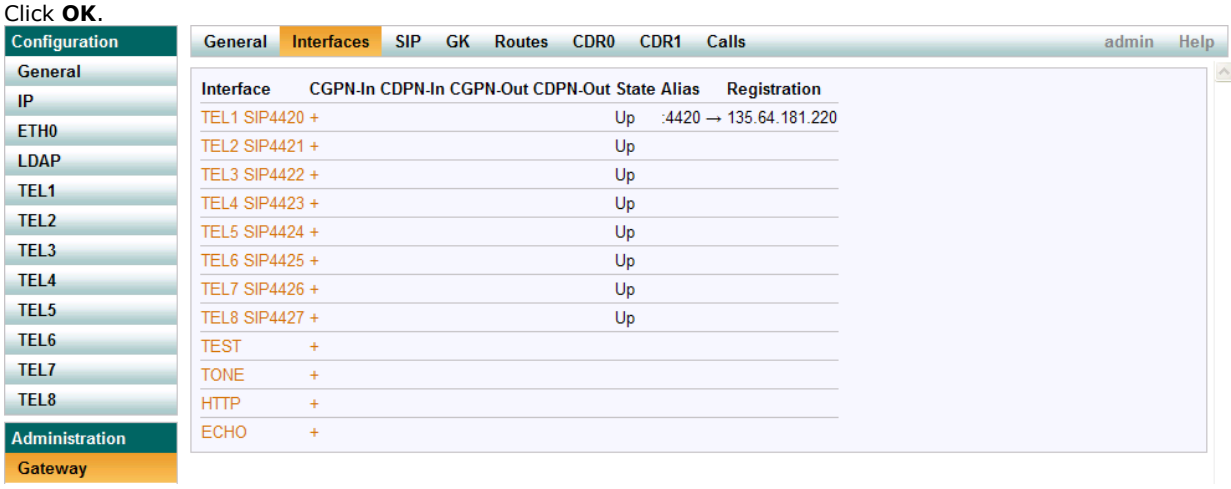
5. Select **TEL1** in the **Interfaces** page.



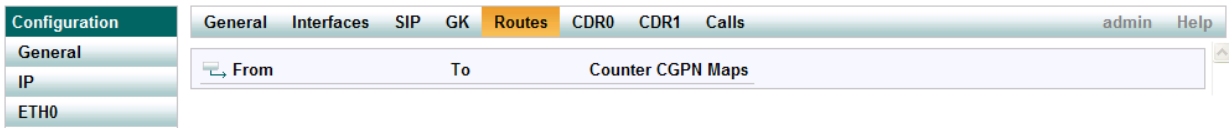
6. In the **Protocol** drop down list select ***SIP***. Enter the details as indicated below to match your IP Office SIP extension and user.



7. Click **OK**.

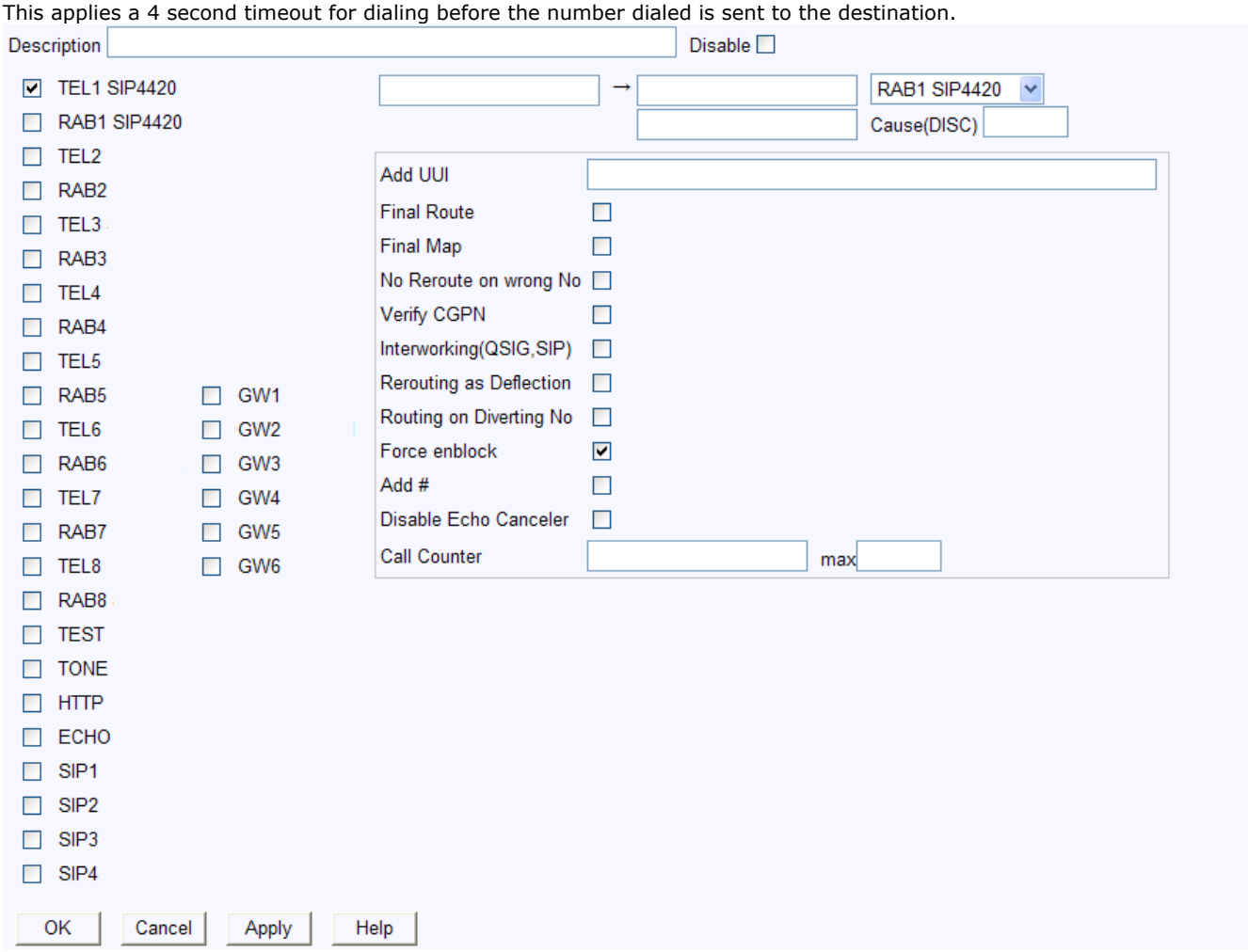


8. Select **Routes**.



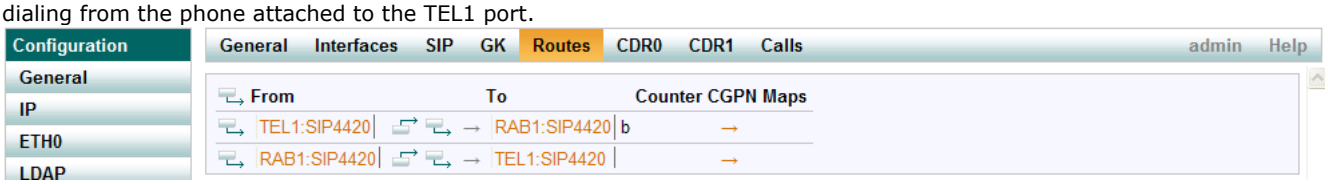
9. Two new routes are needed, one for dialing from the phone attached to the TEL port and one for incoming calls to the SIP account registered with the TEL port.

10. Click on the top-left icon. For the source select the checkbox for the **TEL** port just configured. For the destination use the drop down list to select the matching **RAB** entry. Ensure that **Force enblock** is selected. This applies a 4 second timeout for dialing before the number dialed is sent to the destination.



11. Click **OK**. Click on the next to the newly added route. This time selecting the check box for the same RAB entry and in the drop-down list selecting the TEL entry. Click **OK**.

12. The **Routes** form should show the routes just added. The b indicates the Force enblock setting of the outgoing dialing from the phone attached to the TEL1 port.



13. To edit an existing route click on the → arrow just before the To column.

B. If installed using extension and user auto-creation, check the settings of the IP Office SIP extension and user created by the SIP devices registration.

C. Make test calls from and to the SIP device.

D. If not installing any further SIP devices, **Disable Auto-Create Extn/User** if it is enabled.

8.7 Nokia S60 v3 SIP Client

The Nokia S60 SIP Client is a SIP client application that can be installed and used on a range of Nokia phones. The process below was performed on a Nokia e64 but

For Nokia S60 SIP Clients, the IP Office SIP Extension setting **Force Authorization** should be disabled.

A. Either enable **Auto-Create Extn/User** or otherwise manually add SIP extensions and users to the IP Office configuration.

1. Select **Menu | Tools | Settings | Connection | Sip settings | New SIP profile**.
2. Enter the following settings:
   - **Profile name:** Give the profile a name that indicates its function.
   - **Service profile:** Select ***IETP***.
   - **Default access point:** Enter your access point.
   - **Public user name:** Enter an address of the form ***<IP Office extension number>@<IP Office SIP Enabled LAN IP address>***, for example ***338@192.168.42.1***.
   - **Use compression:** Select ***no***.
   - **Registration:** Select ***always on***.
   - **Use security:** Select ***no***.
   - **Proxy server:** Leave blank.
   - **Registrar server:**
     - **Registrar server adress:** Enter the IP Office SIP Enabled LAN IP address.
     - **Realm:** Enter an address of the form ***<IP Office user name>@<IP Office SIP Enabled LAN IP address>***, for example ***Extn338@192.168.42.1***.
     - **User name:** Enter the IP Office extension number.
     - **Password:** Enter the IP Office user's login code.
     - **Transport type:** Select auto.
     - **Port:** Match the port set on the IP Office LAN **SIP Registrar** tab, by default this is ***5060***.
3. Select **Menu | Tools | Settings | Connection | Internet telephone | New profile**.
   - Select the SIP profile just created above.
4. Select **Menu | Communication | Internet tel. | Options | Settings**.
   - Change the **Default call type** to ***Internet call***.

B. If installed using extension and user auto-creation, check the settings of the IP Office SIP extension and user created by the SIP devices registration.

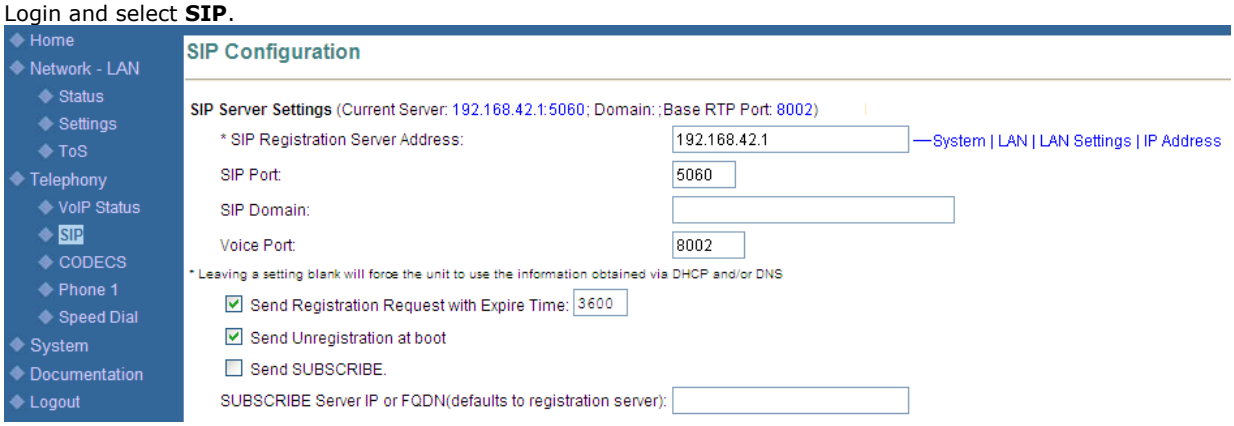
C. Make test calls from and to the SIP device.

D. If not installing any further SIP devices, **Disable Auto-Create Extn/User** if it is enabled.

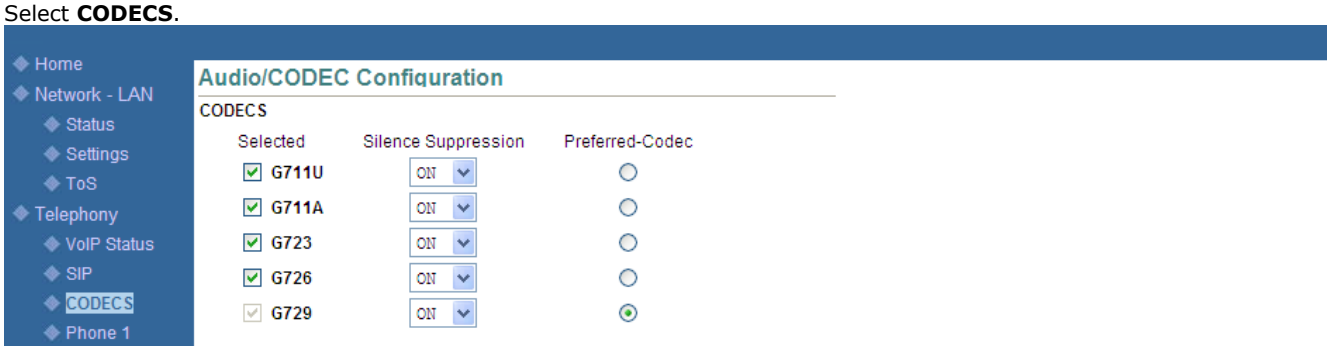
8.8 Patton Micro ATA

A. Either enable **Auto-Create Extn/User** or otherwise manually add SIP extensions and users to the IP Office configuration.

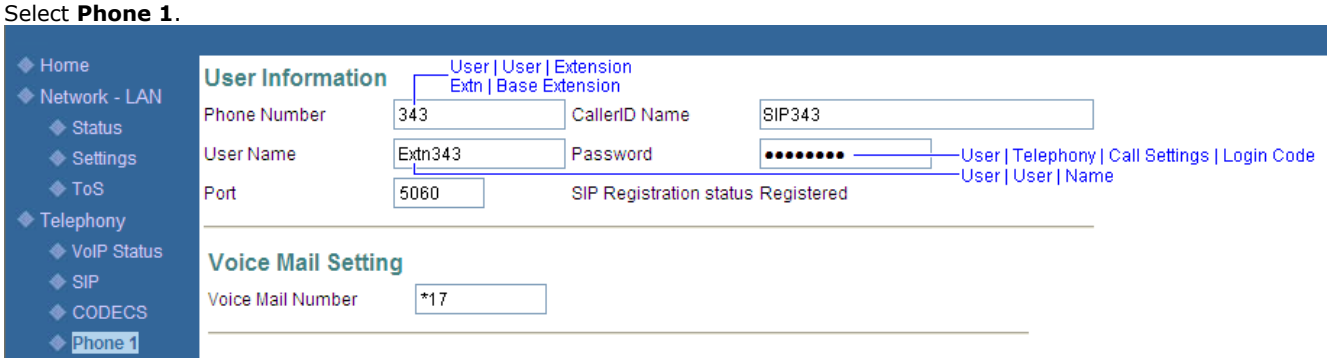
1. Browse to the IP address of the Micro ATA.
2. Login and select **SIP**.



3. Enter the values to match the settings of the IP Office LAN on which the SIP Registrar is enabled. Click **Save**.
4. Select **CODECS**.



5. Set the codecs to match those set for the IP Office SIP extension. Click **Save CODEC Configuration**.
6. Select **Phone 1**.



7. Enter the values to match the IP Office SIP extension and user settings. Click **Save**.

B. If installed using extension and user auto-creation, check the settings of the IP Office SIP extension and user created by the SIP devices registration.

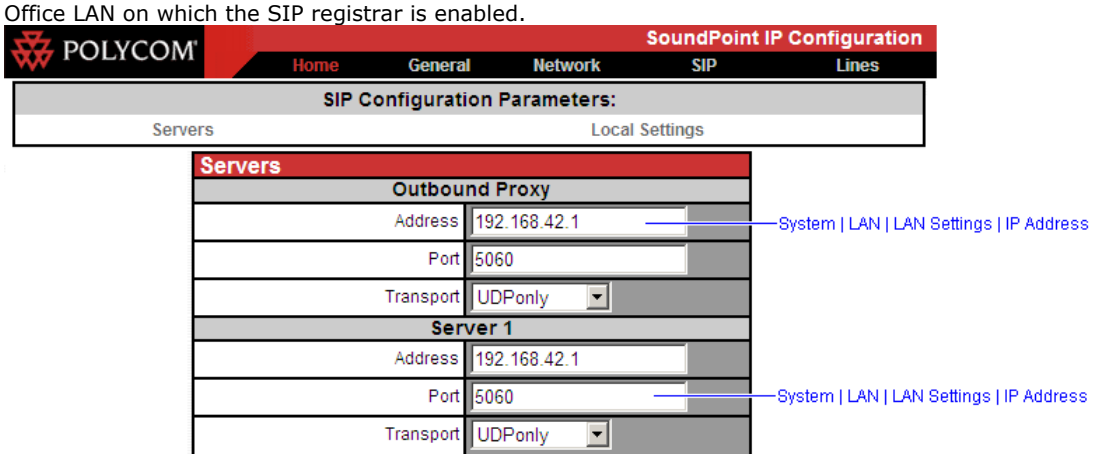
C. Make test calls from and to the SIP device.

D. If not installing any further SIP devices, **Disable Auto-Create Extn/User** if it is enabled.

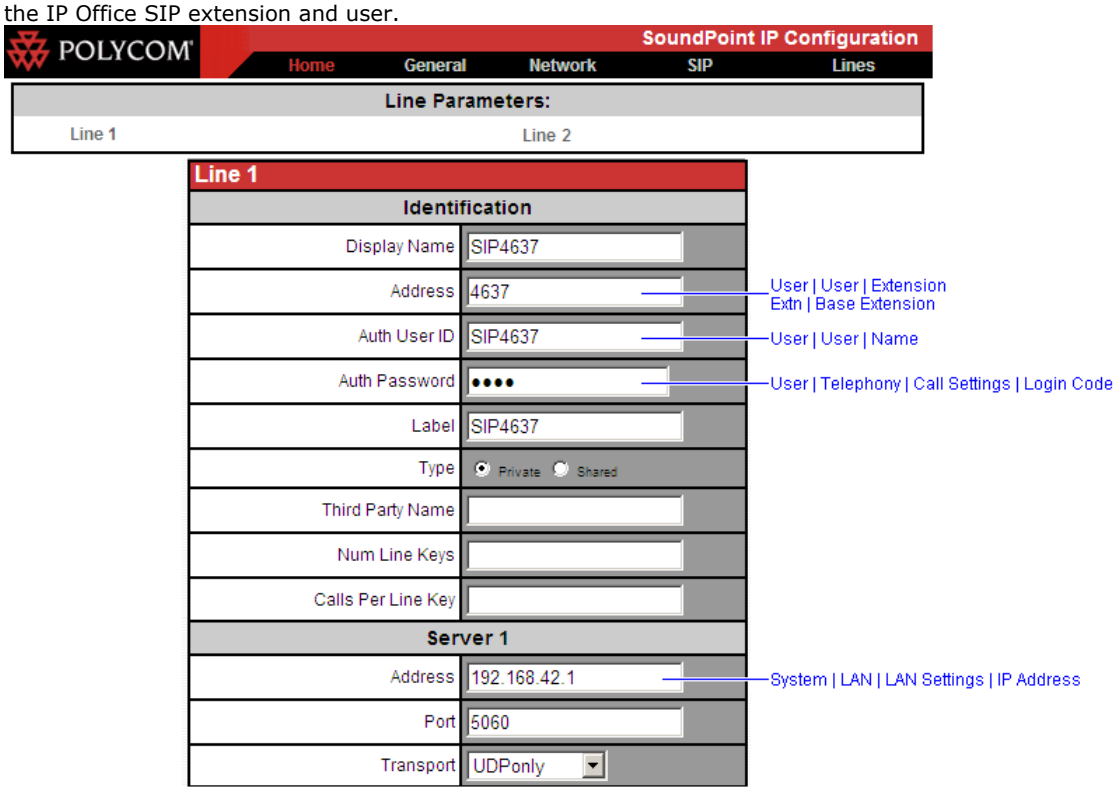
8.9 Polycom SoundPoint Phones

A. Either enable **Auto-Create Extn/User** or otherwise manually add SIP extensions and users to the IP Office configuration.

1. Browse to the IP address of the phone. By default the phone uses DHCP and displays its IP address on the display.
2. Select **SIP**. You will be requested to enter the administrator name and password. The default values are ***Polycom*** and ***456***.
3. in the **Outbound Proxy** and **Server 1** sections, set the **Address**, **Port** and **Transport** details to match the IP Office LAN on which the SIP registrar is enabled.



4. Click **Submit**. The phone will reset and load the new settings. That can take up to 2 minutes.
5. When you can return to the administration menu, select **Lines**. In the Line 1 section, enter the details to match the IP Office SIP extension and user.



6. Click **Submit**. The phone will reset and load the new settings. That will take up to 2 minutes.
7. Select **Network** and then **Audio Processing**. Check that the codecs match those configured for the SIP extension on the IP Office. If you make any changes click **Submit** and wait for the phone to reset.

B. If installed using extension and user auto-creation, check the settings of the IP Office SIP extension and user created by the SIP devices registration.

C. Make test calls from and to the SIP device.

D. If not installing any further SIP devices, **Disable Auto-Create Extn/User** if it is enabled.

Chapter 9.
Document History

9. Document History

Date	Issue	Changes
23rd November 2016	**01a**	• Generic IP Office SIP phone installation manual.
1st December 2016	**01b**	• First issue to support forthcoming release of IP Office R10 SP2.
7th December 2016	**01c**	• Minor typo corrections. • Statement regarding SIP phone hot desking.

Index

1

1100 Series Phones 54
1200 Series Phones 54
176 24

2

242 24, 40

3

3rd-Party IP Phones license 9

A

Account Code 14
Allow Direct Media 21
Allow Direct Media Path 26
Application Notes 15
Applications 10
Apply to Avaya IP Phones Only 23
Aura 14
Authorisation Code 14
Auto-answer 26
Auto-Creation
  Extensions 29
  Users 29
Auto-generation 12
Avaya IP Endpoints license 9

B

B100 Series Phones 54
Base Extension 26
Blacklisting 52
Branch 14

C

Calls
  Monitor 52
Centralized Branch 14
Certificates 42
Challenge Expiry Time 19
Codec
  Extension 26
  Lockdown 26
Codecs 21
Create identity certificates 46

D

D100 Series Phones 54
Data 10
DHCP 10, 11
  242 40
  Apply to Avaya IP Phones Only 23
  Mode 23
  Option 40
  Pools 23
  Settings 22
  SSON 24, 40
DHCP Server
  Alternate 38
Direct Media 21, 26
Disk 33
Documentations 15
Domain Name 19
Download
  Certificate 43
DTMF 21, 26

E

E100 Series Phones 55
Edit
  Extension 26
  Scope 40
  Settings 13
  SSON 66
  User 25
Extension
  Auto-creation 29
  Codec 26
  Register 30
  User 25

F

Failback 14
Failover 14
File Server 12, 32
  Certifcate 48
  Upload files 34
Files
  Upload 34
Force Authorization 25
FQDN 19
Fully Qualified Domain Name 19

H

H100 Series Phones 62
Hold Music 26
Hot desking 14
HTTP
  Clients Only 33
  File Server Address 33
  Redirection 33

I

Identity Certificate
  File Server 48
Inband 26

J

J100 Series Phones 63

L

Layer 4 Protocol 19
Licenses 9
Local Hold Music 26
Log in 14
Log out 14
Login Code 25

M

Manuals 15
Media Security 26
Memory Card 33
Minimum Assessment Target 10
Monitor 52

N

Name
  User 25
network assessment 10

O

Option 40

P

Packet Loss 10
Phone
  Register 30
Phones
  1100 Series 54
  1200 Series 54
  3rd-Party 68
  B100 54

Phones
D100 54
E100 Series 55
H100 Series 62
J100 Series 63
PoE 11
Pools 23
Power 11
Protocol 19
Provisioning Server 12, 32

Q

Quality 10

R

Register 30
Blacklisting 52
View 52
Registrar 19
Remote Extension
Enable 19
Remote Worker 14
Reserve License 26
Resilience 14
RFC2833 21, 26
RFC5373 26

S

Scope
Activate 40
Create 39
Security 42
Server
DHCP 11
File 12, 32
Provisioning 12
Settings
Auto-generation 12
Editing the settings file 13
Silence Suppression 26
SIP
Domain Name 19
FQDN 19
Registrar 19
SSON 24, 39, 40
Change 66
Static addressing 65
System Default
Codecs 21
System Monitor 52

T

TCP
Port 19
TLS
Port 19

U

UDP
Port 19
Upload files 34
User
Auto-creation 29
Extension 25
Login Code 25
Name 25

V

VCM 11
View 52
Voice Compression 11
VoIP 10

© 2016 Avaya Inc. All rights reserved.