IP Office SIP Telephone Installation Notes

Release 12.0
Issue 23
April 2024

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Part 1: IP Office SIP Phone Installation Notes

Chapter 1: IP Office SIP Phone Installation Notes

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

This document covers the general installation of SIP telephones with IP Office 11.1 or higher systems. It assumes that you are familiar with IP Office configuration and maintenance.

It begins with a generic installation process which is suitable for most types of SIP telephone. Additional notes 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.

Note:

- The previous sections for Avaya Workplace Client and Avaya Spaces have been moved to the separate IP Office Avaya Workplace Client Installation Notes manual.

Related links

Supported Avaya SIP Phones on page 11

Supported Avaya SIP Phones

The following Avaya SIP telephones are supported on IP Office Release 11.1 systems. The supported phones depend on the systems operating mode (no IP phones are supported in IP Office Basic Edition mode).

Series	Description	IP Office Subscription
1010, **1040**	-	-
1120E, **1140E**	-	-
1220, **1230**	-	-
B169, **B179**, **B199**	The B169 is a DECT phone that connects to a DECT base station. The base station connects to the IP Office via either a SIP base station.	✓

Table continues…

Series	Description	IP Office Subscription
D160	These DECT handsets use a base stations that connect to the IP Office system using a SIP trunk and appear on the IP Office as SIP extensions.	-
D240, **D260**		✓
H175	SIP video telephone	-
H229, **H239**, **H249**	Hospitality phones for use in hotels and similar environments.	✓
J129	A simple SIP desk phone	–
J139, **J159**, **J169**, **J179**, **J189**	Advanced SIP desk phones that support IP Office interactive menus and button programming.	✓
K155, **K165**, **K175**	These are Android telephones that can host a different dialer applications. However, aspects of their installation and maintenance are similar to that required for standard SIP desk phones so IP Office specific notes are included in this manual.	✓
K155 V3, **K175 V3**	These updated Vantage phones run a dedicated dialer application.	✓
Avaya Workplace	This SIP softphone application can be used on a range of platforms.	✓

Related links

IP Office SIP Phone Installation Notes on page 11

Chapter 2: General Installation Notes

This section provides a general overview of issues that should be considered in order to support SIP extensions.

Related links

Licenses and Subscriptions on page 13
Remote Operation on page 14
Avaya Aura Branch Operation on page 14
Third-Party SIP Phones on page 14
Network Assessment on page 15
Voice compression channels on page 16
Telephone power supply on page 16
DHCP server requirements on page 17
File (Provisioning) server requirements on page 17
Polling on page 18
Centralized branch extensions on page 18

Licenses and Subscriptions

IP Office systems use either a license file loaded onto the system or subscriptions obtained from a subscription server.

- **Subscription Systems**

  For subscription systems, all extension entitlements are based on the user subscription:

  - SIP desk phones require the associated user to have a valid user subscription.
  - SIP softphone applications require the associated used to have a **Unified Communications User** user subscription.

- **Other Systems**

  For non-subscription systems, for following license requirements apply to SIP extensions:

  - Avaya SIP desk phones require **Avaya IP Endpoint** licenses.
  - Avaya SIP softphone applications require various user licenses that may vary depending on the particular application and the type of IP Office system.

- 3rd-party SIP telephones and extensions require **3rd Party IP Endpoint** licenses.

When using **Avaya IP Endpoint** and **3rd Party IP Endpoint** 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. Unlicensed users cannot login to an extension.

Related links

General Installation Notes on page 13

Remote Operation

Many of the SIP phones above can be used as remote extensions, that is, from locations outside the network hosting the IP Office system. For details refer to the Deploying Remote IP Office SIP Phones with an ASBCE manual.

Related links

General Installation Notes on page 13

Avaya Aura Branch Operation

When used as a branch system in a centralized Avaya Aura® network , a wider range of Avaya SIP telephones are supported but only during failover operation. That is, during normal operation, they are registered and supported by servers in the Avaya Aura network rather than the IP Office. During failover, the IP Office only provides support for making and answering calls. See Centralized branch extensions on page 18.

Related links

General Installation Notes on page 13

Third-Party SIP Phones

The IP Office supports non-Avaya SIP telephones. See Third-Party SIP Phones on page 186.

Related links

General Installation Notes on page 13

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:**

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.

The network assessment targets are:

Measure	Description
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/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.

Related links

General Installation Notes on page 13

Voice compression channels

To support VoIP trunks and phones, the IP Office system must support with voice compression channels, also known as VCM channels.

- For Linux-based IP Office systems, no additional hardware is required.
- For IP500 V2 systems, voice compression channels are added to a system using a combination of the following options.
    - **IP500 VCM Base Cards:** 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.
    - **IP500 Combination Cards**: 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.

The IP Office requires a voice compression channel for:

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

Related links

General Installation Notes on page 13

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 non-PoE power supply unit.

- On phones that support PoE, that support may vary depending on whether the phone has any button modules attached. Adding buttons modules may change the level of PoE power required or may require the phone to use a separate non-PoE power supply unit.
- Use of a separate power supply unit requires each phone to have access to a mains power outlet.

Related links

General Installation Notes on page 13

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:** 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. See DHCP settings on page 42.
- **Third-Party DHCP:** 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. See Alternate DHCP server setup on page 65.

Related links

General Installation Notes on page 13

File (Provisioning) server requirements

When starting, Avaya IP phones request various files from an HTTP or HTTPS file server. This is sometimes also called the 'provisioning server'.

For example, a phone may request:

- **An upgrade file:** This file tells the phone what firmware the IP Office supports.
- **Firmware Files:** If the phone is not already running that firmware, it then requests the necessary files indicated by the upgrade file.
- **Settings File:** This provides the phone with settings specific to how it should operate on the customer's IP Office system.
- **Additional Files:** Some phones may also request specific languages and font files. Also if specified in the settings files, image files for displays and screen savers.

For IP Office operation, the IP Office system can act as the file server for most phones. This is the recommend method since normally the appropriate firmware, language and font files needed by the phones are already present on the system and are automatically upgraded if necessary when the system is upgraded. The IP Office also auto-generates any necessary settings files.

However, if necessary a third-party file server can be used. That then means that the files on that server need to be manually updated and maintained.

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

File Server Redirection

For some types of phone, the phones and IP Office support **HTTP Redirection**. Using this, when the phone requests firmware files from the IP Office, the phone is redirected to a separate third-party HTTP file server.

Phones	Description
H175 and Vantage telephones	A separate HTTP/HTTPS file server must be used. If the IP Office is set as the file server for these phones, it automatically redirects their firmware file requests to its **HTTP Server IP Address** or **HTTP Server URI** setting regardless of whether **HTTP Redirection** is enabled or not.
9600 Series and J100 Series phones	The **HTTP Redirection** setting can be enabled. When that is the case, the IP Office system redirects firmware requests for .bin files from those phone to the system's **HTTP Server IP Address** of a separate file server.
B199 Phones	For B199 phones running B199 R1.0 FP6 or higher firmware, IP Office R11.1 FP2 SP4 supports the use of **HTTP Redirection**.

Related links

General Installation Notes on page 13

Polling

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

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

Related links

General Installation Notes on page 13

Centralized branch extensions

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

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

Related links

General Installation Notes on page 13

Chapter 3: Phone file requests

When starting, Avaya IP phones go through a process of requesting various files from the file server. By default, the file server is the IP Office system.

The following is a general summary of file requests.

Files	Description
Upgrade File For example: • `J100Supgrade.txt` • `K1xxSupgrade.txt`	The process starts with the phone requesting an upgrade file: • Different files are used for different types of phone. For example `J100Supgrade.txt` for J100 Series phones, `K1xxSupgrade.txt` for K100 Series phones, and so on. • For some Avaya phones, the system can auto-generate the upgrade file if there is no static file. • The upgrade file indicates what firmware the phone should run. If that differs from the firmware the phone is already running, the phone requests the firmware files listed in the upgrade file. See below. • The last line of the upgrade file tells the phone to request a settings `46xxsettings.txt` file.
Firmware Files	If the phone needs to upgrade, it requests the firmware files indicated in the upgrade file. • Due to the size of some firmware files, for some phone, either by default or configuration, the IP Office redirects the phone to a separate file server for the firmware. • Following the upgrade, the phone restarts and requests the upgrade file again. This instructs the phone to request the settings file.

Table continues…

Files	Description
Settings File • `46xxsettings.txt`	The phone requests a `46xxsettings.txt` settings file. See The 46xxsettings.txt File on page 190. • The IP Office system auto-generates this file when requested. It populates the file with settings from the current IP Office system configuration. • Avaya strongly recommended that you use the auto-generated file. You should put customer specific settings into a `46xxspecials.txt` file. This eases support for IP Office configuration changes, and for new settings and phones supported when upgrading the IP Office. • The file can list additional files that the phone needs. For example, language files and screen savers. • The last line of the settings file can tell the phone to load the `46xxspecials.txt` specials.
Specials File • `46xxspecials.txt`	You can use a `46xxspecials.txt` file to provide settings not present in the upgrade and settings files. See The 46xxspecials.txt File on page 197. • The `46xxspecials.txt` file is supported for the Avaya Workplace Client for IP Office R11.1.2.4 and higher.

Related links

File Auto-Generation on page 21
Test the file server on page 22

File Auto-Generation

When using the IP Office system as the file server, when the phone requests a file, if that file is not available the IP Office system auto-generate a temporary file for the phone.

- The settings in an auto-generated file can vary depending on the type of phone requesting the file.
- The settings also vary depend on whether the request is from a phone on the same network as the IP Office system or from a remote phone.
- The auto-generated files are not cached by the IP Office. The files are generated when requested and deleted after the request.
- If an actual file with the same name is uploaded to the system, auto-generation of that particular file stops. See Loading files onto the system on page 55.

Related links

Phone file requests on page 20

Test the file server

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

- You cannot browse the auto-generated files if the setting **System** > **System** > **Avaya HTTP Clients Only**is enabled.

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.

Related links

Phone file requests on page 20

Chapter 4: Example additional phone settings

Additional commands can be used to configure the phone behaviors. For full details of commands available refer to the appropriate Avaya administrator's manual for the particular series of phones.

There are several **NoUser** source numbers used for remote extensions. They operate differently in that they change existing values in the auto-generated settings file given to a phone when the system detects that the phone requesting the file is a remote extension. See the Deploying Remote IP Office SIP Phones with an ASBCE manual.

Related links

46xxspecials.txt on page 23
Additional phone settings on page 24
NoUser source numbers on page 25
Configuration File Editing on page 26

46xxspecials.txt

For systems using the auto-generated `46xxsettings.txt` file, additional manual settings can be added using a file called `46xxspecials.txt`. When such a file is added to the system, the command `GET 46xxspecials.txt` appears as the last line of the auto-generated `46xxsettings.txt` file.

- The `46xxspecials.txt` file is supported for the Avaya Workplace Client for IP Office R11.1.2.4 and higher.

The `46xxspecials.txt` file needs to be manually created and then placed on the phone file server. It can be a simple text file containing a single command or a complex settings file with settings based on phone type, model and/or group. See Configuration File Editing on page 26.

To obtain an example of a complex structure, you can browse to `https://<IPOffice>/46xxspecials.txt` to obtain a sample file . Save and edit that file before uploading it back to the system.

Related links

Example additional phone settings on page 23

Additional phone settings

The auto-generated `46xxsettings.txt` settings files are suitable for most installations, see File Auto-Generation on page 21. However, in some scenarios it may be necessary to amend the value of the file settings or to add additional settings. This can be done in a number of ways:

- **Use a `46xxspecials.txt` File:**
  - If a file called `46xxspecials.txt` is present on the system, then the auto-generated `46xxsettings.txt` file instructs the phone to request that file. This allows you to upload a special file that contains any additional settings or override selected settings in the auto-generated file. See 46xxspecials.txt on page 23.
  - The `46xxspecials.txt` file is supported for the Avaya Workplace Client for IP Office R11.1.2.4 and higher.
- **Use NoUser Source Numbers:**
  - There are a number of NoUser source number settings that can be used to add special values to the auto-generated settings file. See NoUser source numbers on page 25.
- **Using Static Files:**
  - Replace the auto-generated file with an actual file. The method is only recommended for those experienced with the editing of Avaya phone settings files. The major drawback is that you no longer benefit from the automatic changing of settings to match changes in the IP Office configuration. See Configuration File Editing on page 26.

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

Description	Setting File Command
Set the PROCPSWD specified in the auto-generated `46xxsettings.txt` file where X is the password. This is useful scenarios such as TLS operation which cannot be enabled on phones with the default PROCPSWD.	**`SET PROCPSWD X`**
Set the Vantage phone administrator password specified in the autogenerated `46xxsettings.txt` file where X is the password.	**`SET ADMIN_PASSWORD X`**
By default, the phone headset goes back on-hook when the other party disconnects. Setting this source number changes that behavior so that headset remains off-hook when the other party disconnects.	**`SET HEADSYS 1`**
Sets the timer in minutes for the phone backlight timer.	**`SET BAKLIGHTOFF 60`**

Table continues…

Description	Setting File Command

This set of commands enable the screen saver, set the name of screen saver to download and sets the name of the current downloaded file to use.	**`SET SCREENSAVERON SET`**
	`SCREENSAVER_IMAGE J179scr_svr.jpg`
	`SET SCREENSAVER_IMAGE_DISPLAY J179scr_svr.jpg`

This set of commands set the name of the background image to download and the name of the current downloaded file to use.	**`SET BACKGROUND_IMAGE J179bck_grnd.jpg`**
	`SET BACKGROUND_IMAGE_DISPLAY J179bck_grnd.jpg`

For Avaya Workplace Client on PCs and Vantage phones, L100 headsets can be used to control calls. This is enabled/disabled through the phone settings. This setting is automatically enabled in the auto-generated `46xxsettings.txt` file.	**`SET AUDIO_DEVICE_CALL_CONTROL_ENABLED 1`**

There are several **NoUser** source numbers used for remote extension. They operate differently in that they change existing values in the auto-generated settings file given to a phone when the system detects that the phone requesting the file is a remote extension. Refer to the Deploying Remote IP Office SIP Phones with an ASBCE manual.

Related links

Example additional phone settings on page 23

NoUser source numbers

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

- Since these changes are applied to the values in the auto-generated `46xxsettings.txt` file, they are overridden by any setting entered in the `46xxspecials.txt` file if present.
- There are a number of **NoUser** source number settings used for remote extensions. They operate differently in that they change existing values in the auto-generated settings file given to a phone when the system detects that the phone requesting the file is a remote extension. See the Deploying Remote IP Office SIP Phones with an ASBCE manual.

Example **NoUser** source numbers are:

- `SET_46xx_PROCPSWD=NNNNN`

  This **NoUser** source number adds the command **`SET PROCPSWD X`** to the auto-generated settings file where NNNN is the numeric password set. This password is used by 1600, 9600 and J100 Series phones.
- `SET_ADMINPSWD=NNNNN`

This **NoUser** source number adds the command **`SET ADMINPSWD X`** to the auto-generated settings file where NNNNN is the numeric password set. This password is used by Vantage phones.

- `SET_HEADSYS_1`

  This **NoUser** source number adds the command **`SET HEADSYS 1`** to the auto-generated settings file.

- `SET_BAKLIGHTOFF=N`

  This **NoUser** source number adds the command **`SET BAKLIGHTOFF N`** to the auto-generated settings file provided to a remote extension. N is the timeout in minutes.

- `ENABLE_J100_FQDN`

  Use FQDN values rather than IP addresses in the server address values provided to J100 Series phones. This requires that the FQDN values are correctly routable by the customer DNS servers and that the phones use the DNS server address (either obtained through DHCP or set manually).

- `ENABLE_J100_AUTO_UPDATE_POLICY`

  This NUSN adds settings for J100 Series phone auto-upgrade support to the system's auto-generated `46xxsettings.txt` file. See J100 Series Phone Upgrade Settings on page 127.

Related links

Example additional phone settings on page 23

Configuration File Editing

Procedure

1. Browse to the system and enter the name of the particular phone settings file required. For example: `https://192.168.42.1/46xxsettings.txt`. The auto-generated file is displayed in the browser.
   - Most Phones: `46xxsettings.txt`
   - 1100/1200 Series: `11xxsettings.txt`
   - H175: `H1xxsettings.txt`
2. Save the file as a local text file. The method will depend on your browser.
3. Using a text editor, edit the downloaded file.
4. When completed, upload the file to the file server being used by the telephones. To upload to the IP Office if that is the file server, see Loading files onto the system on page 55.
5. Restart the phone or phones in order for them to reload their files including downloading the edited settings file.

Related links

Example additional phone settings on page 23

Chapter 5: Phone operation notes

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

Related links

Account/Authorization code entry on page 28
Auto Answer on page 28
Codec Selection on page 29
Hot Desking on page 29
Conference Auto-Close on page 30
Resilience on page 30

Account/Authorization code entry

On SIP phones other than J100 stimulus 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 #.

Related links

Phone operation notes on page 28

Auto Answer

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

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

3rd Party Auto Answer Setting Value	Description
None	The extension device does not support auto answer.

Table continues…

3rd Party Auto Answer Setting Value	Description
RFC 5373	The extension device supports auto answer using an RFC 5373 header added to the call invitation message.
answer-after	The extension device supports auto answer using a 'answer-after' header message.
device auto answers	The system relies on the extension device auto answering calls. The IP Office does not indicate to the device that it should auto-answer a call.

Related links

Phone operation notes on page 28

Codec Selection

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

- On system's with B199 phones, the codec used for calls affects the maximum number of participants supported in conferences hosted by the phone. See B199 Notes on page 86.

Related links

Phone operation notes on page 28

Hot Desking

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

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

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

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

Related links

Phone operation notes on page 28

Conference Auto-Close

For J100 Series phones (except J129), when all other parties leave a conference the conference is automatically ended. However, for other types of SIP extension, the conference continues until the extension leaves.

Related links

Phone operation notes on page 28

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.

Related links

Phone operation notes on page 28

Chapter 6: Simultaneous mode

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

Related links

Simultaneous Mode Devices on page 31

Simultaneous Mode Notes on page 31

Moving Calls Between Simultaneous Devices on page 32

Simultaneous Mode Devices

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

Telephony Client	Notes
A physical desk phone	A physical phone, including a SIP, H.323 or DECT extension. This also includes clients running on a Vantage phone.
A desktop (PC) VoIP client:	• Avaya Workplace Client for Windows • Avaya Workplace Client for macOS
A mobile VoIP client:	• Avaya Workplace Client for Android • Avaya Workplace Client for iOS
A WebRTC client:	• Spaces Calling using the Chrome extension.

Related links

Simultaneous mode on page 31

Simultaneous Mode Notes

The following notes relate to the operation of simultaneous telephony:

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

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

Related links

Simultaneous mode on page 31

Moving Calls Between Simultaneous Devices

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

Action	Description
Transfer	Users can transfer calls to their own extension number. That causes the call to alert on their other simultaneous devices.
Steal	For IP Office R11.1.2.4 and higher, a **Call Steal** shortcode set to with the user's extension number will retrieve a current call from their other simultaneous device.
Workplace Clients	For IP Office R11.1.3 and higher, Avaya Workplace Client users can use their client to move and retrieve calls: • Using move, the user can send a call from their Avaya Workplace Client to their other simultaneous devices. • Using retrieve, the user can move a call answered on their simultaneous device to their Avaya Workplace Client. These features are enabled by a `SET IPO_CALL_HANDOVER_ENABLED 1` line in the `46xxsettings.txt` file.

Related links

Simultaneous mode on page 31

Part 2: Generic SIP Phone Installation Process

Chapter 7: 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:

Role	Server	Description
SIP Registrar **SIP Proxy**	IP Office	The IP Office system is the SIP registrar.
DHCP Server	IP Office	The IP Office system acts as the DHCP server. To use a separate DHCP, see Alternate DHCP server setup on page 65.
File Server	IP Office	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 on page 52.
TLS Certificates	IP Office	If TLS is enabled, the IP Office system's own default identity certificate is used. For additional options, see Security Certificates on page 69.

Related links

Generic Installation Process Options on page 35
Enabling SIP extension support on page 36
IP Office System SIP Settings on page 37
Changing the system default codec preferences on page 38
Direct Media Configuration on page 40
Setting the default extension password on page 42
DHCP settings on page 42
Configuring a basic SIP user on page 44
Configuring a SIP extension on page 45
SIP Extension Settings on page 47
Enabling SIP extension/user auto creation on page 49
Attaching the Phones on page 50

Generic Installation Process Options

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

Using manual configuration

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

1. For non-IP Office Subscription mode systems, check that the system has the appropriate licenses to support both the SIP telephone extensions (Avaya and third-party) and the extension users.
2. Enable SIP extension support
3. Adjust the system Codecs (Optional)
4. Check the system DHCP settings
5. Add SIP Users to the configuration
6. Add SIP Extensions to the configuration
7. Attach the phones

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. For non-IP Office Subscription mode systems, check that the system has the appropriate licenses to support both the SIP telephone extensions (Avaya and third-party) and the extension users.
2. Enable SIP extension support
3. Adjust the system Codecs (Optional)
4. Check the system DHCP settings
5. Enable Auto-Create Extn/User
6. Attach the phones
7. Modify the IP Office user and extension settings
8. Disable Auto-Create Extn/User

Related links

Generic installation process on page 34

Enabling SIP extension support

About this task

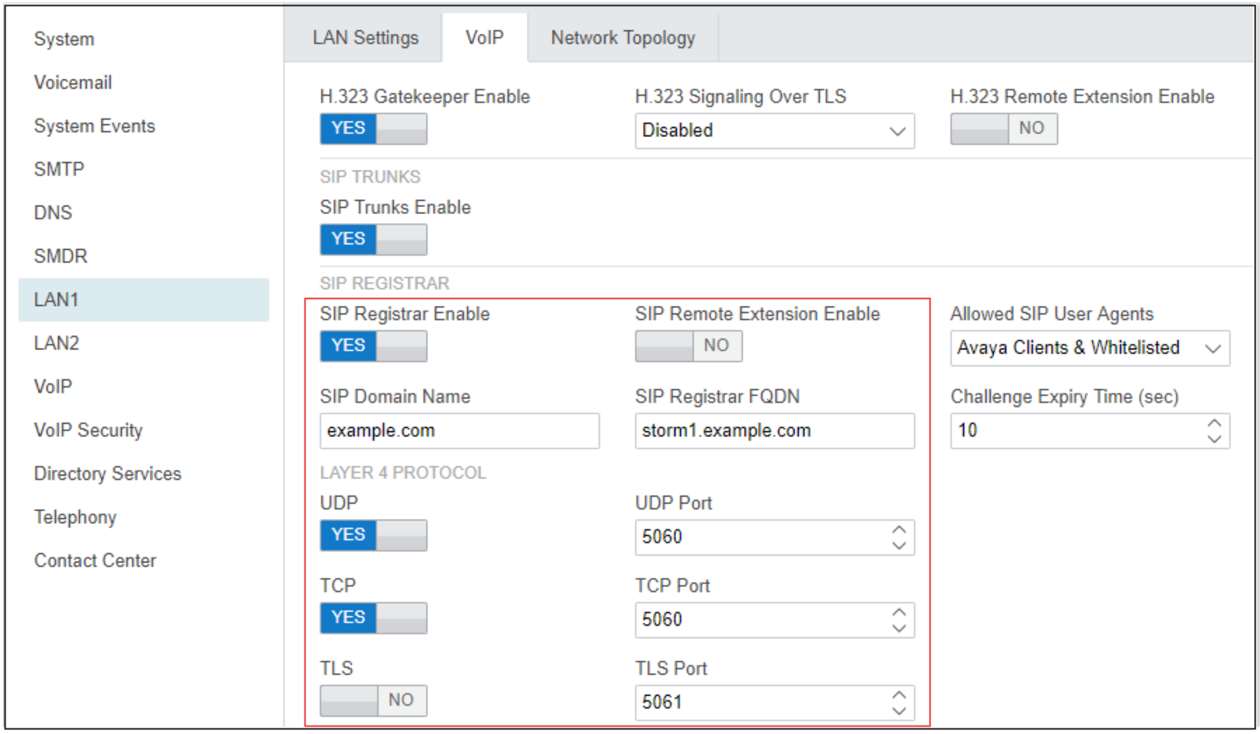
The IP Office system support SIP extensions on its LAN1 and/or LAN2 interfaces. For phone's being supported using auto-generated files, these values are included in the auto-generated settings file downloaded by the phones when they restart.

Before you begin

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

Procedure

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



H.323 Gatekeeper Enable: YES

H.323 Signaling Over TLS: Disabled

H.323 Remote Extension Enable: NO

SIP TRUNKS

SIP Trunks Enable: YES

SIP REGISTRAR

SIP Registrar Enable: YES

SIP Remote Extension Enable: NO

Allowed SIP User Agents: Avaya Clients & Whitelisted

SIP Domain Name: example.com

SIP Registrar FQDN: storm1.example.com

Challenge Expiry Time (sec): 10

LAYER 4 PROTOCOL

UDP: YES

UDP Port: 5060

TCP: YES

TCP Port: 5060

TLS: NO

TLS Port: 5061

5. Adjust the settings as required. See IP Office System SIP Settings on page 37.
6. If you have made any changes, save the configuration back to the IP Office.

Related links

Generic installation process on page 34

IP Office System SIP Settings

Setting	Description
SIP Registrar Enable	Check that SIP Registrar Enable is selected. This setting is automatically disabled on systems with no SIP extensions configured.
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. • Leaving this settings enabled is strongly deprecated. The system automatically disables the settings 24-hours after it is enabled. • Not Supported with WebLM Licensing: The auto-create extension/user options are not useable on systems using WebLM licensing.
SIP Remote Extn Enable	Default = Off Currently remote SIP extension options are only supported for Avaya SIP phones and client applications. Remote connection is not supported for third-party SIP telephones.
SIP Domain Name	Default = Blank This value is used by SIP endpoints for registration with the system. If left blank, registration uses the LAN IP address. The entry should match the domain suffix part of the **SIP Registrar FQDN** below, for example `example.com`. • For Avaya SIP telephones supported for resilience, this value must be common to all systems in the network. • If you are using TLS, this value needs to be included in the security certificates 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 the system, for example `ipoffice.example.com,` to which the SIP endpoint should send its registration and other requests. This address must be resolvable by DNS back to the IP address of the system. • For Avaya Vantage™ and Avaya Workplace Client, this field must be set. • For resilience, this value, if set on the failover server, is the value passed to Avaya Vantage™ and Avaya Workplace Client as the address for resilience. If not set, the system's IP address is sent to those clients as the failover address instead.

Table continues…

Setting	Description
Layer 4 Protocol	Default = Both TCP & UDP These fields set the transport protocol for SIP traffic between the IP Office and SIP extensions. ❗ **Important:** Do not enable a protocol unless it is intended to be used. Many phones only use the first enabled protocol that they support in the order TLS, TCP, UDP. They will not fallback to another enabled protocol if problems are encountered in the first protocol. For example, if TLS is enabled, that is indicated to phones through the IP Office's auto-generated phone settings files. The phones will then attempt to use TLS (for example requesting certificates etc) and will not fallback to TCP or UDP even if TLS operation is not fully or correctly configured.
UDP Port	Default = Enabled/5060 Select whether to support UDP for SIP and, if enabled, the port on which the system listens for extensions. The default is 5060.
TCP Port	Default = Enabled/5060 Select whether to support TCP for SIP and, if enabled, the port on which the system listens for extensions. The default is 5060.
TLS Port	Default = Disabled/5061 Select whether to support TLS for SIP and, if enabled, the port on which the system listens for extensions. 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 has been complete.
Challenge Expiry Time	Default = 10 seconds The challenge expiry time is used during SIP extension registration. When a telephone registers, the system sends back a challenge and waits for a response. If the response is not received within this timeout the registration fails.

Related links

Generic installation process on page 34

Changing the system default codec preferences

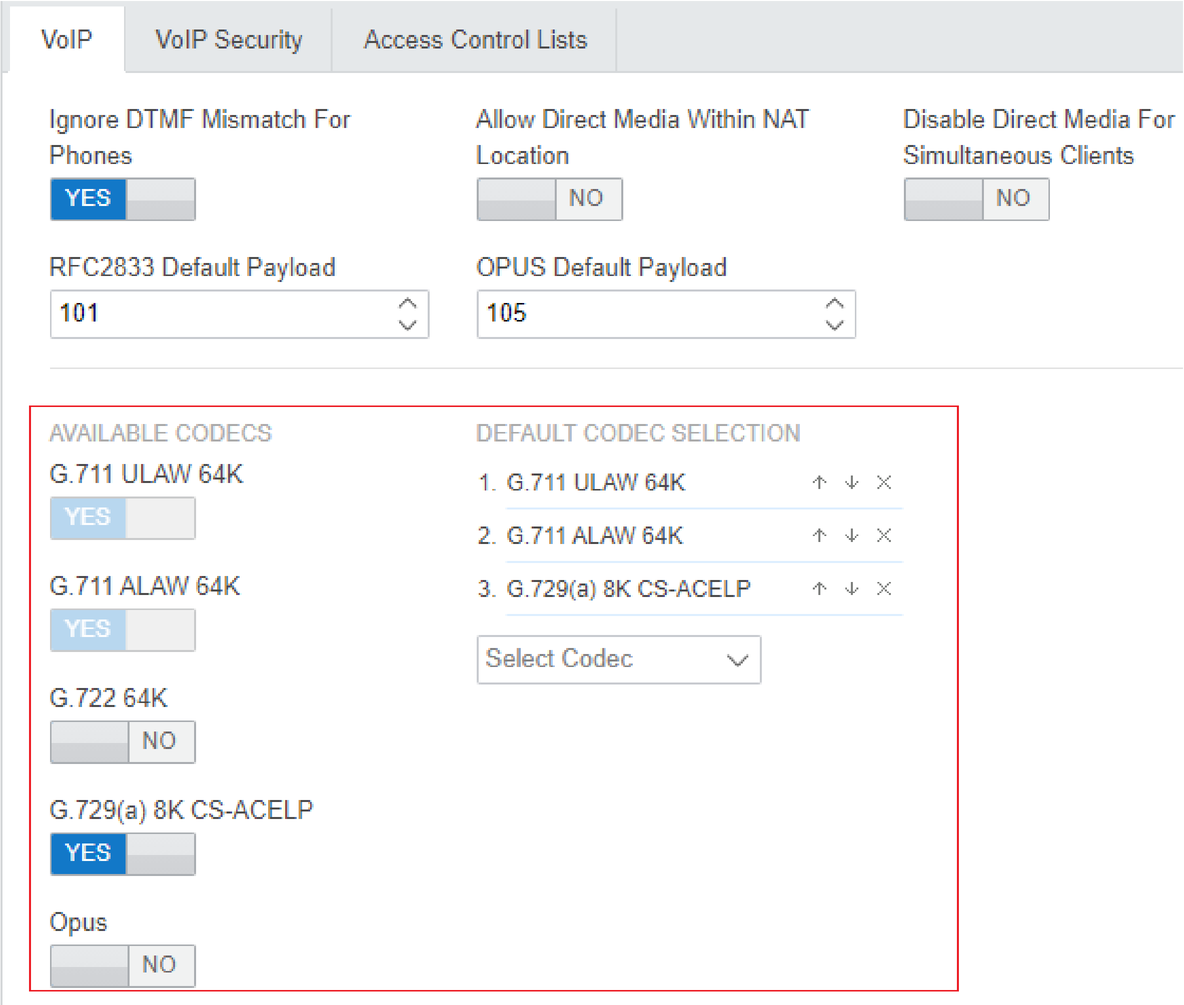
By default, all VoIP extensions added to the configuration use the system's default codec preferences. This is shown by the **Codec Selection** settings on the individual IP trunk or extension being set to **System Default**.

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

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

Procedure

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



Ignore DTMF Mismatch For Phones: YES

Allow Direct Media Within NAT Location: NO

Disable Direct Media For Simultaneous Clients: NO

RFC2833 Default Payload: 101

OPUS Default Payload: 105

AVAILABLE CODECS

G.711 ULAW 64K: YES

G.711 ALAW 64K: YES

G.722 64K: NO

G.729(a) 8K CS-ACELP: YES

Opus: NO

DEFAULT CODEC SELECTION

1. G.711 ULAW 64K
2. G.711 ALAW 64K
3. G.729(a) 8K CS-ACELP

Select Codec

4. 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 newly added IP extension and lines.

- The **AVAILABLE CODECS** list displays the codecs the system supports.
  - **G.723/G.729b:** These codecs are only supported on IP500 V2 systems.
  - **Opus:** This codec is not supported by IP500 V2 systems.
- 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.
- On system's with B199 phones, the codec used for calls affects the maximum number of participants supported in conferences hosted by the phone. See B199 Notes on page 86.
- Deselecting a codec automatically removes it from any line, system or extension codec list that are using it.

5. If these settings need to be changed, do so and then save the configuration back to the system.

Related links

Generic installation process on page 34

Direct Media Configuration

Direct media allows the media for IP calls to be routed directly between both ends of the call rather than through the IP Office system. This reduces the use of system bandwidth and other resources.

The use of direct media is subject to various checks during call setup. If these fail the call will normally fallback to routing through the system.

- Matching protocol (H323 or SIP).
- Matching codec.
- Matching security settings.
- Matching DTMF settings.

Procedure

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** > **System** or **System Settings** > **System**.
3. Select **VoIP**.
4. The following settings affect the system's use of direct media:

Setting	Description
Ignore DTMF Mismatch For Phones	Default = On When enabled, the system's SIP (and H323) extension settings includes a **Requires DTMF** setting. If for an extension, that setting is off (the default), then DTMF checking is ignored on calls between two IP phones when determining whether direct media is allowed.
Allow Direct Media Within NAT Location	Default = Off. When enabled, the system allows direct media between devices that reside behind the same NAT. That is, devices appear to the system with the same public IP address. The default is to apply this setting to both H323 and SIP remote workers and to IP Office lines. For some routers, such as those with H323 or SIP ALG, it may be desirable to only allow direct media only between certain types of device. This can be configured by adding a `MEDIA_NAT_DM_INTERNAL=X` setting to the system's **NoUser** user **Source Numbers**. The value `X` is the sum of the following: • 1 = Include H323 phones. • 2 = Include SIP phones. • 4 = Include IP Office lines. For example, if the router has SIP ALG that can't be disabled, you can disable NAT direct media for SIP devices using `MEDIA_NAT_DM_INTERNAL=5` to include only H323 phones and IP Office lines.
Disable Direct Media For Simultaneous Clients	Default = Off (Use direct media) For IP deskphones, the **Allow Direct Media Path** setting of the extension entry in the IP Office configuration sets whether the device attempts to use direct media. Simultaneous clients, such as Avaya Workplace Client, can be used with having a extension entry in the system configuration. In that case, this setting controls whether those clients attempt to use direct media.

5. If these settings need to be changed, do so and then save the configuration back to the system.

Related links

Generic installation process on page 34

Setting the default extension password

About this task

Registration of most SIP phones requires entry of a password. The password can either be set against the individual extension entry in the system configuration (see Configuring a SIP extension on page 45) or using the system's **Extension Default Password** setting below.

The auto-create extension settings in a system cannot be enabled until this value is set. It is then used as the password for any auto-created extensions.

Procedure

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** > **System** or **System Settings** > **System**.
3. Select **VoIP**.
4. Select **VoIP Security**.
5. In the **Extension Default Password** section set the password as required. The password can be between 9 to 13 digits (0-9) in length.
6. If you have changed the password, save the settings.

Related links

Generic installation process on page 34

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 on page 65.
- 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.

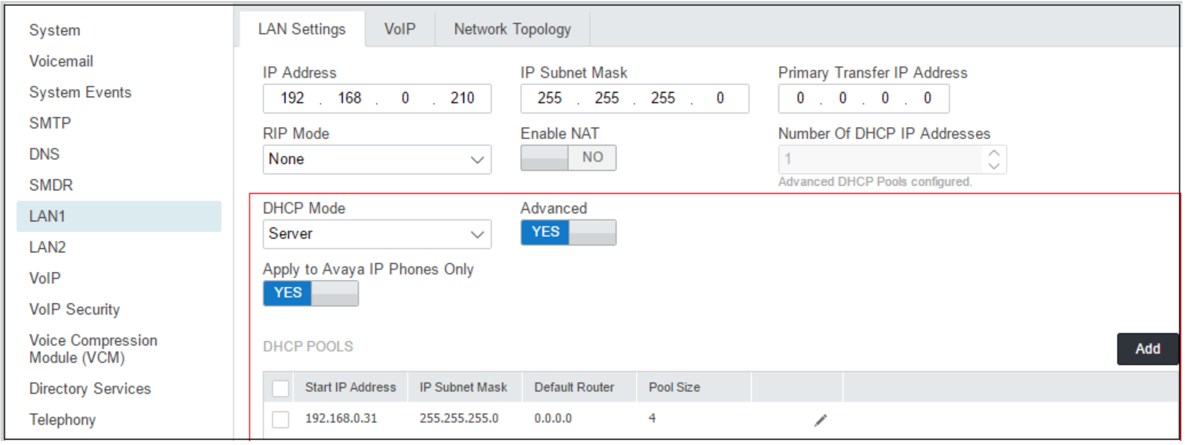
Related links

Generic installation process on page 34
Changing the system's DHCP settings on page 43
Changing the system's SSON settings on page 43

Changing the system's DHCP settings

Procedure

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



IP Address: 192 . 168 . 0 . 210
IP Subnet Mask: 255 . 255 . 255 . 0
Primary Transfer IP Address: 0 . 0 . 0 . 0
RIP Mode: None
Enable NAT: NO
Number Of DHCP IP Addresses: 1
Advanced DHCP Pools configured.
DHCP Mode: Server
Advanced: YES
Apply to Avaya IP Phones Only: YES

DHCP POOLS

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

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

Related links

DHCP settings on page 42

Changing the system's SSON settings

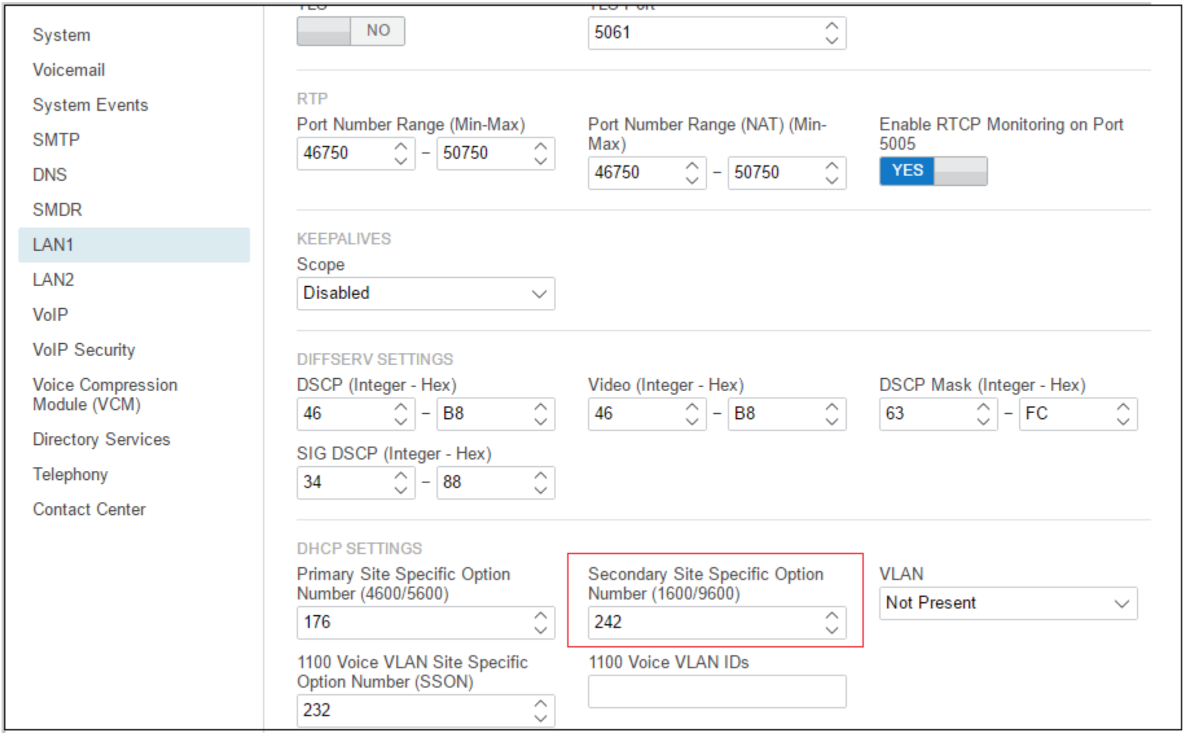
When requesting address settings from a DHCP server, each phone also requests additional information that the DHCP server may have. It does this by sending a Site Specific Option Number (SSON) request. If the DHCP server has information matching the requested SSON, that information is included in the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

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

Procedure

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.

2. Select **System** > **System** or **System Settings** > **System**.
3. Select **LAN1** or **LAN2** as required.
4. Select the **VoIP** tab.



NO

5061

RTP

Port Number Range (Min-Max): 46750 – 50750

Port Number Range (NAT) (Min-Max): 46750 – 50750

Enable RTCP Monitoring on Port 5005: YES

KEEPALIVES

Scope: Disabled

DIFFSERV SETTINGS

DSCP (Integer - Hex): 46 – B8

Video (Integer - Hex): 46 – B8

DSCP Mask (Integer - Hex): 63 – FC

SIG DSCP (Integer - Hex): 34 – 88

DHCP SETTINGS

Primary Site Specific Option Number (4600/5600): 176

Secondary Site Specific Option Number (1600/9600): 242

VLAN: Not Present

1100 Voice VLAN Site Specific Option Number (SSON): 232

1100 Voice VLAN IDs:

5. 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.
6. If this setting needs to be changed, save the configuration back to the system.

Related links

DHCP settings on page 42

Configuring a basic SIP user

About this task

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

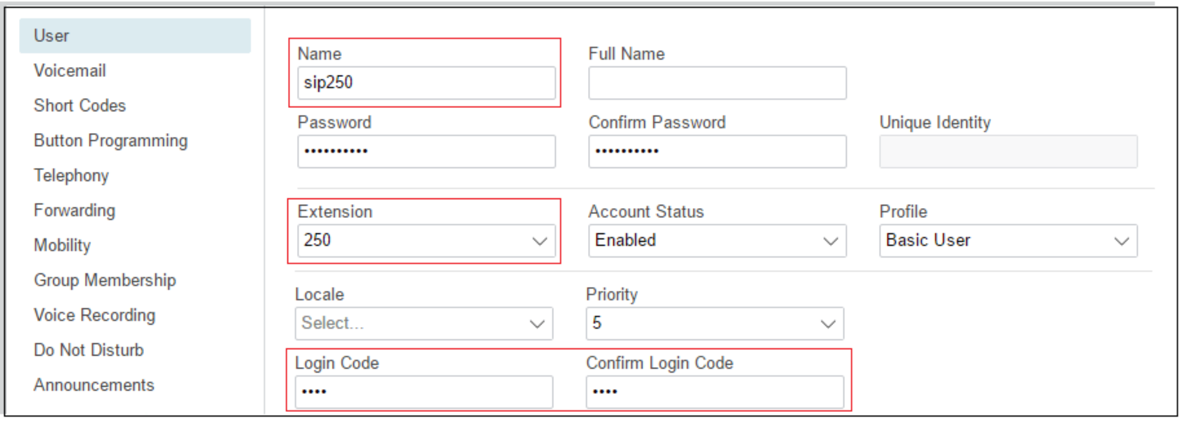
Procedure

1. Using either IP Office Manager or IP Office Web Manager, load the system configuration.
   - If using IP Office Manager:
     a. To edit an existing user, select the existing user record.

   b. To add a new user , select the system on which the user record should be created and then select > **User**.

- If using IP Office Web Manager:
   a. Select **Call Management** > **Users**.
   b. To edit an existing user, click the ✎ icon next to the user.
   c. To add a new user, click **+Add User** and select the system on which the user record should be created.

2. Configure the user settings.



Name	Full Name	
sip250		
Password	Confirm Password	Unique Identity
••••••••••	••••••••••	
Extension	Account Status	Profile
250	Enabled	Basic User
Locale	Priority	
Select...	5	
Login Code	Confirm Login Code	
••••	••••	

3. Select **Extension**

   This should match the **Base Extension** setting of the SIP extension in the IP Office configuration.

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

Related links

Generic installation process on page 34

Configuring a SIP extension

About this task

This section looks just at the key configuration settings that affect SIP extensions. For full details of all the fields shown, refer to the Administering Avaya IP Office™ Platform with Web Manager.

Procedure

1. Using either IP Office Manager or IP Office Web Manager, load the system configuration.
   - If using IP Office Manager:
      a. Select the system on which the extension record should be created.

b. Select **SIP Extension**.

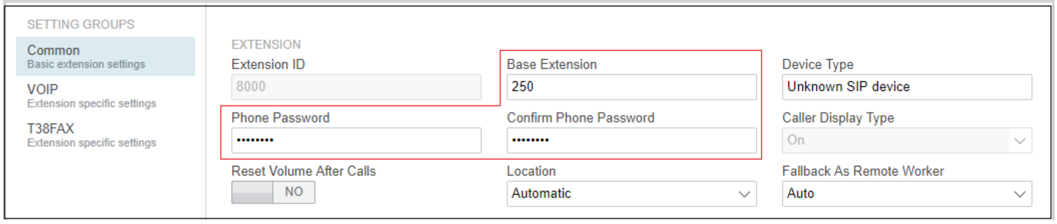
- If using IP Office Web Manager

a. Select **Call Management** > **Extensions**.

b. Click **+Add Extension**.

c. Select SIP Extension and the system on which the extension record should be created and click **OK**.

2. Configure the extension settings.



SETTING GROUPS

Common
Basic extension settings

VOIP
Extension specific settings

T38FAX
Extension specific settings

EXTENSION

Extension ID: 8000

Base Extension: 250

Device Type: Unknown SIP device

Phone Password: ••••••••

Confirm Phone Password: ••••••••

Caller Display Type: On

Reset Volume After Calls: NO

Location: Automatic

Fallback As Remote Worker: Auto

a. Enter **Base Extension**.

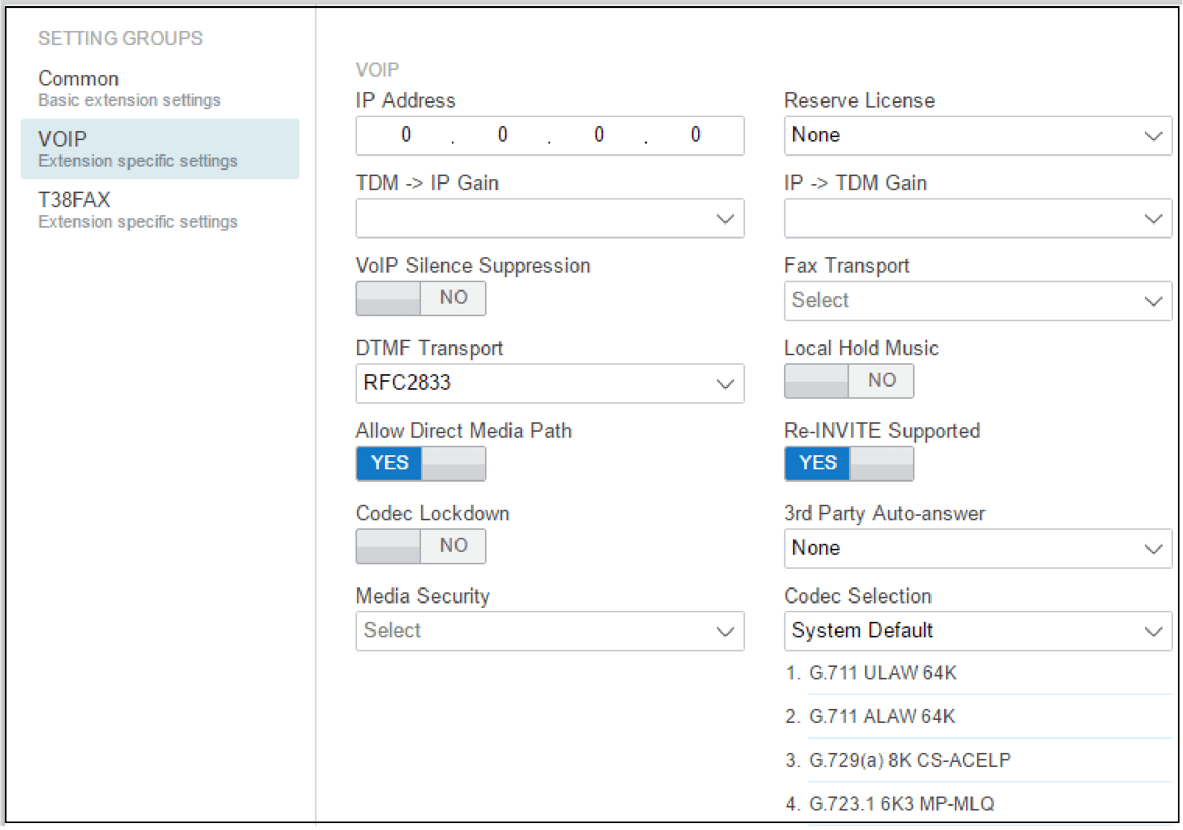
This should match the Extension setting of the SIP user added to the IP Office configuration.

b. Enter a **Phone Password**. This password is used for the extension registration.

Warning:

For J100 phones, the extension **Phone Password** must be used for initial registration of the telephone.

3. Select **VoIP**. See SIP Extension Settings on page 47.



SETTING GROUPS

Common
Basic extension settings

VOIP
Extension specific settings

T38FAX
Extension specific settings

VOIP

IP Address: 0 . 0 . 0 . 0

Reserve License: None

TDM -> IP Gain:

IP -> TDM Gain:

VoIP Silence Suppression: NO

Fax Transport: Select

DTMF Transport: RFC2833

Local Hold Music: NO

Allow Direct Media Path: YES

Re-INVITE Supported: YES

Codec Lockdown: NO

3rd Party Auto-answer: None

Media Security: Select

Codec Selection: System Default

1. G.711 ULAW 64K
2. G.711 ALAW 64K
3. G.729(a) 8K CS-ACELP
4. G.723.1 6K3 MP-MLQ

Related links

Generic installation process on page 34

SIP Extension Settings

Function	Description
IP Address	The IP address of the phone. The default setting accepts connection from any address. If an address is entered, registration is only accepted from that address.
Codec Selection	If left set to **System Default**, the extension uses the system's default codec preferences (see Changing the system default codec preferences on page 38). This is the recommended setting as it ensures consistency for all IP trunks and extensions.

Table continues…

Function	Description
Reserve License	For non-IP Office Subscription mode systems, Avaya IP desk phones require an **Avaya IP Endpoint**IP Endpoint license, non-Avaya IP phones require a **3rd Party IP Endpoint** license. Normally the available licenses are issued in the order that extensions register. This option allows an extension to be pre-licensed before the extension has registered. On system's using WebLM licensing, this option is fixed to reserve a license.
TDM->IP Gain	These settings are only available on IP500 V2 systems. They allow adjustment of the gain on audio between the system's TDM (non-IP telephony) interface and IP connections.
IP->TDM Gain	
DTMF Transport	This can be set to one of the two common methods used by SIP devices; **RFC2833** or **Inband**. The selection should be set to match the method used by the SIP extension.
Requires DTMF	Default = Off This setting is shown when the system setting **Ignore DTMF Mismatch For Phones** is enabled (the default). It sets whether, on calls between two phones, matching DTMF should be included in the checks for direct media support.
3rd Party Auto Answer	System functions such as paging are only supported to extensions that can auto-answer calls. For 3rd-party SIP extensions the ability to auto answer and the method used to enable that function may vary and needs to be configured. • **None**: The extension device does not support auto answer. • **RFC 5373**: The extension device supports auto answer using an RFC 5373 header added to the call invitation message. • **answer-after**: The extension device supports auto answer using a 'answer-after' header message. • **device auto answers**: The system relies on the extension device auto answering calls. That is, it does not specifically indicate to the phone to that the call should be auto answered.
Media Security	These settings allow the adjustment of the settings for SRTP security if used. Normally these are adjusted at the system level for the whole system rather than at the individual extension level.
VoIP Silence Suppression	When selected, this option detects periods of silence during a call and does not send any data during those silences. IP500 V2 systems only.
Local Hold Music	Select this option if the SIP device supports its own hold music source.
Re-invite Supported	If the SIP device is able to receive REINVITE messages select this option. This option should be selected for extensions that support video as it is necessary to enable switching between audio only and video operation.

Table continues…

Function	Description
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 occurs 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 calls to another IP device must be routed via the IP Office system or can be routed directly between the devices. For more details, see Direct Media Configuration on page 40. • If enabled, IP calls can take routes other than through the IP Office system. • If disabled, or not supported at on one end of the call, the call is routed via the system.

Related links

Generic installation process on page 34

Enabling SIP extension/user auto creation

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

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

⚠ **Warning:**

Leaving this settings enabled is strongly deprecated. The system automatically disables the settings 24-hours after it is enabled.

- Not Supported with WebLM Licensing: The auto-create extension/user options are not useable on systems using WebLM licensing.
- Reboot Required: Note that changing the SIP registrar settings of an IP Office system requires the IP Office system to be rebooted.

Procedure

1. Auto-creation cannot be enabled until the **Extension Default Password** has been set. See Setting the default extension password on page 42.

2. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
3. Select **System** > **System** or **System Settings** > **System**.
4. Select **LAN1** or **LAN2** as required.
5. Select the **VoIP** tab.
6. Change the **Auto-create Extn/User** settings to the state required.
7. Save the configuration back to the IP Office.

Related links

Generic installation process on page 34

Attaching the Phones

About this task

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:

Procedure

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 its file storage.
    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.
    - 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. When prompted for a `username` or similar, enter the IP Office user's `Extension` number.
7. When prompted for a `password` or similar, enter the **Phone Password** set for the extension entry in the configuration. .

Related links

Generic installation process on page 34

Chapter 8: 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 is supported for settings and upgraded text files for supported Avaya SIP phones.
- If either of the options above are not acceptable, a 3rd party HTTP/HTTPS file server is required. The necessary phone firmware and settings files need to be loaded onto that server.
- Avaya H175 and Vantage phones always require a separate 3rd-party HTTP/HTTPS files server to host and deliver their firmware. They can accept settings files, including auto-generated settings files, from the IP Office system as their file server, but the system will redirect their request for firmware files to the system's configured **HTTP Server IP Address** or **HTTP Server URI** address.

Related links

Changing the file server settings on page 53
System settings for file server support on page 53
Loading files onto the system on page 55
Loading files onto a third party server on page 59
Adding additional MIME file types on page 59

Changing the file server settings

About this task

If the IP Office system is being used for DHCP support 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.

Procedure

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** > **System** or **System Settings** > **System**.
3. Check the file server settings. See System settings for file server support on page 53 for details of the individual settings. These are used in DHCP responses provided by the system and when the system is asked to provide files.
4. If any changes have been made, save the configuration back to the system.

Related links

File (Provisioning) server settings on page 52

System settings for file server support

The following IP Office system settings relate to support of file requests from phones including SIP phones.

Setting	Description
Phone File Server Type This setting sets the location used for files requested by phones.	
Memory Card (IP500 V2)	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.
Disk (IP Office Server Edition)	
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** > **Enable BootP and TFTP Server**.
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.

Table continues…

Setting	Description
The remaining settings are used to customize the operation.	
HTTP Server IP Address	This field is used if the **Phone File Server Type** is set to **Custom**. It is also used if **HTTP Redirection** is set to **Phone Binaries**. • When used, this server address is used for file requests by devices on both LAN1 and LAN2. Therefore, the address must be reachable by devices on both LAN. If necessary additional network configuration and or addition of IP route settings are required. • B199, H175 and Vantage phones use this address for their firmware (`.kt`, `.sig`, `.tar`) and application (`.apk`) files regardless of the **HTTP Redirection** setting. • The **PUBLIC_HTTP** NoUser source number can be used to provide a separate address to remote worker connected phones.
HTTP Server URI	This field is used for IP Office subscription mode systems and is normally automatically configured to the required address during the system's initial subscription. • If set, it is used to redirect requests for Vantage™ phone firmware and Workplace client software. • If not set, those clients use the **HTTP Server IP Address**.
HTTP Redirection	Default = Off Allows firmware requests made to the IP Office from certain types of phone to be redirected to an alternate HTTP file server. This option is supported for: • Supported for 9600 Series and J100 Series (except J129) phones. • B199, H175 and Vantage phones use HTTP redirection regardless of whether this setting is enabled or not. - Supported for B199 phones running B199 R1.0 FP6 or higher firmware. Note: • This field is only available when the **Phone File Server Type** is set to **Memory Card** or **Disk**. • The alternate file server address is set by the **HTTP Server IP Address** setting.

Table continues…

Setting	Description
Use Preferred Phone Ports	This setting can be used to reduce the use of the HTTP/HTTPS ports configured in the system's security configuration (by default ports 80 and 443) for phone file requests. The system will still provide files on those ports in order to support legacy phones but its auto-generated file response directs newer phones to use ports 441 and 8441. • When not enabled: - Auto-generated phone settings files provided by the system to local phones indicate the ports 80/411 or 80/443 depending on the phone type. - Auto-generated phone settings files provided by the system to remote phones indicate the ports 8411/411 or 8411/443 depending on the phone type. • When enabled: - Auto-generated phone settings files for locale phones will indicate port 8411 for HTTP and 411 for TLS.
Avaya HTTP Clients Only	This option can be used to restrict the system to responding to file requests from Avaya phones and applications only. • This option should not be used if the system is also supporting 1100 and or 1200 Series phones.

Related links

File (Provisioning) server settings on page 52

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 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.

Related links

File (Provisioning) server settings on page 52
Manually copying files on page 56
Using manager to upload files on page 57
Using web manager to upload files on page 58

Manually copying files

About this task

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.

Procedure

1. First shutdown the memory card using IP Office Manager or IP Office Web Manager:
   - IP Office Web Manager:
     a. Click **Solution**.
     b. Click **Actions** and select **Service Commands** > **Memory Card Stop** > **System**.

     and click **OK**.
   - IP Office Manager:
     a. Select **File** > **Advanced** > **Memory Card Command** > **Shutdown**.

        The **Select IP Office** menu is displayed.

     b. 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/primary` folder.

Next steps

When the card is reinserted into the system, card usage is automatically restarted.

Related links

Loading files onto the system on page 55

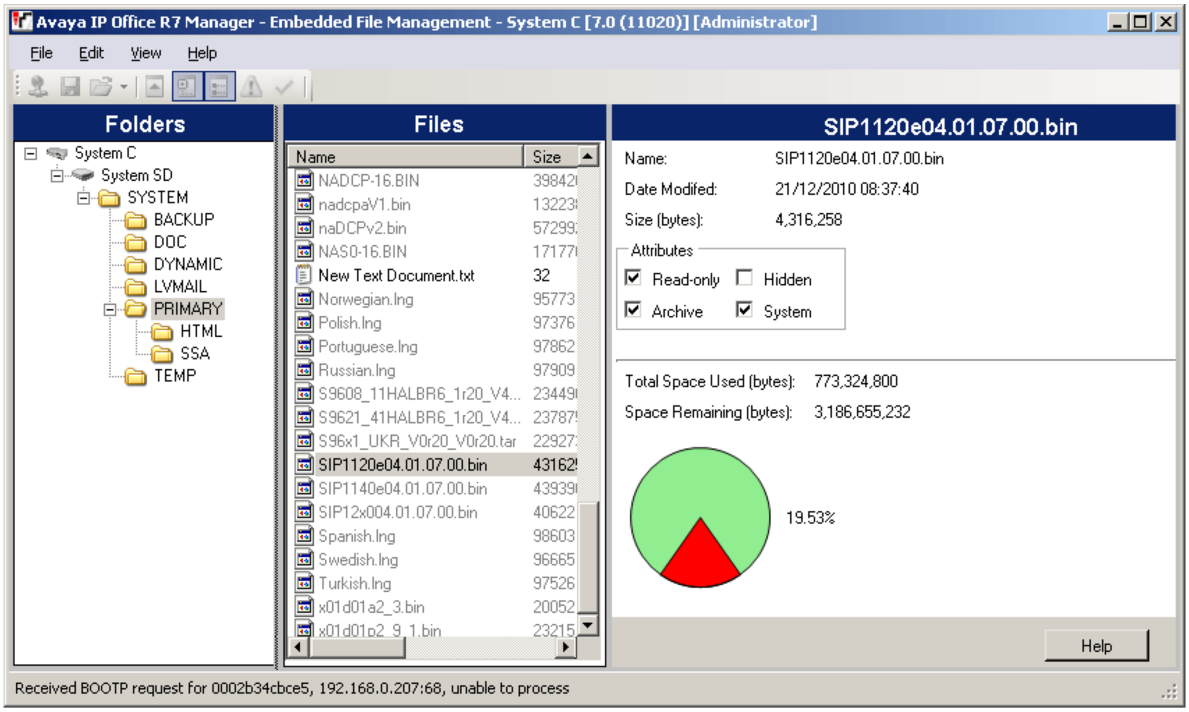
Using manager to upload files

About this task

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

Procedure

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



Name	Size
NADCP-16.BIN	39842
nadcpaV1.bin	13223
naDCPv2.bin	57299
NAS0-16.BIN	17177
New Text Document.txt	32
Norwegian.lng	95773
Polish.lng	97376
Portuguese.lng	97862
Russian.lng	97909
S9608_11HALBR6_1r20_V4...	23449
S9621_41HALBR6_1r20_V4...	23787
S96x1_UKR_V0r20_V0r20.tar	22927
SIP1120e04.01.07.00.bin	43162
SIP1140e04.01.07.00.bin	43939
SIP12x004.01.07.00.bin	40622
Spanish.lng	98603
Swedish.lng	96665
Turkish.lng	97526
x01d01a2_3.bin	20052
x01d01p2_9_1.bin	23215

Name: SIP1120e04.01.07.00.bin
Date Modifed: 21/12/2010 08:37:40
Size (bytes): 4,316,258

Attributes
☑ Read-only ☐ Hidden
☑ Archive ☑ System

Total Space Used (bytes): 773,324,800
Space Remaining (bytes): 3,186,655,232

19.53%

Received BOOTP request for 0002b34cbce5, 192.168.0.207:68, unable to process

4. 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`.

5. 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**.

Related links

[Loading files onto the system](#) on page 55

Using web manager to upload files

About this task

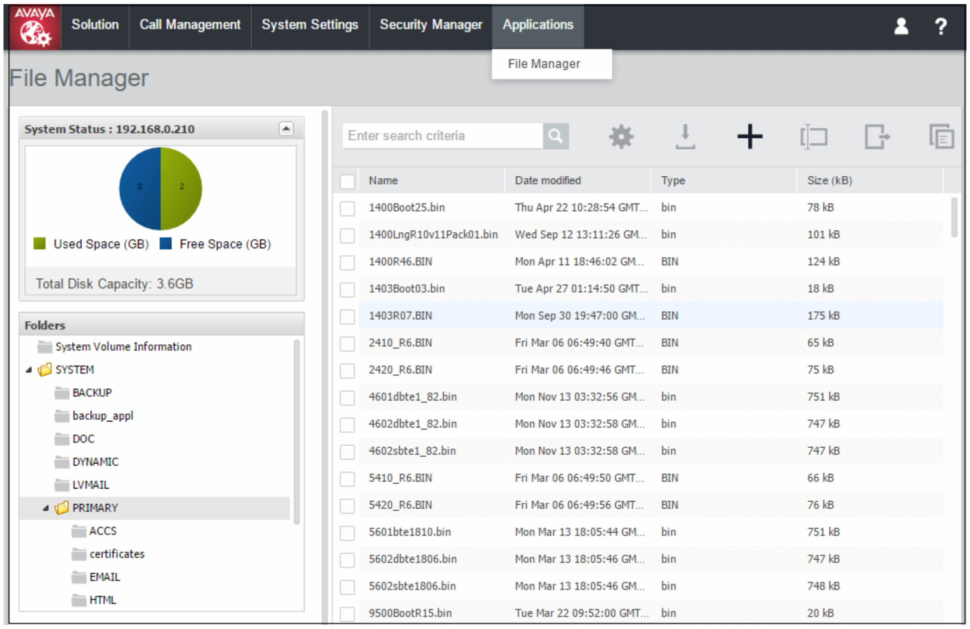
Within IP Office Web Manager you can use file manager to view files and if necessary upload new files.

Before you begin

This process is not supported in Chrome.

Procedure

1. Log into the system using IP Office Web Manager.
2. Click **Applications** and select **File Manager**.



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

3. Open the `/system/primary` or `/disk/system/primary` folder.
4. Click on the **+** icon to upload a new file.
5. Browse for and select the file to upload. Click **Upload File**.

Related links

[Loading files onto the system](#) on page 55

Loading files onto a third 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`.

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

Related links

File (Provisioning) server settings on page 52

Adding additional MIME file types

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

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

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

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

Related links

File (Provisioning) server settings on page 52
Adding a MIME type to an IIS server on page 59
Adding a MIME type to an IIS sever configuration file on page 60
Adding a MIME type to an apache server on page 60
Vantage installation on page 143

Adding a MIME type to an IIS server

Procedure

1. Open the **Internet Information Services (IIS) Manager**.

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

Related links

Adding additional MIME file types on page 59

Adding a MIME type to an IIS sever configuration file

Procedure

1. Locate the server's configuration file.

   For example `C:\Windows\System32\inetsrv\config\applicationHost.config`.

2. Add the additional MIME types required to the **<staticContent>** section.

   For example

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

Related links

Adding additional MIME file types on page 59

Adding a MIME type to an apache server

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

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

Related links

Adding additional MIME file types on page 59

Chapter 9: Phone registration control

The system provides a number of methods to control which SIP phones and devices can register with it.

Related links

Disabling registrars on page 61
IP Address/Extension Blacklisting on page 61
Blocking default passcodes on page 62
User Agent Control on page 62
Editing the SIP User Agent lists on page 63

Disabling registrars

As a general principal, the system's SIP Registrar options should only be enabled when required to support SIP telephones.

By default the registrars are disabled and warnings are displayed if they are enable in a configuration that does not include SIP extensions.

Related links

Phone registration control on page 61

IP Address/Extension Blacklisting

The system logs failed H323/SIP registration requests. Multiple failed attempts can lead to the extension and/or IP address being blocked from further registration attempts for 10 minutes.

Blocking applies as follows:

Blocking Method	Description
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.

Table continues…

Blocking Method	Description
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. • The system's **IP Whitelist** is used to set IP addresses which should not be blocked. See Editing the SIP User Agent lists on page 63.

- When blocking occurs:
  - The system generates an alarm in System Status Application
  - It 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).
- SysMonitor can display details of blacklisted IP addresses and extensions, select **Status** > **Blacklisted IP Addresses** and **Status** > **Blacklisted Extensions**.

Related links

Phone registration control on page 61

Blocking default passcodes

About this task

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

Procedure

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

Related links

Phone registration control on page 61

User Agent Control

In addition to automatic IP address and extension number blacklisting, the system can apply registration control based on the UA (user agent) string that the registering devices provides.

- These settings are not available on IP500 V2/V2A systems.
- These settings are applied to new registration only, not to keep-alive or unregistration requests. When blocking is applied the system does not respond to the registration request.

Procedure

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** > **System** or **System Settings** > **System**.
3. Select **LAN1** or **LAN2** as required.
4. Select the **VoIP** tab.
5. Select the required method of User Agent control in the **Allowed SIP User Agents** setting.

Setting	Description
Allow All	Allow registration from any user agent.
Block Blacklist Only	This is the default setting for systems. It allows registration from any user agent not listed in the system's **SIP UA Blacklist** (see Editing the SIP User Agent lists on page 63). Registration is also blocked if no user agent is presented.
Avaya Clients & White Listed	Only allow registration for Avaya user agents and those user agents listed in the system's **SIP UA Whitelist**.
Avaya Clients Only	Only allow registration from Avaya user agents.
Whitelisted Only	Only allow registration from user agents listed in the system's **SIP UA Whitelist**.

6. Save the settings.

Related links

Phone registration control on page 61

Editing the SIP User Agent lists

The SIP User Agent lists are used by the user agent control settings. See User Agent Control on page 62.

Procedure

1. Using either IP Office Manager or IP Office Web Manager in offline mode, load the system configuration.
2. Select **System** > **System** or **System Settings** > **System**.
3. Select **LAN1** or **LAN2** as required.
4. Select the **VoIP** tab.
5. Select **Access Control Lists**. The lists are:

Setting	Description
SIP UA Blacklist	This list is used when the LAN **Allowed SIP User Agents** setting is set to blacklist matching entries. • This option is not supported on IP500 V2 systems.
SIP UA Whitelist	This list is used when the LAN **Allowed SIP User Agents** setting is set to only allow recognized user agents. • This option is not supported on IP500 V2 systems.
IP Whitelist	This list can be used to set IP addresses that should not be automatically blacklisted by the system (see IP Address/Extension Blacklisting on page 61). This may be useful when multiple clients frequently register from behind the same IP address. • For R11.1 FP2 and higher, this option is supported on IP500 V2 systems.

6. To edit the lists as required. You can enter a partial string for left-to-right string matching.
7. Save the settings.

Related links

Phone registration control on page 61

Chapter 10: 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)

Related links

Checking for DHCP server support on page 65
Creating a scope on page 66
Adding an option on page 67
Activating the Scope on page 68

Checking for DHCP server support

Procedure

1. On the server, select **Start** > **Program** > **Administrative Tools** > **Computer Management**.
2. Under **Services and Applications** in the Computer Management Tree, locate **DHCP**.

   If DHCP is not present then you need to install the DHCP components. Refer to the Microsoft documentation.
3. Create a scope of addresses for use by IP phones. See Creating a scope on page 66.

Related links

Alternate DHCP server setup on page 65

Creating a scope

About this task

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.

Procedure

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
7. Click **Next**.
8. You can specify addresses to be excluded. Enter a range.

   For example 200.200.200.5 to 200.200.200.7
9. Click **Add**.

   - You can also enter a single address and click **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.
10. Click **Next**.
11. 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.
12. Click **Next**.

    The wizard gives the option to configure the most common DHCP options.
13. Select **Yes** and then click **Next**.
14. Enter the address of the gateway and click **Add**.

    You can enter several addresses.

15. Click **Next**.
16. Enter the DNS domain (eg. example.com) and the DNS server addresses.
17. Click **Next**.
18. Enter the WINS server addresses and click **Add** and then click **Next**.
19. You will then be asked if you wish to activate the scope. Select **No** and then click **Next**.
20. Click **Finish**.

    The new scope will now be listed and the status is set to **Inactive**.

Result

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

Related links

Alternate DHCP server setup on page 65

Adding an option

About this task

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 option should include defining the address of the phone's file server.

Procedure

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.

    ```
    HTTPSRVR=xxxx, HTTPPORT=y, HTTPDIR=z
    ```

String	Role
`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.

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, enter the option number. For example 242.
12. Verify the String value is correct and click **OK**.

Next steps

Having created a 242 option and associated with the scope we want used by the IP phones, we now need to activate the scope. See Activating the Scope on page 68.

Related links

Alternate DHCP server setup on page 65

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.

Related links

Alternate DHCP server setup on page 65

Chapter 11: 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 Trusted Certificate Store on page 71.
- **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.
  - **Option 2:** 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

Related links

Using the IP Office Certificate on page 69

Adding a root CA certificate to the IP Office Trusted Certificate Store on page 71

Create an identity certificate for the IP Office on page 72

Adding the identity certificate to the IP Office on page 74

File server certification on page 74

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.
- Downloading the IP Office certificate from a Linux based IP Office.

Related links

Security Certificates on page 69
Downloading the Linux certificate on page 70
Downloading the IP500 V2 certificate on page 71

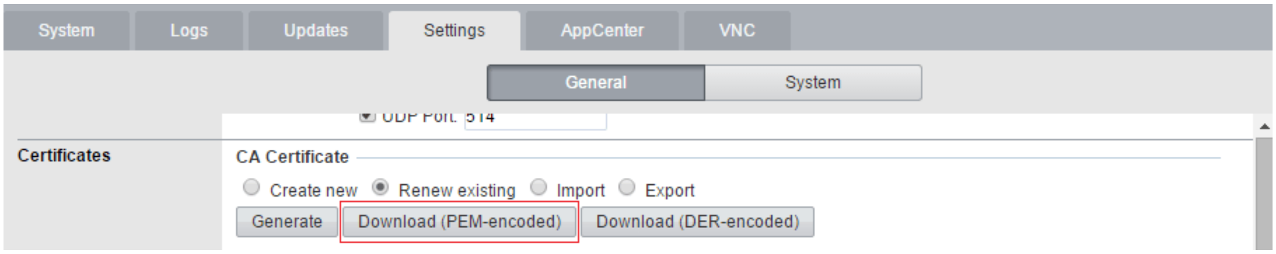
Downloading the Linux certificate

About this task

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.

Procedure

1. Browse to the IP Office system IP address and select IP Office Web Manager. For example, IP address: `https://<server_address>`
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 40 being used by the phones.

Related links

Using the IP Office Certificate on page 69

Downloading the IP500 V2 certificate

About this task

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.

Procedure

1. Browse to the IP Office system IP address. For example IP address is `https://<server address>`.
2. From the web page select IP Office Web Manager and login to the system.
3. From **Security Manager**. click **Certificates**.
4. Click **Export** to download the system's certificate file.
5. Rename the file as **WebRootCA.pem**. This is the default name set in the settings file using the **TRUSTCERTS** parameter.
6. Upload the file to the file server being used by the phones.

Related links

Using the IP Office Certificate on page 69

Adding a root CA certificate to the IP Office Trusted Certificate Store

About this task

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 perform the following:

Procedure

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

Related links

Security Certificates on page 69
Adding a certificate using file manager on page 72

Adding a certificate using file manager

About this task

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

- Using one of the methods for loading files onto the system , add the certificate to the `/SYSTEM/PRIMARY/certificates/TCS/ADD` folder. See Loading files onto the system on page 55.

Related links

Adding a root CA certificate to the IP Office Trusted Certificate Store on page 71

Create an identity certificate for the IP Office

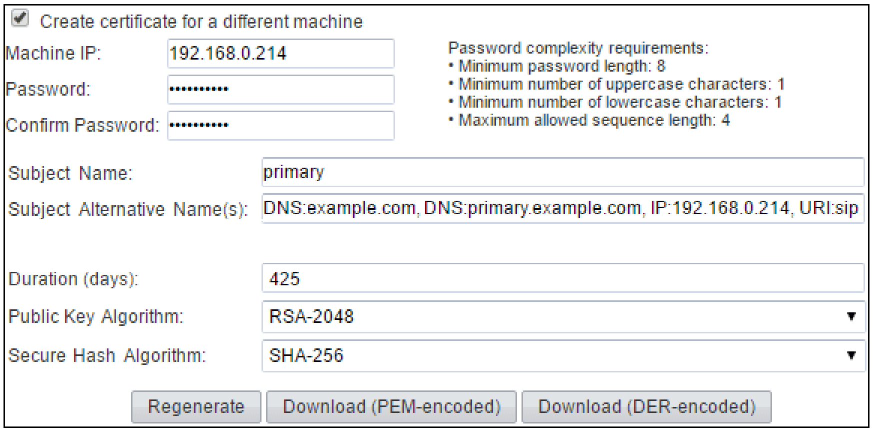
About this task

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.

Procedure

1. Within the server's web management menus, select **Platform View**.
2. Select **Settings** and then **General**.

3. Locate the **Certificates** section and select **Create certificate for a different machine**.



☑ Create certificate for a different machine

Machine IP: 192.168.0.214

Password: ••••••••••

Confirm Password: ••••••••••

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

Subject Name: primary

Subject Alternative Name(s): DNS:example.com, DNS:primary.example.com, IP:192.168.0.214, URI:sip

Duration (days): 425

Public Key Algorithm: RSA-2048

Secure Hash Algorithm: SHA-256

4. Enter the details for theIP Office's SIP server. Enter the **Subject Alternative Name(s)** in the following format:

   The 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.
     - For example: `DNS:example.com`
   - DNS entries for the system's LAN1 and/or LAN2 SIP Registrar FQDN.
     - For example: `DNS:ipoffice.example.com`
   - IP entries for the system's LAN1 and/or LAN2 IP addresses.
     - For example: **`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.
     - For example: `URI:sip:example.com`
   - SIP URI entry for the LAN1 and/or LAN2 IP address.
     - For example: `URI:sip:192.168.42.1`
   - If using a separate HTTPS file server, add a SIP URI entry for the file server's domain name.
5. Click on the lower **Regenerate** button.
6. Click on **Download (PEM-encoded)** to download the file.

Related links

Security Certificates on page 69

Adding the identity certificate to the IP Office

Procedure

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 the **Certificates**.
     b. Click **Set**.
2. Select the previously generated IP Office identity file and load it.

Result

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.

Related links

Security Certificates on page 69

File server certification

The same root CA certificate added to the IP Office system 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.

Related links

Security Certificates on page 69
Enabling the certificates snap-in on page 74
Adding the trusted root CA certificate to the windows certificate store on page 75
Create an identity certificate for the file server on page 75
Adding an identity certificate to a Microsoft IIS server on page 76

Enabling the certificates snap-in

About this task

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

Procedure

1. Click the **Start** .

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 MCC.

Related links

File server certification on page 74

Adding the trusted root CA certificate to the windows certificate store

Procedure

1. Click the **Start**.
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.

Related links

File server certification on page 74

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.

Related links

[File server certification](#) on page 74
[Creating an IP Office identity certificate for file server](#) on page 76

Creating an IP Office identity certificate for file server

About this task

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.

Procedure

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. Enter the details of the computer.

   For 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`
5. Click on the lower **Regenerate** button.
6. Click on **Download (PEM-encoded)** to download the file.

Result

The identity certificate can now be added to the web server.

Related links

[Create an identity certificate for the file server](#) on page 75

Adding an identity certificate to a Microsoft IIS server

About this task

The identity certificate generated for the server needs to be added to the HTTP server.

Procedure

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.

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.

Related links

File server certification on page 74

Chapter 12: Monitoring SIP Phones

The following methods can be used to view SIP extension activity.

Related links

Viewing SIP phone communications on page 78
Viewing registrations on page 78
Configuring and enabling syslog output on page 79

Viewing SIP phone communications

About this task

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

Procedure

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**.

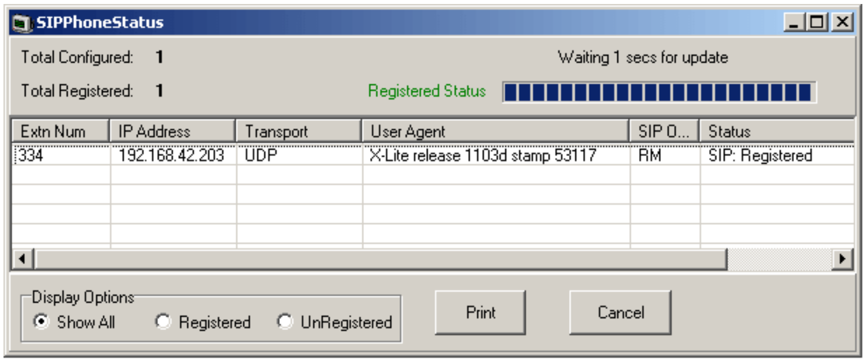
Related links

Monitoring SIP Phones on page 78

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.



SIPPhoneStatus

Total Configured: 1

Total Registered: 1

Waiting 1 secs for update

Registered Status

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

Display Options: ● Show All ○ Registered ○ UnRegistered

Related links

Monitoring SIP Phones on page 78

Configuring and enabling syslog output

About this task

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

Procedure

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

Related links

Monitoring SIP Phones on page 78

Part 3: B100 Series Conference Phones

B100 Series Conference Phones

IP Office supports the B100 Series of high-quality conference phone. The following sections provide notes for those B100 phones that use SIP. This is in addition to the full documentation for those phones.

Chapter 13: B169 Conference Phone

The B169 is a high-quality conference phone that connects to a B100 DECT base station. That base station then connects to the telephone system using SIP. B169 phones are supported with IP Office R10.1.0.6 and R11.0.4.2 and higher.

The following is a example for connecting a single B169 internally on the same network LAN as the IP Office system. For more details of the installation options, refer to the *Installing and Administering IP DECT SC Base Station* manual.

Configure the system for SIP telephone support and create a user and extension for the B169. See Generic installation process on page 34.

Related links

B169 Phone Connection on page 81
B100 DECT Base Station Connection/Login on page 82
B100 DECT Base Station Configuration on page 82

B169 Phone Connection

About this task

Connect the B169 to the DECT base station. Whilst it will not connect to the IP Office at this stage, it allows the phone to be selected within the base station menus and to view the base station IP address.

Procedure

1. Assemble base station and connect to LAN.
2. The base station lamp flashes amber for a few seconds. Once it has an IP address from the network, it will change to green.
3. Assemble the B169 phone and switch on by pressing the ☎ button.
4. When the phone displays **START REGISTRATION?**, press **OK**.
5. The phone scans for an available base station and when connected, displays **AVAYA B169**.

Related links

B169 Conference Phone on page 81

B100 DECT Base Station Connection/Login

Procedure

1. On the phone
    a. Press the menu ⚙ button.
    b. Scroll the display to **Status** and press **OK**.
    c. Scroll the display until the base station's IP address is shown.
2. Using a browser, browse to that address.
3. Enter default name and password.

    For example: name: admin, password: admin)

Related links

B169 Conference Phone on page 81

B100 DECT Base Station Configuration

Procedure

1. Using a browser, login to the configuration menus.
2. Selected **Network**.
    a. Change **DHCP/Static IP** from **DHCP** to **Static**.
    b. Change the **RTP** port value from **50004** to match the minimum RTP port setting of the IP Office system (by default **40750**).
    c. Change the **RTP port range** from **254** to a value that matches the upper values of the IP Office RTP port range.
    d. Click **Save**.
3. Select **Servers**.

    We need a server entry that matches the IP Office. This server entry is then selectable when we add the extension.

    a. Click **Add Server**.
    b. Set the **Server Alias** to a name that identifies its purpose, for this example, IP Office.
    c. Set the **Registrar** to match the FQDN of the IP Office.

        For this example, 192.168.0.180.

    d. Set the **Primary Proxy** to match the FQDN of the IP Office plus the SIP port being used.

        For this example, 192.168.0.180:5060.

    e. Set **SIP Transport** to **TCP**.
    f. Click **Save**.

4. Select **Extension**.
    a. Click the **Idx** number of an unused extension slot (the **Idx** numbers are underlined).
    b. Set **Extension** to the required extension number, for this example 710.
    c. Set **Authentication User Name** to also match the extension number. This value is used for registration on the IP Office system.
    d. Set the **Authentication Password** to match the Phone Password set for the extension in the IP Office configuration.
    e. In the **Server** drop-down, select the server entry created for the link to the IP Office.
    f. In the **Select Handset(s)** table, select the connected B169 phone.
    g. Click **Save**.
5. Select **Home/Status**.
    a. Click **Reboot**.
    b. Wait for the base station to restart. It flashes red for about 3 seconds and then returns to steady green.
    c. Make some test calls to and from the phone.

Related links

B169 Conference Phone on page 81

Chapter 14: B179 conference phone

About this task

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.

Procedure

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 ● ←.

Chapter 15: B199 conference phone

The B199 is a SIP conference phone in the B100 Series. Through the phone's display, it can create and manage conference calls with up to 4 other parties. These conferences are hosted on the phone rather than using IP Office conferencing resources.

- IP Office R11.1 with B199 R1.0 FP1 or higher firmware adds support for automatically obtaining an auto-generated `avayab199.xml` containing SIP settings from the IP Office system.
- IP Office R11.1 FP1 uses version 3 of the XML format used for B199 settings files and should be used with B199 1.0 FP3 (1.0.8.3.2) firmware or higher. Existing B199 phones should be upgraded to the latest firmware.
- IP Office R11.1 FP2 SP4 supports B199 R1.0 FP8 firmware. This release of IP Office supports HTTP redirection for B199 phones running R1.0 FP6 or higher firmware.

This section covers just basic methods of installation. Full details of B199 installation and administration are covered in *Installing and Administering Avaya Conference Phone B199*.

Whilst the phone can be configured through its display, it also supports a set of browser menus which can be accessed from a PC and simplify access to key settings.

Related links

B199 Conference Capacity on page 86
B199 Notes on page 86
The B199 Admin Password on page 87
Overview of B199 Installation Methods on page 87
Downloading the B199 Firmware on page 88
Setting the Auto-Generated B199 Firmware Version on page 88
Method 1: Installing the B199 phone using an HTTP file server on page 89
Method 2: Installing the B199 phone using an HTTP file server and HTTP redirection on page 91
Method 3: Installing a B199 without a file server on page 92
Checking the B199 Status on page 94
Manually upgrading the B199 firmware on page 94
Resetting a B199 Phone on page 95
Performing a hard reset on a B199 on page 95

B199 Conference Capacity

For conferences initiated through the phone's own menus, the B199 hosts the conference itself. It does not use the IP Office conference resources.

This affects the maximum number of participants as follows:

- - The phone supports conferences with up to 4 other participants. However the actual number depends on the codecs being used by those other participants.
  - Each codec has an assigned load value as listed below. If the addition of another participant would reach or exceed a total load of 100, the phone will not allow the additional participant and displays "`Number of participants limited by quality settings.`".

Codec	Codec Weight
G.711	20
G.722/G.729	33
Opus	50

Related links

B199 conference phone on page 85

B199 Notes

The following notes and known limitations apply to the operation of B199 phones with IP Office systems.

- The IP Office system's **HTTP Redirection** setting is only support for IP Office R11.1 FP2 SP4 and B199 phones running R1.0 FP6 or higher.
- Phone register commands from system monitor are not applied to B199 phones.
- B199 DES option cannot be disabled on a factory reset phone unless IP Office is acting as the DHCP server.
- The B199 does not provide dial-pad for early media scenarios to enter the mid-call digits. Therefore, it cannot support early media calls where a user needs to input digits, for example for account code/authorization code entry or for input to an IVR
- B199 phones do not support dual RTCP monitoring.
- Group Call does not work using Avaya Conference Assistance and IP Office. Only the first contact in the group is called when doing a group call using Avaya Conference Assistant and IP Office.

Related links

B199 conference phone on page 85

The B199 Admin Password

When the phone is started for the first time or has been defaulted, it requests that an admin password is set. Unlike other Avaya phones, it cannot receive a password via a settings file. If the password is not known, the phone will require a hard reset. See Performing a hard reset on a B199 on page 95.

Related links

B199 conference phone on page 85

Overview of B199 Installation Methods

These methods of B199 installation uses a separate HTTP file server to upgrade the new phone, if necessary. The phone then gets its settings file from the IP Office system.

The following methods of installation are supported.

Method	Description
1.	**Using a Third-Party HTTP Server for B199 phones with R1.0 FP5 or earlier firmware** This method: 1. The phone requests the `avayab199_fw_version.xml` file from the third-party HTTP file server. 2. If necessary to upgrade, the phone requests the `firmware-1.0.8.3.2-release.kt` file from the third-party HTTP file server. 3. The phone requests an `avayab199.xml` settings file from the third-party file server. 4. The custom `avayab199.xml` file provided by the third-party file server instructs the phone to connect to the IP Office system. 5. The phone restarts and now requests the full `avayab199.xml` file from the IP Office system.
2.	**Using a Third-Party File Server for B199 phones with R1.0 FP6 or higher firmware** This method is only supported with IP Office R11.1 FP2 SP4 and higher and B199 phones already running R1.0 FP6 or higher.. 1. The phone requests the `avayab199_fw_version.xml` file from the IP Office system. 2. If necessary to upgrade, the phone requests the `firmware-1.0.8.3.2-release.kt` file from the IP Office. HTTP Redirection is used to redirect this request to the third-party HTTP file server hosting that file. 3. The `avayab199.xml` file is provided from the IP Office system.

Table continues…

Method	Description
3.	**Installing Without a File Server** In this method of B199 installation, the IP Office system is not acting as a DHCP server and the customer's DHCP server does not redirect the new B199 phones to a file server.

Related links

B199 conference phone on page 85

Downloading the B199 Firmware

About this task

The IP Office can auto-generate the `avayab199_fw_version.xml` and `avayab199.xml` files for the B199 release that it supports. However, it does not include the matching `firmware-nnnn-release.kt` firmware file indicated in the `avayab199_fw_version.xml` file.

Procedure

1. Browse to the Avaya Support website (https://support.avaya.com).
2. Select **Product Support** > **Downloads**.
3. In **Search Product**, enter `B100` and select **Avaya Conference Phone B100 Series**.
4. In **Choose Release** select **B199 1.0.x**.
5. Select the required firmware release.
    - B199 R1.0 FP8 is supported for IP Office R11.1.2.4 and higher.
6. Download the firmware file, for example `avayab199_fw_version.xml`.

Related links

B199 conference phone on page 85

Setting the Auto-Generated B199 Firmware Version

The IP Office can auto-generate the `avayab199_fw_version.xml` file requested by B199 phones. By default, that file assumes a particular supported firmware release. For example, for IP Office R11.1.2.4, B199 firmware `firmware-1.0.8.0.13-release.kt` is assumed.

If required, using a NoUser source number you can set the B199 firmware version to a different value.

1. In the IP Office configuration, locate the **Source Number** settings of the `NoUser` user.

2. Add the source number `SET_B199_FW_VER=`*nnnn* where *nnnn* is the required B199 firmware version. The IP Office then uses `firmware-nnnn-release.kt` in its auto-generated `avayab199_fw_version.xml` file.
3. Save the new configuration using a reboot.

Related links

B199 conference phone on page 85

Method 1: Installing the B199 phone using an HTTP file server

This method is needed with B199 phones running R1.0 FP5 or earlier firmware. The earlier firmware does not support HTTP redirection.

Before you begin

Having downloaded the B199 R1.0 FP8 file set (see Downloading the B199 Firmware on page 88), place the following files on the third-party file server:

- **`firmware-1.0.8.3.2-release.kt`:** The firmware file for B199 phones.
- **`avayab199_fw_version.xml`**: This file is requested by the phone and used to inform it of the firmware available to be downloaded and installed from the file server. Using a text editor, ensure that the file contents match the B199 firmware file name.

```
<?xml version="1.0" encoding="UTF-8"?>
<firmware_version>
<version>1.0.8.0.13</version>
<filename>firmware-1.0.8.0.13-release.kt</filename>
<checksum></checksum>
</firmware_version>
```

- **`avayab199.xml`**: This custom file gives the phone the IP Office address as its new file server setting. This causes the phone to restart after which it will requests the auto-generated `avayab199.xml` from the IP Office system.

```
<?xml version="1.0" encoding="UTF-8"?>
<B199>
<device_management>
<server type="string">http://192.168.0.180</server>
</device_management>
</B199>
```

Procedure

1. First enable SIP phone support and create a user and extension for the B199 phone as per the generic SIP phone installation processes.
2. Connect the PoE network cable from the network to the phone.
3. Once started, if the phone prompts whether to perform auto-provisioning, select **No**.
4. The phone prompts you to set a password, select **Yes**. Set and confirm the password. This password is required for access to the phone's admin and web browser menus.

5. Click on **<** twice.

   If you click **<** too often, the phone reboots. If so, after rebooting, press ⚙ **Settings** and click **Admin Login**.

6. Press **V** to scroll down and click **Device Management**.

   a. Click **Provisioning Server** and enter the address of the third-party HTTP file server. For example, `http://192.168.0.50`.

   b. Press **V** to scroll down and click **DES Provisioning**.

   c. Click **DES Enablement** and select **Disabled**.

   d. Click **<** repeatedly until you exit the admin menus. The phone will reboot.

7. After rebooting, the phone requests the `avayab199_fw_version.xml` from the HTTP file server.

   a. Using the details in the `avayab199_fw_version.xml` file, the phone upgrades its firmware if necessary. This is shown by the message `Upgrade in progress, please wait`

   b. Once it has loaded the new firmware, the phone reboots.

8. The phone request the `avayab199.xml` file from the HTTP file server. This is the custom `avayab199.xml` file which instructs the phone to change its provisioning server address to the IP Office address. This change causes the phone to reboot again.

   - If not using custom `avayab199.xml` file from the HTTP file server, you need to manually change the **Provisioning Server** address to the address of the IP Office system with which the phone needs to register.

9. Following the reboot, the phone requests the `avayab199.xml` file again but this time from the IP Office system.

10. The phone displays `Avaya B199` and `Not Registered`.

11. Press ⚙ **Settings**. Click **Admin Login** and enter the phone's admin password.

    a. Click **SIP**.

    b. Click **Primary Account**.

       a. In **User**, enter the phone's extension number.

       b. Press **V** to scroll down and click **Credentials**.

       c. In **Authentication Name**, enter the phone's extension number.

       d. In **Password**, enter the IP Office extension password.

       e. Click **<** twice.

    c. If the phone is being installed in an IP Office network that has resilience configured, click **Fallback Account** and enter the same details again.

    d. Click **<** to exit the menus. The phone is rebooted again.

e. Following the reboot, the phone displays `Avaya B199` and the system's IP address.

Related links

B199 conference phone on page 85

Method 2: Installing the B199 phone using an HTTP file server and HTTP redirection

This method can be used with B199 phones running R1.0 FP6 or higher firmware.

Before you begin

1. Having downloaded the B199 R1.0 FP8 file set (see Downloading the B199 Firmware on page 88), place the following file on the third-party file server:
    - **`firmware-1.0.8.3.2-release.kt`:** The firmware file for B199 phones.
    - No other files are required. The IP Office provides its own `avayab199_fw_version.xml` and `avayab199.xml` files.
2. Enable **HTTP Redirection** on the IP Office and set the **HTTP Server IP Address** address to the third-party HTTP file server. See Changing the file server settings on page 53.

Procedure

1. First enable SIP phone support and create a user and extension for the B199 phone as per the generic SIP phone installation processes.
2. Connect the PoE network cable from the network to the phone.
3. Once started, if the phone prompts whether to perform auto-provisioning, select **No**.
4. The phone prompts you to set a password, select **Yes**. Set and confirm the password. This password is required for access to the phone's admin and web browser menus.
5. Click on **<** twice.

    If you click **<** too often, the phone reboots. If so, after rebooting, press ⚙ **Settings** and click **Admin Login**.
6. The phone prompts you to set a password, select **Yes**. Set and confirm the password. This password is required for access to the phone's admin and web browser menus.
7. Click on **<** twice.

    If you click **<** too often, the phone reboots. If so, after rebooting, press ⚙ **Settings** and click **Admin Login**.
8. Press **V** to scroll down and click **Device Management**.
    a. Click **Provisioning Server** and enter the address of the IP Office system. For example, `http://192.168.0.42`.

   b. Press **V** to scroll down and click **DES Provisioning**.
   c. Click **DES Enablement** and select **Disabled**.
   d. Click **<** repeatedly until you exit the admin menus. The phone will reboot.

9. After rebooting, the phone requests the `avayab199_fw_version.xml` from the HTTP file server.
   a. Using the details in the `avayab199_fw_version.xml` file, the phone upgrades its firmware if necessary. This is shown by the message `Upgrade in progress, please wait`
   b. Once it has loaded the new firmware, the phone reboots.
10. Following the reboot, the phone requests the `avayab199.xml` file from the IP Office system.
11. The phone displays `Avaya B199` and `Not Registered`.
12. Press ⚙ **Settings**. Click **Admin Login** and enter the phone's admin password.
    a. Click **SIP**.
    b. Click **Primary Account**.
       a. In **User**, enter the phone's extension number.
       b. Press **V** to scroll down and click **Credentials**.
       c. In **Authentication Name**, enter the phone's extension number.
       d. In **Password**, enter the IP Office extension password.
       e. Click **<** twice.
    c. If the phone is being installed in an IP Office network that has resilience configured, click **Fallback Account** and enter the same details again.
    d. Click **<** to exit the menus. The phone is rebooted again.
    e. Following the reboot, the phone displays `Avaya B199` and the system's IP address.

Related links

[B199 conference phone](#) on page 85

Method 3: Installing a B199 without a file server

About this task

In this method of B199 installation, the IP Office system is not acting as a DHCP server and the customer's DHCP server does not redirect the new B199 phones to a file server.

Download the B199 firmware from https://support.avaya.com. This documentation assumes that version 1.0.8.3.2 is being used.

Procedure

1. First enable SIP phone support and create a user and extension for the B199 phone as per the generic SIP phone installation processes.
2. Connect the PoE network cable from the network to the phone.
3. Once started, if the phone prompts whether to perform auto-provisioning, select **No**.
4. The phone prompts you to set a password, select **Yes**. Set and confirm the password. This password is required for access to the phone's admin and web browser menus.
5. Click on **<** twice.

   If you click **<** too often, the phone reboots. If so, after rebooting, press ⚙ **Settings** and click **Admin Login**.
6. Click **Status**. The menu displays key information:
   - The **IP Address** is used to access the phone's admin menus in a web browser.
   - If the **Software Version** is lower then 1.0.8.3.2, the phone should be upgraded (see Manually upgrading the B199 firmware on page 94.) . Otherwise, press the **<** icon.
7. Press **V** to scroll down and click **Device Management**.

   a. Click **Provisioning Server** and enter the address of the IP Office system.

   b. Press **V** to scroll down and click **DES Provisioning**.

   c. Click **DES Enablement** and select **Disabled**.

   d. Click **<** repeatedly until you exit the admin menus. The phone will reboot.
8. The phone requests the `avayab199.xml` file from the IP Office system. When received, the phone reboots again.
9. The phone displays `Avaya B199` and `Not Registered`.
10. Press ⚙ **Settings**. Click **Admin Login** and enter the phone's admin password.

    a. Click **SIP**.

    b. Click **Primary Account**.

       a. In **User**, enter the phone's extension number.

       b. Press **V** to scroll down and click **Credentials**.

       c. In **Authentication Name**, enter the phone's extension number.

       d. In **Password**, enter the IP Office extension password.

       e. Click **<** twice.

    c. If the phone is being installed in an IP Office network that has resilience configured, click **Fallback Account** and enter the same details again.

    d. Click **<** to exit the menus. The phone is rebooted again.

    e. Following the reboot, the phone displays `Avaya B199` and the system's IP address.

Related links

B199 conference phone on page 85

Checking the B199 Status

Use the following process to check the phone's current IP address and firmware level.

1. On the phone's display, press **Settings** and then **Status**.
2. The menu displays key information:
   - The **IP Address** is used to access the phone's admin menus in a web browser.
   - If the **Software Version** is lower then 1.0.8.3.2, the phone should be upgraded, see Manually upgrading the B199 firmware on page 94. Otherwise, press the **<** icon to exit the menus and proceed to configuring the phone.

Related links

B199 conference phone on page 85

Manually upgrading the B199 firmware

About this task

B199 firmware is available from the Avaya support website (see Downloading the B199 Firmware on page 88). You must also download and read any release notes associated with the firmware.

For methods of upgrading multiple phones together, refer to Installing and Administering Avaya Conference Phone B199 .

Procedure

1. Copy the firmware file onto your PC.
2. Using the phone's IP address, browse to `https://<IP_Address>`. The address can be obtained from the phone's status menu (see Checking the B199 Status on page 94)
3. Log in using the phone's admin password.
4. Select the **Provisioning** tab.
5. In the **Firmware** section, click **Choose File** and select the firmware file on your PC.
6. Click **Save**.
7. The phone displays `Upgrade in progress, please wait`. Once it has upgraded, the phone reboots. Do not remove power from the phone until these processes have been completed.

8. Proceed to configuring the phone.

Related links

B199 conference phone on page 85

Resetting a B199 Phone

About this task

The following processes can be used to reset the phone.

Procedure

1. On the phone's display, press ⚙ **Settings**.
2. Click **Admin Login** and enter the phone's admin password.
3. Click **Phone** and scroll down.
4. Click **Factory Reset**.
5. Click **OK**.

Result

The phone is rebooted and all existing settings returned to default.

Related links

B199 conference phone on page 85

Performing a hard reset on a B199

About this task

This method of resetting the phone also causes it to revert to its previous version of firmware if it has been upgraded.

Procedure

1. Disconnect the power supply cable. This is the same as the network cable as the phone uses power over Ethernet.
2. Insert the PoE cable into the network connection socket.
3. Repeatedly tap the mute button on the touch screen.
4. When the LED's turn red, press the volume up button once.

Result

- The phone reboots to its default settings.

- The phone also reverts to any previous firmware it has if any. Therefore, if required, upgrade the phone firmware. See Manually upgrading the B199 firmware on page 94.

Related links

B199 conference phone on page 85

Part 4: J100 Series Phones

Chapter 16: 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.

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

Related links

Restrictions/Limitations on page 98
Known Problems on page 99
Files on page 100
Simple installation of J129 on page 101
Static IP address configuration on page 101
J129 dial plan settings on page 102
Changing the phone SSON on page 103
Viewing the phone settings on page 103
Factory Reset on page 104

Restrictions/Limitations

- **Emergency Calls:** The Emerg soft key feature is not supported. Emergency calls are not available when the phone is not registered.
- **Distinctive Ringing:** There is no support for distinctive ringing on this phone.
- **# 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.
- **Contacts Menu:** The phone only support the user's personal contacts. It does not display system directory contacts.
  - Support for contacts/recents requires the phone to be installed using HTTPS. If not, contacts using HTTP is possible if **HTTP Directory Read** and **HTTP Directory Write** are enabled in the system's security settings. This also affects the display and operation of the phone's Recents menu.
- **Unsupported Phone Features:**
  - Call Frwd menu
  - Transfer on Hangup
  - Automatic Callback
  - Hot Desking

Related links

J129 on page 98

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 on the phone.
- **Changing IP Office Systems:**

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

- **Contacts/Recents Display:**

  The phone only support the user's personal contacts. It does not display system directory contacts.

  Support for contacts/recents requires the phone to be installed using HTTPS. If not, contacts using HTTP is possible if **HTTP Directory Read** and **HTTP Directory Write** are enabled in the system's security settings. This also affects the display and operation of the phone's Recents menu.

Related links

[J129](#) on page 98

Files

During a restart, J100 Series telephones requests a series of files, using HTTPS or HTTP, from the configured file server. 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 theIP Office system as the file server, the file is auto-generated if not physically present.

- `46xxsettings.txt`

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

Related links

[J129](#) on page 98

Simple installation of J129

About this task

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.

Procedure

1. Download the J129 firmware file set from the IP Office download pages on Avaya Support.
2. Unpack the files to a temporary folder.
3. Upload the files to the system's primary folder
4. Enable SIP extension support on the system
5. Create the SIP users and SIP extensions
6. Attach and register the phones

Related links

J129 on page 98

Static IP address configuration

About this task

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

Procedure

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**.

6. 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. Press **Save**.
7. Press **Back** to exit from the **IP Configuration** and then the **Admin** menus The phone restarts automatically.
8. When prompted to enter the user credentials, at the **Username** prompt enter the user extension number and then the user password.

Related links

J129 on page 98

J129 dial plan settings

When making calls, by default the J129 requires the user to dial the digits required and then press **Call** to send those digits to the system for processing. If the user does not press **Call**, then after 5 seconds it assumes dialing is complete and send the digits dialed so far to the system.

Both of those aspects of J129 operation can be configured through the use of settings added to the system's `46xxspecials.txt` file (see 46xxspecials.txt on page 23).

- `SET INTER_DIGIT_TIMEOUT N`

  Set the number of seconds from the last digit dialed after which the phone assumes dialing is complete and send the digits dialed to the system. N can be a value between 1 and 20 seconds. The default used if no settings is specified is 5 seconds.

- `SET DIALPLAN <dial plan>`

  Set number patterns which, when matched by the users dialing, are taken as dialing complete and sent to the system. The dial plan can include the following characters:

  - |: This character is used to separate each different number pattern.
  - X: This character is a wildcard for any single digit match.
  - [ ]- Square brackets can be used to contain possible specific single digit matches. For example:
    - [1237] matches 1, 2, 3 or 7. A - character can be used to match a range of digits.
    - [1-4] matches any digit from 1 to 4.

For full details of available settings, refer to the *Installing and Administering J100 Series IP Deskphones SIP* manual.

The following dial plan could be used on a system where all user extension numbers are in the range 200 to 299, group extensions in the range 300 to 399 and *17 is used for voicemail access.

```
SET DIALPLAN [2-3]XX|*17
SET INTER_DIGIT_TIMEOUT 2
```

Related links

J129 on page 98

Changing the phone SSON

About this task

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.

Procedure

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**.

Related links

J129 on page 98

Viewing the phone settings

About this task

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

Procedure

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. Use the cursor keys to scroll through the settings and their current values.

5. Press **Back** to return to the normal menu.

Related links

J129 on page 98

Factory Reset

Procedure

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**.

Related links

J129 on page 98

Chapter 17: J100 Series 'Stimulus' Phones

Apart from the J129 (see J129 on page 98), IP Office supports other J100 Series phones using an operating mode referred to as 'stimulus' mode. In that mode they support the full set of IP Office phone menus.

- The J169/J179 SIP phones are supported from Release 11.0.
- The J139 is supported from R11.0 SP1.
- The J159 is supported from FP4 SP1.
- The J189 is supported from R11.1 FP1.

They can largely be installed using the generic installation process. which provides the phones with the required `J100Supgrade.txt` and `46xxsettings.txt` files.

- The phones support "trust on first use" for HTTPS connections. The phones allow an initial connection to an HTTPS server without validating the full certificate chain as long as the server certificate name is valid. They then download and use that certificate for subsequent connections. This only applies to a new or defaulted phone on first connection.
- Server Root Certificate installation for HTTPS firmware download:
  - If the phone is installed in a local network, it automatically downloads the IP Office system's root certificate using an unsecure HTTP connection. You must ensure that the IP Office system's root certificate(s) are installed in the system's certificate store (**Security** > **System** > **Certificates** > **Trusted Certificate Store**).
  - If the phone is installed in the remote network environment, the IP Office system's root certificate must to be pre-installed on the phone before it is connected in the remote network. Do this by connecting the phone to the IP Office system's local network and make sure that the phone's HTTP server setting points to the IP Office. During initial installation, the phone downloads the root certificate(s) from the system. Pre-staging is not a requirement if an Avaya Session Border Controller is not being used.

Related links

System settings on page 106
Simple J100 connection procedure on page 106
Advanced J100 connection procedure on page 107

System settings

If adding these phones to an existing system with a static `46xxsettings.txt` file, it is recommended that you first examine the settings in the system's auto-generated `46xxsettings.txt` file and compare them to your static file.

The key sections relevant to J100 Series telephone operation are labeled `J1X9AUTOGENERATEDSETTINGS`, `STIMULUSPHONECOMMONSETTINGS` and `STIMULUSSETTINGS`. See 46xxspecials.txt on page 23.

If the correct settings are not specified, the J100 Series phones will operate as standard SIP telephone with no IP Office specific menus.

Related links

J100 Series 'Stimulus' Phones on page 105

Simple J100 connection procedure

About this task

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

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

Procedure

1. Connect the LAN cable to the phone. If not using PoE, connect the power adapter cable.
2. The lamp (top-right) comes one though the screen remains blank.
3. The phone goes through its software loading cycle. During this it displays the Avaya logo above a progress bar, followed by displaying the Avaya splash screen.
4. When **Do you want to activate Auto Provisioning now?** is displayed select either option, **Yes** or **No**.
5. The phone displays **Starting...** followed by **Waiting for DHCP...**.
6. If the DHCP response did not include the file server address the phone should use, it displays a **Configure provisioning server** or **Enter file server address** prompt. Select **Config**.
    a. Enter the address of the server holding the `J100Supgrade.txt` file. You must prefix the address with `http://` or `https://`.
        - The **abc**, **ABC**, **123** or **hex** key indicates the current mode of character entry being used by the phone. Press the key to change mode.
        - To enter a **/**, press **More** and press the **/** key.

        - To enter a **:**, select **abc** mode and press **1** until the **:** character is selected for entry.
        - To enter a **.** when in **123** mode, press the ***** key on the dial pad.

    b. Check the address and click **Save**. If **Connection error** is displayed, check and correct the file server address.

7. The phone displays **Restarting...** and then repeats it software loading cycle.
8. If the phone needs to load new software from the file server, it displays **Updating software** and a progress bar after which it restarts again.
9. When the phone displays **Login**. Enter the following:

    a. For the **Username**, enter the extension number.

    b. For the **Password**, enter the extension's **Extension** > **Phone Password** set in the IP Office configuration.

Related links

J100 Series 'Stimulus' Phones on page 105

Advanced J100 connection procedure

About this task

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

Procedure

1. Attach the network cable.
2. Access the administration menu:

    a. If shown on the display, press **Admin**. Otherwise, press **More** and **Admin** or press ≡ and select **Administration**.

    b. Enter the administration password and press **Enter**. These phones do not support pressing **#** to enter the password.

3. **If you want the phone to use Wi-Fi:** Wireless connection is supported on phones with the optional Wi-Fi module installed. Select **Network interfaces**.

    a. Change the **Network mode** from **Ethernet** to **Wi-Fi**.

    b. Press **Save**. The phone scans for available wireless networks.

    c. Select the required network and click **Connect**. Press **OK**.

        - If hidden Wi-Fi is enabled (see Enabling hidden Wi-Fi SSID support on page 123), you can click scroll down and select **Add Network** to add details for connecting to a network that does not broadcast its SSID.

    d. In the **Password** field, enter the password for the wireless network and press **Wi-Fi**. If the phone is able to connect to the network, it is restarted.

4. Select **IP Configuration**.
5. **If you want to use a static address rather than DHCP:** Select **Ethernet IPv4** or **Wi-Fi IPv4** depending on whether the phone was connected to the network using a wired connection or Wi-Fi.
    a. Change **Use DHCP** to off.
    b. Set the **Phone**, **Gateway** and **Mask** details to match the requirements of the customer network.
    c. Click **Save**.
6. Set the **File Server**. If the phone has not obtained the file server address through its initial DHCP start-up (for example, it is not getting DHCP from the IP Office or from a DHCP server configured with Option 242), then you need to configure the file server address manually:
    a. Select **Servers**.
    b. Enter the **HTTPS server** and or **HTTP server** address of the file server containing the J100 settings and firmware files.
        - The **abc**, **ABC**, **123** or **hex** key indicates the current mode of character entry being used by the phone. Press the key to change mode.
        - To enter a **/**, press **More** and press the **/** key.
        - To enter a **:**, select **abc** mode and press **1** until the **:** character is selected for entry.
        - To enter a **.** when in **123** mode, press the ***** key on the dial pad.
    c. Press **Save**.
7. Press **Back** until you exit the admin menus.
8. The phone displays **Restarting...** and then repeats it software loading cycle.
9. If the phone needs to load new software from the file server, it displays **Updating software** and a progress bar after which it restarts again.
10. When the phone displays **Login**. Enter the following:
    a. For the **Username**, enter the extension number.
    b. For the **Password**, enter the extension's **Extension** > **Phone Password** set in the IP Office configuration.

Related links

J100 Series 'Stimulus' Phones on page 105

Chapter 18: Additional J100 Series Phone Processes

This section covers some additional processes that can be used with J100 Series phones.

Related links

Resetting the phone on page 109
Branch deployment on page 110
Changing the phone's group setting on page 110
JEM24 Button Module Support on page 111
J100 Display mode on page 111
J189 D01B phone support on page 112
Headset Profile on page 112

Resetting the phone

About this task

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

Procedure

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

Next steps

When the phone restarts, follow the process for initial configuration.

Related links

Additional J100 Series Phone Processes on page 109

Branch deployment

In addition to support as local IP Office extensions, J100 Series phones are also supported as Avaya Aura® extensions which, in rainy-day scenarios, can failover to the IP Office for basic call functions. Within the IP Office configuration these are referred to as 'centralized' extensions. This is called 'branch deployment'.

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

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

Related links

Additional J100 Series Phone Processes on page 109

Changing the phone's group setting

About this task

In some scenarios, the group ID value is used with the `46xxspecials.txt` files to control which files and settings are used by different phones. If the J100 series phone needs to use a group value use the following process to set the value.

Procedure

1. Access the administration menu:
   a. If shown on the display, press **Admin**. Otherwise, press **More** and **Admin** or press ≡ and select **Administration**.
   b. Enter the administration password and press **Enter**. These phones do not support pressing **#** to enter the password.

2. Scroll down and select **Group**.
3. Enter the **Group** number required and press **Save**.
4. Press **Back**.

Result

The phone is automatically restarted. This will cause it to load any settings specified by the new group number value.

Related links

Additional J100 Series Phone Processes on page 109

JEM24 Button Module Support

The JEM24 button module is supported with the J169, J179 and J189 phones.

J169/J179 with JEM24 Expansion Modules

These phones can support up to 3 JEM24 button modules. However, depending upon the amount of power supplied by PoE, it may be necessary to power the phone using a separate 5V power supply.

J189 with JEM24 Expansion Modules

These phones can support up to 2 JEM24 button modules. For a J189 with JEM24 buttons modules, power can be supplied by PoE or a 5V power adaptor.

- When the phone is powered using a 5V power adaptor, you can connect up to 2 JEM24 expansion modules.
- On the back of each J189, a switch sets the phone's PoE power level as either high (**H**) and low (**L**). On PoE power J189 phones with JEM24 buttons modules attached, the switch must be set to **H**. The switch must only be changed when the phone off.

Related links

Additional J100 Series Phone Processes on page 109

J100 Display mode

The J100 Series phones can white text on a dark background (dark mode) or black text on a white background. Using settings in a `46xxspecials.txt` (see 46xxspecials.txt on page 23), you can control the mode used, and whether users can change the mode.

- This feature requires the J100 Series phones to run J100 R4.1.2.0 or high firmware. See Upgrading the J100 phone firmware on page 125. Phones on earlier firmware use dark mode.

Settings file command

Add the setting `DISPLAY_MODE N` to the `46xxspecials.txt` file, where `N` is:

- `0` = Dark mode. User switchable.
- 1 = Light mode. User switchable.
- `2` = Dark mode. Not user switchable.
- `3` = Light mode. Not user switchable.

For example:

```
IF $MODEL4 SEQ J139 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J169 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J179 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J159 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J189 GOTO J1X9SPECIALS
GOT END
# J1X9SPECIALS
SET DISPLAY_MODE 1
#END
```

User control

If you choose to make the option user switchable, users can select ≡ > **Settings** > **Display** > **Display mode** on their phone.

Related links

Additional J100 Series Phone Processes on page 109

J189 D01B phone support

J189 phones labeled as J189 D01B use version 4 hardware. That hardware uses a different chipset from previous J189 phones and therefore requires different firmware. The firmware, and updated `J100Supgrade.txt` to install that firmware, are part of J100 R4.0.12.1 or high firmware.

- To install the J100 R4.0.12.1 firmware on the IP Office system, see Upgrading the J100 phone firmware on page 125.
- If a J189 D01B phone is attached to an IP Office that is using a lower release of firmware, the J189 D01B will run using its factory installed firmware.

Related links

Additional J100 Series Phone Processes on page 109

Headset Profile

The phone supports headsets from a range of suppliers. For optimal sound and performance, the phone's headset profile setting may need to be changed to match the headset, The following is a list of the headsets tested and supported by Avaya and their matching profile setting. Other headsets may also work but have not been tested by Avaya.

Profile	Description
1	Default
2	Plantronics: SupraPlus Wideband HW251N/HW261N (HIS). Sennheiser: SH330, SH350, CC510, CC550 (CAVA-31).
3	Plantronics: EncorePro HW291N/HW301N (HIS). Sennheiser: Circle SC230/260 (CAVA-31).
4	Jabra: BIZ 2400 (GN1216). Sennheiser: Century SC630/660 (CAVA-31). VXI: CC Pro 4010V DD, CC Pro 4021V DC (OmniCord-V)
5	Jabra: GN2000 (GN1216).
6	Jabra: PRO 9470 (14201-33).
7	Plantronics: CS500 Series CS510, CS520, CS530, CS540 (APV-63). Savi 700 Series - W710, W720, W730, W740, W745 (APV-63)
8	Sennheiser: DW Pro1, DW Pro2, DW Office, SD Pro1, SD Pro2, SD Office (CEHS-AV03/AV04).

Normally setting an individual phone's headset profile can be done through that phone's administration menus, following the path **Settings** > **Audio** > **Headset profile**. However, currently that menu option does not work. As an alternative, the **SET HEADSET_PROFILE_DEFAULT X** option, where X is the required headset profile, can be used in the settings provided to the phone.

This can be done through a `46xxspecials.txt` file added to the system. Depending on the mix of phones and headphones supported on the customer system, it may be necessary to enclose the company is some logical control such as a group or phone model setting.

For example:

```
# GROUP SETTINGS
IF $GROUP SEQ 1 GOTO GROUP_1
IF $GROUP SEQ 1 GOTO GROUP_2
...
GOTO END
# GROUP_1
SET HEADSET_PROFILE_DEFAULT 4
GOTO END
# GROUP_1
SET HEADSET_PROFILE_DEFAULT 7
GOTO END
...
# END
```

Related links

Additional J100 Series Phone Processes on page 109

Chapter 19: Restarting SIP phones

You can use the following processes to restart a J100 phone or phones.

Related links

Restarting SIP phones using System Status Application on page 114
Restarting SIP phones using SysMonitor on page 114
Restarting a J100 phone on page 115

Restarting SIP phones using System Status Application

About this task

You can use this process to restart multiple phones, including remote extensions.

Procedure

1. Start System Status Application and connect to the IP Office.
2. Select **System** > **SIP Extensions** > **Avaya SIP Endpoints**.
3. Select the phone or phones that you want to restart.
4. Click **Restart**.

Related links

Restarting SIP phones on page 114

Restarting SIP phones using SysMonitor

About this task

You can use this process to restart multiple phones, including remote extensions.

Procedure

1. Start SysMonitor and connect to the IP Office.
2. Select **Status** > **SIP Phone Status**.
3. Select the phone or phones that you want to restart.

4. Click **Reset Phones**.

Related links

Restarting SIP phones on page 114

Restarting a J100 phone

About this task

This process restarts the phone.

Procedure

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

Related links

Restarting SIP phones on page 114

Chapter 20: Controlling the J100 Screensaver and Background Images

This section covers the commands you can use to control the background and screensaver images on J100 phones.

Related links

J100 Image File Details on page 116
J100 Phone Background Image Controls on page 117
J100 Phone Screensaver Image Controls on page 117
JEM24 Background image control on page 118
JEM24 Phone Screensaver Image Controls on page 119
Image File Paths on page 120

J100 Image File Details

Each J100 Series phone can load up to 5 images for use as screen backgrounds and screen savers. The following limitations apply to the image files:

- `.jpeg`/`.jpg` format files only.
- 256kB maximum file size.
- 16-bit Color depth.
- The file names are case sensitive.
- Image sizes as follows:

Phone	Main Screen	Secondary Screen
J139/J169/J179	320 x 240 pixels	–
J159	320 x 240 pixels	160 x 240 pixels
J189	800 x 480 pixels	240 x 320 pixels

Related links

Controlling the J100 Screensaver and Background Images on page 116

J100 Phone Background Image Controls

The following is an example of the commands you can use to set the background image operation on J100 Series phones.

```
## MAIN SCREEN
SET BACKGROUND_IMAGE "J159main01.jpg,J159main02.jpg"
SET BACKGROUND_IMAGE_DISPLAY J159back01.jpg
SET BACKGROUND_IMAGE_SELECTABLE 1
## SECONDARY SCREEN
SET BACKGROUND_IMAGE_SECONDARY "J159secondary.jpg"
SET BACKGROUND_IMAGE_DISPLAY_SECONDARY J159secondary.jpg
SET BACKGROUND_IMAGE_SELECTABLE_SECONDARY 1
```

The individual commands are:

- `SET BACKGROUND_IMAGE "<filename1>,<filename2>,..."`

  This commands specifies a list of images the phone requests from the file server. This is a comma-separated list of file names enclosed in " " quotation marks.

- `SET BACKGROUND_IMAGE_DISPLAY <filename>`

  Set which of the requested images the phone uses as its default background image.

- `SET BACKGROUND_IMAGE_SELECTABLE <N>`

  Set whether the phone user can change the background image using the **Settings** > **Display** > **Background** menu..

  - 0 = The user cannot select the background image. They do not see the selection menu.
  - 1 = The user can select the background image from the phone menu.

A similar set of commands, shown in the example, exist for phones which have a secondary screen.

Related links

Controlling the J100 Screensaver and Background Images on page 116

J100 Phone Screensaver Image Controls

The following is an example of the commands you can used to set the screensaver image operation on J100 Series phones.

```
SET SCREENSAVERON 10
SCREENSAVER_CLOCK_ENABLE 1
## MAIN SCREEN
SET SCREENSAVER_IMAGE "J159scrsaver.jpg"
SET SCREENSAVER_IMAGE_DISPLAY J159scrsaver.jpg
SET SCREENSAVER_IMAGE_SELECTABLE 0
```

The individual commands are:

- `SET SCREENSAVERON <minutes>`

Set the number of minutes of idle time after which the phone should display a screensaver image.

- The value can be set between 0 to 480 minutes.
- The default is 240 minutes if no value is specified.
- A value of 0 means that the screensaver is not automatically displayed. The user can activate the screensaver when required using the **Applications** > **Activate Screensaver** option.

- `SET SCRRENSAVER_CLOCK_ENABLE <N>`

  Specify whether the clock should be displayed on the screensaver screen. The user can change this on the phone's **Settings** > **Display** > **Screensaver** menu.

  - 0 = Do not display the clock.
  - 1 = Display the clock.

- `SET SCREENSAVER_IMAGE "<filename1>,<filename2>,..."`

  This commands specifies a list of images the phone requests from the file server. This is a comma-separated list of file names enclosed in " " quotation marks.

- `SET SCREENSAVER_IMAGE_DISPLAY <filename>`

  Set which of the requested images the phone uses as its default screensaver image.

- `SET SCREENSAVER_IMAGE_SELECTABLE <N>`

  Set whether the phone user can change the screensaver image using the **Settings** > **Display** > **Screensaver** menu..

  - 0 = The user cannot select the background image. They do not see the selection menu.
  - 1 = The user can select the background image from the phone menu.

Related links

Controlling the J100 Screensaver and Background Images on page 116

JEM24 Background image control

For J100 R4.1.0.0 and higher, you can also add up to 5 separate background images for use by JEM24 modules.

- This feature requires the J100 phones to use J100 R4.1.0.0 or higher firmware. See Upgrading the J100 phone firmware on page 125).

You can add the following commands to the `46xxspecials.txt` file to control the use of the files.

- `SET BACKGROUND_IMAGE_JEM_FOLLOW_PRIMARY <N>`

Sets whether the JEM24 button modules image can differ from the background image selected on the J100 phone primary display. Where `<N>` is:

- `0` = The JEM24 can differ from the phone primary display. You can use the commands below to controlled operation.
- `1` = The JEM24 matches the phone primary display and cannot be overridden through the phone menu. **This settings overrides the following commands and is the default used if the command is not specified.**

- `SET BACKGROUND_IMAGE_JEM <filenames>`

  Set the list of JEM24 image files to download to the phone. You can specify up to 5 filenames, separating each name with a comma. See Image File Paths on page 120.

- `SET BACKGROUND_IMAGE_DISPLAY_JEM <filename|N>`

  Set the default file to show as the JEM24 image. This uses either a file name or a number:

  - `<filename>` = Select one of the downloaded image files.
  - `<N>` = Use one of the 7 default images, where 0 to 6 matches defaults images 1 to 7 respectively.

- `SET BACKGROUND_IMAGE_SELECTABLE_JEM <N>`

  Sets whether the user can select the JEM24 image through their phone menu. Where `<N>` is:

  - `0` = Users cannot change the JEM24 image.
  - `1` = Users can change the JEM24 image, overriding any previous set image. This is the default if the command is not specified.

Related links

Controlling the J100 Screensaver and Background Images on page 116

JEM24 Phone Screensaver Image Controls

You can add up to 5 separate screensaver images for use by JEM24 modules.

- This feature requires the J100 phones to use J100 R4.1.0.0 or higher firmware. See Upgrading the J100 phone firmware on page 125).

You can add the following commands to the `46xxspecials.txt` file to control the use of the files.

- `SET SCREENSAVER_IMAGE_JEM_FOLLOW_PRIMARY <N>`

  Sets whether the JEM24 button modules image can differ from the background image selected on the J100 phone primary display. Where `<N>` is:

  - `0` = The JEM24 can differ from the phone primary display. You can use the commands below to controlled operation.
  - `1` = The JEM24 matches the phone primary display and cannot be overridden through the phone menu. **This settings overrides the following commands and is the default used if the command is not specified.**

- `SET SCREENSAVER_IMAGE_JEM <filenames>`

  Set the list of JEM24 image files to download to the phone. You can specify up to 5 filenames, separating each name with a comma. See Image File Paths on page 120.

- `SET SCREENSAVER_IMAGE_DISPLAY_JEM <filename|N>`

  Set the default file to show as the JEM24 image. This uses either a file name or a number:

  - `<filename>` = Select one of the downloaded image files.
  - `<N>` = Use one of the 7 default images, where 0 to 6 matches defaults images 1 to 7 respectively.

- `SET SCREENSAVER_IMAGE_SELECTABLE_JEM <N>`

  Sets whether the user can select the JEM24 image through their phone menu. Where `<N>` is:

  - `0` = Users cannot change the JEM24 image.
  - `1` = Users can change the JEM24 image, overriding any previous set image. This is the default if the command is not specified.

Related links

Controlling the J100 Screensaver and Background Images on page 116

Image File Paths

You can use the following types of file paths for file name:

Option	Description
Simple Path	You can specify files using just the file name. For example: • `SET BACKGROUND_IMAGE image1.jpg` • This assumes that the files are in the root of the file server specified in the DHCP information or set through the phone menus during installation. • The file server can also be set using `HTTPSRVR` and `TLSSVR` commands.
Relative Path	You can specify a path relative to the folder on the file server that the phone has been told to use. For example: • `SET BACKGROUND_IMAGE images/image1.jpg"` • This method is not supported when using the IP Office as the file server for phones.

Table continues…

Option	Description
Absolute Path	You can specify a path relative to the root directory of the file server, regardless of any `HTTPDIR` or `TLSDIR` settings commands to use a specific directory. For example: • `SET BACKGROUND_IMAGE /files/images/image1.jpg` • This method is not supported when using the IP Office as the file server for phones.
URL File Path	You can use files hosted on another HTTP file server by using a full URL enclosed in " " quotation marks. For example: • `SET BACKGROUND_IMAGE "http://files.example.com/image1.jpg"` • This feature requires the J100 phones to use J100 R4.1.0.0 or higher firmware. See Upgrading the J100 phone firmware on page 125).
Using Macros	You can include the following macros in a file path. The phone replaces the macro with the matching value when requesting the file: • `"$SERIALNO"` = The phone serial number in uppercase. • `"$MACADDR"` = The phone MAC address, in lowercase and without colons. • `"$MODEL4"` = The phone 4-character model number in uppercase.

Related links

Controlling the J100 Screensaver and Background Images on page 116

Chapter 21: J100 Phone Wi-Fi Support

You can add a wireless module to J159, J179, and J189 phones. That allows the phone to connect to the IP Office system through the customer's Wi-Fi network. Using Wi-Fi lets you to use the phone in a location where a wired ethernet connection is not available.

Related links

Disable user access to the J100 network settings on page 122

Enabling Wi-Fi on page 123

Enabling hidden Wi-Fi SSID support on page 123

Disable user access to the J100 network settings

By default, J100 phone users can change their phones network settings using ≡ > **Settings** > **Network**. By adding `SET ENABLE_NETWORK_CONFIG_BY_USER 0` to the `46xxspecials.txt` file, users can still access the Network menu to view but not change the current settings.

For example:

```
IF $MODEL4 SEQ J139 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J169 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J179 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J159 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J189 GOTO J1X9SPECIALS
GOT END

# J1X9SPECIALS
SET ENABLE_NETWORK_CONFIG_BY_USER 0

#END
```

The command does not affect network configuration through the **Administration** (≡ > **Administration** > **Network interfaces**).

Related links

J100 Phone Wi-Fi Support on page 122

Enabling Wi-Fi

About this task

You can use the following process to manually enable Wi-Fi connection on a J100 phone with the wireless module installed.

Procedure

1. Access the administration menu:
    a. If shown on the display, press **Admin**. Otherwise, press **More** and **Admin** or press ≡ and select **Administration**.
    b. Enter the administration password and press **Enter**. These phones do not support pressing **#** to enter the password.
2. **If you want the phone to use Wi-Fi:** Wireless connection is supported on phones with the optional Wi-Fi module installed. Select **Network interfaces**.
    a. Change the **Network mode** from **Ethernet** to **Wi-Fi**.
    b. Press **Save**. The phone scans for available wireless networks.
    c. Select the required network and click **Connect**. Press **OK**.
        - If hidden Wi-Fi is enabled (see Enabling hidden Wi-Fi SSID support on page 123), you can click scroll down and select **Add Network** to add details for connecting to a network that does not broadcast its SSID.
    d. In the **Password** field, enter the password for the wireless network and press **Wi-Fi**. If the phone is able to connect to the network, it is restarted.

Related links

J100 Phone Wi-Fi Support on page 122

Enabling hidden Wi-Fi SSID support

You can enable an **Add Network** option. J100 phones will show this at the bottom of the list of available Wi-Fi networks list.

Using this option, you can connect a J100 phone to a Wi-Fi network that is not broadcasting its SSID. To enable the **Add Network** option, add `SET ENABLE_HIDDEN_WIFI 1` to the `46xxspecials.txt` file.

- This command requires the J100 phones to run J100 R4.1.0.0 or higher firmware. See Upgrading the J100 phone firmware on page 125.

For example:

```
IF $MODEL4 SEQ J139 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J169 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J179 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J159 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J189 GOTO J1X9SPECIALS
```

```
GOT END

# J1X9SPECIALS
SET ENABLE_HIDDEN_WIFI 1

#END
```

Related links

J100 Phone Wi-Fi Support on page 122

Chapter 22: Upgrading the J100 phone firmware

When installed or upgraded, IP Office systems install the release of J100 phone firmware tested with that release of IP Office. For example, IP Office R11.1.3 installs J100 R4.0.10.3.2 firmware.

You can install an alternate release of J100 firmware. For example, to benefit from a particular fix required by your customer site, or to access a feature not included in the release installed by the IP Office.

Note:

- If you install an alternate release:
    - The IP Office system will not benefit for any changes to the J100 releases installed by IP Office as part of future upgrades.
    - On IP500 V2, recreating the SD card will remove all files relating to the alternate firmware.

Related links

Alternate J100 phone firmware features on page 125
Adding alternate J100 phone firmware on page 126
Updating a J100 phone on page 127
J100 Series Phone Upgrade Settings on page 127

Alternate J100 phone firmware features

The following features are supported by J100 firmware releases higher than the J100 R4.0.10.3.2 currently installed as part of IP Office R11.1.3.

J100 Firmware	Feature
4.0.12.1	Support of firmware for J189 phones with version 4 hardware (labeled `J189 D01B`). See J189 D01B phone support on page 112.
4.0.13.0	Increase the number of languages other than English from 4 to 6. See Adding additional languages to J100 phones on page 129.

Table continues…

J100 Firmware	Feature
4.1.0.0	Support for separate JEM24 Button module background and screensaver image setting. See JEM24 Background image control on page 118 and JEM24 Phone Screensaver Image Controls on page 119.
	Support for connecting J100 phones to Wi-Fi networks which do not broadcast their SSID. See Enabling hidden Wi-Fi SSID support on page 123.
4.1.2.0	Support absolute URLs background and screensaver image files. See Image File Paths on page 120.
	Dark or light display mode selection. See J100 Display mode on page 111.

Related links

Upgrading the J100 phone firmware on page 125

Adding alternate J100 phone firmware

About this task

This process assumes that you are using the IP Office system as the file server for J100 phone firmware. If using a separate file server, copy the new firmware files to that server.

Before you begin

Procedure

1. Unpack the J100 firmware file onto your PC.
2. Start IP Office Manager.
3. Select **File** > **Advanced** > **Embedded File Management**
4. Select the IP Office system and click **OK**.
5. In the **Folders** window, navigate to the `/disk/system/primary` (Linux-based server) or `System SD/SYSTEM/PRIMARY` (IP500 V2) folder.
6. From the PC, drag the following files from the J100 firmware to the **Files** window.
    a. Drag and drop the `J100Supgrade.txt` file. If prompted to confirm replacing an existing file, click **Yes**. When completed, click **Close**.
    b. Repeat for all the `.bin` files.
    c. Repeat for all the `.xml` files other than `release.xml`.
7. Repeat the process for any other IP Office systems in the network.

Next steps

The J100 need to load the new files and upgrade. They will do that when either:

- After being restarted. See Restarting SIP phones on page 114.
- Following their configured update policy. See J100 Series Phone Upgrade Settings on page 127.

- Note: Button modules update using files transferred from the phone. That process can take up to 3 hours after the phone has upgraded. When completed, the module prompts the user to select when the module should upgrade.

Related links

Upgrading the J100 phone firmware on page 125

Updating a J100 phone

About this task

You can use this process to make a J100 phone check for any updates to settings files, including the phone firmware.

Procedure

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

Related links

Upgrading the J100 phone firmware on page 125

J100 Series Phone Upgrade Settings

You can instruct the J100 phones to regularly check for any updates to their firmware and settings files.

Enabling the default upgrade settings

For IP Office R11.1 FP2 and higher, you can add the `NoUser` source number `ENABLE_J100_AUTO_UPDATE_POLICY` to the IP Office system configuration (see NoUser source numbers on page 25).

- This adds the following commands to the auto-generated `46xxsettings.txt` file:

```
SET AUTOMATIC_UPDATE_POLICY 1
SET AUTOMATIC_UPDATE_REBOOT_PROMPT 1
```

These instruct the phones to:

- Poll the server daily for updated settings or firmware. The default is for this to occur between 02:00 and 04:00.
- Show a reboot prompt to the user to allow or cancel the update.

Changing the upgrade settings

You can add upgrade policy settings to a `46xxspecials.txt` file on the IP Office system. If used, these settings override the default upgrade settings above if enabled.

The possible settings are:

Command	Description
`AUTOMATIC_UPDATE_POLICY`	Sets the frequency of the update checks: • `0` = Disabled (Default) • `1` = Daily • `2` = Weekly • `3` = Monthly
`AUTOMATIC_UPDATE_WINDOW`	Sets the hours during which phones check for updates. The actually time within this period is determined randomly by each individual phone. • If this command is not specified, the default is to update between 02:00 and 04:00. • To specify a different period, set the start hour and end hour with a comma between them. For example: - `AUTOMATIC_UPDATE_WINDOW 3,4` sets the update period to between 03:00 to 04:00. - `AUTOMATIC_UPDATE_WINDOW 3,3` or similar sets the update period to any time in the 24-hour period. - The period can run past midnight. For example, `AUTOMATIC_UPDATE_WINDOW 20,4` sets the update period to between 20:00 on the first day and 04:00 on the next day.
`AUTOMATIC_REBOOT_PROMPT`	Set whether the user is prompted to allow the update. • `0` = Do not prompt the user. Update during the specified `AUTOMATIC_UPDATE_WINDOW` period or otherwise between 02:00 to 04:00. • `1` = Prompt the user to allow the update or cancel it. If canceled, the phone will prompt again following the next check for updates.

Related links

Upgrading the J100 phone firmware on page 125

Chapter 23: J100 Phone language files

The text strings used on J100 phones on IP Office divide into two types as follows:

- **Avaya admin menu strings**

  The strings used after pressing ≡ or **Admin** come from the following sources:

  - English strings are part of the J100 phone firmware.
  - The IP Office auto-generated `46xxsettings.txt` file specifies 4 additional languages as `.XML` files that the phone should load.
    - The XML .files for supported languages are included as part of the IP Office software.
    - The languages specified in the auto-generated `46xxsettings.txt` file depend on the IP Office system locale. See Avaya IP Office Locale Settings.
    - For some languages, additional font file are also specified.
- **IP Office phone strings**

  Strings for IP Office specific menus, such as the **Features** menu, as provided by the IP Office through the connection to the phone.

Related links

J100 admin menu customization on page 129
IP Office Phone Language File Customization on page 131

J100 admin menu customization

You can use the following processes to change the non-IP Office strings shown on J100 phones.

Related links

J100 Phone language files on page 129
Adding additional languages to J100 phones on page 129
Creating additional J100 admin language files on page 130

Adding additional languages to J100 phones

You can override the languages specified in the `46xxsettings.txt` by adding a `SET LANGUAGES` command for each phone in the `46xxspecials.txt` file.

- By default, you can specify up to 4 language files (the phones support English by default).

- For J100 R4.0.13, you can specify up to 6 languages. See Upgrading the J100 phone firmware on page 125.

Example

The following is an example from an IP Office system's auto-generated `46xxsettings.txt` file. The command instructs the J189 phones to download language files for Spanish, French, Dutch, and German.

```
...
IF $MODEL4 SEQ J189 GOTO J189AUTOGENERATEDSETTINGS
...
# J189AUTOGENERATEDSETTINGS
SET LANGUAGES
Mlf_J189_CastilianSpanish.xml,Mlf_J189_ParisianFrench.xml,Mlf_J189_Dutch.xml,Mlf_J189_Ge
rman.xml
GOTO NONAUTOGENERATEDSETTINGS
...
```

The `SET LANGUAGES` command in this example `46xxspecials.txt` files overrides the SET LANGUAGES command above and instructs the J189 phones to download the same languages plus Italian and Dutch.

```
...
IF $MODEL4 SEQ J189 GOTO J189SPECIALS
...
# J139SPECIALS
SET LANGUAGES
Mlf_J189_CastilianSpanish.xml,Mlf_J189_ParisianFrench.xml,Mlf_J189_Dutch.xml,Mlf_J189_Ge
rman.xml,Mlf_J189_Italian.xml,Mlf_J189_Dutch.xml
GOTO NONAUTOGENERATEDSETTINGS
...
```

Notes

If the user selects a language through the phone menu that matches one supported by the IP Office for phone strings, the IP Office system will change the user **Locale** setting to match. It will then use the same language in the IP Office menus on the phone. Otherwise, those menus will match the existing system or user **Locale**.

Related links

J100 admin menu customization on page 129

Creating additional J100 admin language files

The downloadable J100 firmware sets include a language tool (`AvayaLanguageTool_SIP.xlsm`). You can use this tool in Microsoft Excel to create additional .XML language files for J100 Series phones.

Related links

J100 admin menu customization on page 129

IP Office Phone Language File Customization

You can customize the language files used for IP Office menus on 1600, 9600 and J100 Series phones.

- This does not alter the strings used in the admin menus accessed through the **A** or ≡ buttons.
    - For J100 Series phones, those are set by strings in the `Mlf_...xml` files uploaded by the phone for each language.
- You need to repeated this process following a system upgrade that includes new 1600, 9600 or J100 IP Office phone menu features.

Related links

J100 Phone language files on page 129
Getting the IP Office phone language files on page 131
Adding Custom IP Office Language Files on page 131

Getting the IP Office phone language files

About this task

You can make the IP Office system output a set of `.XML` language files, containing the current set of phone strings it is using.

Procedure

1. To the **NoUser** user, add the string **PHONE_LANGUAGES**.
2. Reboot the IP Office system.
3. During the reboot, the IP Office outputs the current language `XML` files to the `/system/temp` folder.
    - There is one `phonelanguage_NNN.xml` file for each language, where `NNN` is the language locale code used by the IP Office system.

Related links

IP Office Phone Language File Customization on page 131

Adding Custom IP Office Language Files

Note that there are separate sets of strings for 1600 Series and 9600/J100 Series phones.

Procedure

1. Download the `phonelanguage_NNN.xml` file or files that you want to edit or to use as a template for additional languages.

2. **To change the strings for the system's default locale:** This affects the IP Office phone strings for all users set with either no specific locale or set to the system's default locale.
   a. Create a copy of this base file you want to use as a template and name it just `phonelanguage_xml`.
   b. Edit the strings in the file as required.
   c. Change the 3-character language codes shown for **locale**, **baselocale** and **phonelocale** to match the system's locale.
3. **To change the strings for another locale:** This will affect the IP Office phone strings for all users set to that specific locale.
   a. Either edit the existing xml file for that language or create a new file by copying one of the existing `phonelanguage_NNN.xml` files and changing the language code in the file name.
   b. Edit the strings in the file as required.
   c. Change the 3-character language codes shown for **locale**, **baselocale** and **phonelocale** to match the user locale.
4. Set the locale in the file to the user locale in the system that you will use for users set to this language.
5. Upload the editing XML files to the system's `/system/primary` folder.
6. Reboot the system.

Related links

IP Office Phone Language File Customization on page 131

Chapter 24: J100 Series Phone Troubleshooting

The following methods can be used to monitor the operation of J100 stimulus phones.

Related links

No "Features" Menus on page 133
Monitoring on page 133
Enabling Logging on page 134

No "Features" Menus

If the J100 telephone does not receive the correct settings , it will not display the IP Office specific menus. Principally, the **Features** menu is not shown on the main screen.

If using a previously uploaded `46xxsettings.txt` file, temporarily remove it and using a browser, request the system's auto-generated version of the `46xxsettings.txt` file. Compare the two.

Whilst you could now manually update your previous version of the `46xxsettings.txt` file, we recommend that you continue to use the auto-generated file and put any custom setting required into a `46xxspecials.txt` file.

Related links

J100 Series Phone Troubleshooting on page 133

Monitoring

The J100 Series phones can be monitored in the same way as for normal SIP extensions, see Monitoring SIP Phones on page 78. However, in addition the 'stimulus' traffic can be monitored using the following trace options:

- **Filters** > **Trace Options** > **H.323** > **CCMS Send**
- **Filters** > **Trace Options** > **H.323** > **CCMS Receive**

- **Filters** > **Trace Options** > **SIP** > **SIP: Verbose**
- **Filters** > **Trace Options** > **SIP** > **SIP Stim Rx**
- **Filters** > **Trace Options** > **SIP** > **SIP Stim Tx**
- **Filters** > **Trace Options** > **SIP** > **SIP Rx**
- **Filters** > **Trace Options** > **SIP** > **SIP Tx**

Related links

J100 Series Phone Troubleshooting on page 133

Enabling Logging

About this task

The J100 Series phones support logging to a Syslog server. This is configured through the phone's administrator menus.

Procedure

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

Related links

J100 Series Phone Troubleshooting on page 133

Part 5: Vantage K100 Series Phones

Avaya Vantage™ Phones

The Avaya Vantage™ devices are Android desk phones that are supported with IP Office. The following sections provides notes on their IP Office installation and operation.

These notes should be used in conjunction with the information provided in the full Avaya Vantage™ documentation available from Avaya.

There are two types of Vantage™ phone supported:

- **Original Vantage™ Phones (V1/V2)**
  - These phones are supported with IP Office Release 11.0 and higher. Throughout this documentation they are referred to as V1/V2 phones.
- **New Vantage™ Phones (V3)**
  - These newer versions are fully supported* with IP Office Release 11.1 FP1 and higher. Throughout this documentation they are referred to as V3 phones.
    - These phones can be used with IP Office Release 11.1 SP1 but require additional configuration. Refer to Avaya product support notice PSN005725u.

Chapter 25: Avaya Vantage™ K100 Installation Overview

The Avaya Vantage™ devices are Android desk phones that are supported with IP Office Release 11.0 and higher. The following sections provides notes on their IP Office installation and operation.

These notes should be used in conjunction with the information provided in the full Avaya Vantage™ documentation available from Avaya.

Related links

Vantage K100 V1/V2 Series Phones on page 136
Vantage K100 Series Phones on page 137
Phone files on page 138
File server options on page 140
The Administrator Password on page 141
Emergency call restrictions on page 141
Power options on page 142

Vantage K100 V1/V2 Series Phones

Throughout this document, these phones are referred to as Vantage™ V1/V2 phones. These phone consists of several elements, the desk phone, optional handset modules and a dialer applications:

- **Desk Phones:** The following K100 Series phones are supported with IP Office.
  - **K155 Video Desk Phone:** This is android desk phone which incorporates both a telephone dialing pad and a landscape touchscreen. Supported from 11.0 SP1 onwards.
  - **K165 Audio Desk Phone:** This is an android portrait touchscreen desk phone designed for audio calls. The phone supports handsfree audio calls and connections a wide range of headset types.
  - **K175 Video Desk Phone:** This model is similar to the K165 but also includes an integrated camera and so can be used for both audio-only and video calls.
- **Handset Modules:**
  - **J1B1 Wired Handset Module:** This optional module provides the phone with a standard telephone handset. Note: This module is not compatible with V3 phones.

  - **J2B1 Wireless Handset Module:** This optional module provides the phone with a wireless Bluetooth handset. The handset is charged directly from its phone cradle using contactless charging.
- **Dialer Applications:** For non-IP Office Subscription systems, the dialer is enabled by the phone's **Avaya IP Endpoint** license and so does not require any user profile licenses. For IP Office Subscription systems, the dialer is enabled by the user's IP Office Subscription.
  - **Vantage Connect:** This application provides a simple telephone to make and receive calls. It supports IP Office contacts and a local call log. This application is supported with IP Office R11.0.
    - **Vantage Connect Expansion Module:** This additional application can be used with Vantage Connect dialer application to support a number of IP Office programmable button features. See The Vantage Connect Expansion Module Module App on page 174.
  - **Avaya Workplace Client:** This is a Vantage specific version of the Avaya Workplace Client client for Android devices. Supported with IP Office R11.0.4.0 and Vantage firmware R2.0.1 or higher.
    - Supported on K155, K165 and K175 phones. K155 requires Vantage 2.2 or higher.
    - No support for Avaya Spaces
- **Power Options:**
  - **K100 Power Adapter:** The Vantage phones can be powered through Power over Ethernet (PoE). However, if necessary it can be powered using this mains power adapter. See Power options on page 142.

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

- IP Office Release 11.0 and higher.
- A separate HTTP file server to host the Vantage firmware.

Related links

Avaya Vantage K100 Installation Overview on page 136

Vantage K100 Series Phones

Throughout this document, these phones are referred to as Vantage™ V3 phones. They can be recognized by a N icon bottom-right.

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

- **Desk Phones:** The following K100 V3 Series phones are currently supported with IP Office R11.1 FP1.
  - **K155 V3 Video Desk Phone:** This is android desk phone which incorporates both a telephone dialing pad and a landscape touchscreen.

  - **K175 V3 Video Desk Phone:** This is an android portrait touchscreen desk phone designed for audio calls. The phone supports handsfree audio calls and connections a wide range of headset types. The phone is available with and without an integral camera.
- **Handset Modules:**
  - **J1C1 Wired Handset Module:** This optional module provides the Vantage phone with a standard telephone handset.
  - **J2B1 Wireless Handset Module:** This optional module provides the Vantage phone with a wireless Bluetooth handset. The handset is charged directly from its phone cradle using contactless charging.
- **Dialer Application:**

  For V3 phones, the dialer application is part of the phone's firmware and does not need to be downloaded and installed separately.

  - **Vantage Connect:** This application provides a simple telephone to make and receive calls. It supports IP Office contacts and a local call log. This application is supported with IP Office R11.0.
    - **Vantage Connect Expansion Module:** This additional application can be used with Vantage Connect dialer application to support a number of IP Office programmable button features. See The Vantage Connect Expansion Module Module App on page 174.
- **Power Options:** The Vantage phones can be powered through Power over Ethernet (PoE). However, if necessary it can be powered using this mains power adapter connected to a USB Type-C socket on the phone.

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

- IP Office Release 11.1 FP1 and higher.
- A separate HTTP file server to host the Vantage firmware.

Related links

Avaya Vantage K100 Installation Overview on page 136

Phone files

The Vantage phone is configured, either manually or via DHCP option 242, with the address of a file server. That address is used by the phone to request a variety of files.

The phone requests files whenever it is restarted. By default, it also polls the file server hourly to check for updated files.

- For V1/V2 phones, the K155 phones uses separate firmware from the K165/K175 phones.
- V3 phones use separate firmware from the V1/V2 phones. However, the K155 V3 and K175 V3 use the same firmware.

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

File Type	Description

Upgrade File
`K1xxSupgrade.txt`
`K1xxBSupgrade.txt`
	This file specifies the name and version of the main firmware file. The phone will load the file if it differs from the phone's existing firmware version. The upgrade file then specifies the phone to request the settings file.

Settings File `46xxsettings.txt`*	This file specifies settings for Avaya IP (H323 and SIP) phones supported by IP Office.
Firmware Files `.tar`/`.sig`/`.sig256`	This set of files are used to upgrade the Android operating system on the phone. The name and version of the main firmware file is specified by the `K1xxSupgrade.txt` or `K1xxBSupgrade.txt` file. That first file then specifies any other firmware files that the phone should install as part of the firmware upgrade. • These files cannot be hosted by the IP Office system. Using its **HTTP Server IP Address** or **HTTP Server URI** setting, the IP Office system always redirects requests for these files to the file server specified. This is regardless of the system's **HTTP Redirection** setting. • A firmware upgrade can take up to 2 hours. During that time the phone should not be switched off. • For new installations, it may be practical to configure a temporary HTTP file server that can be used to upgrade new Vantage phones before taking them to the customer site or end user desk.
Application Files `.apk`	Through the settings files you specify the dialer mode supported by the phone and the name of the dialer application file that it should install. For V3 phones the dialer application is part of the phone firmware above. • If the name differs from the existing application file it is using, it will install the new version. • Like the firmware files above, requests to the IP Office for these files are automatically redirected using the system's **HTTP Server IP Address** or **HTTP Server URI** setting. • For phones using the Vantage Connect dialer application, the Vantage Connect Expansion Module application can also be installed. • If the dialer application is not provided from the file server, K165 and K175 phone users can select and install the application through Google Play Store (if access to Play Store is allowed).
Additional Settings File `46xxspecials.txt`	If using the auto-generated files, they may not include all the settings you require. This additional file can be used to provide the additional settings. See Example additional phone settings on page 23 and Other Vantage settings (V1/V2) on page 149.

Related links

Avaya Vantage K100 Installation Overview on page 136

File server options

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

File Server Method	Files on the IP Office	Separate HTTP/ HTTPS File Server	IP Office Settings

Dual File Servers	`K1xxSupgrade.txt`
	`K1xxBSupgrade.txt`
	`46xxsettings.txt`
		`.tar/.sig` files
		`.apk` files
			HTTP Server IP Address: The separate HTTP server's IP address.

Single File Server	-	`.tar/.sig` files
		`.apk` files
		`K1xxSupgrade.txt`
		`K1xxBSupgrade.txt`
		`46xxsettings.txt`
			HTTP Server IP Address: The separate HTTP server's IP address.
			Phone File Server Type: Set to **Custom**.

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

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

  - **Subscription Mode Systems:**

    IP Office systems running in subscription mode can be supported through the cloud-based Customer Operations Manager application provided by the same service that provides the system subscriptions. That service can also host the Vantage firmware. In that case, the **HTTP Server URI** is used rather than the **HTTP Server IP Address**.

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

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

⚠ **Warning:**

The Vantage phones request files types which by default are not recognized or handle correctly by some 3rd-party file servers. You must ensure that the file types above (`.apk`, `.sig`,`.sig256`) are listed in the MIME, media or content type settings of the file server. See Adding additional MIME file types on page 59.

Related links

Avaya Vantage K100 Installation Overview on page 136

The Administrator Password

The Vantage phones require an administrators password to be entered in order to access certain menus, for example factory defaulting the phone.

We strongly recommend that you set an administrator password before installing any Vantage phones, especially if using HTTPS. Either:

- Add **`SET ADMIN_PASSWORD <password>`** to the system's `46xxspecials.txt` file.
- Add **`SET_ADMINPSWD=<password>`** to the system's NoUser source numbers. See NoUser source numbers on page 25.

Defaulting or resetting a Vantage phone that has previously been installed on a system that did not have an admin password set is possible.

- If the original system is still available, configure it to provide an admin password as above and then reboot the phone.
- Otherwise, configure an HTTP server with a K1xxSupgrade.txt file that contains a **`SET ADMIN_PASSWORD`** command. Then change the phone's file server to point to that server. After rebooting from that file server, it should be possible to perform actions that require entry of the admin password.

Related links

Avaya Vantage K100 Installation Overview on page 136

Emergency call restrictions

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

- If the phone is logged out: If the phone is logged out, it cannot be used to make any calls including emergency calls.
- If the phone is locked: If the phone is locked, then by default it cannot be used to make any calls including emergency calls.
  - By default, the IP Office auto-generated settings file disables the screen lock function using the **ENABLE_PHONE_LOCK** command. However, this cannot be guaranteed if using non auto-generated files. Also it cannot be guaranteed if users are able to access the phone settings to manually enable the screen lock functions.
  - If the **PHNEMERGNUM** and/or **PHNMOREEMRGNUMS** commands are added to the settings files, the phone is able to make calls to the numbers specified with those commands when logged out. See Other Vantage settings (V1/V2) on page 149.

Related links

Avaya Vantage K100 Installation Overview on page 136

Power options

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

- **Power over Ethernet (PoE):**

  The power class depends on the following,

  - 802.3af: The Vantage phone acts as a Class 3 device. The phone's USB socket supports 100mA output.
  - 802.3at: The Vantage phone acts as a Class 4 device. The phone's USB socket supports 500mA output.
- **Mains Power:**
  - For V1/V2 phones, if PoE is not available, mains power can be used using an optional 48V dc. adapter. The adapter requires a suitable local main supply cable.
  - For V3 phone, mains power can be used using an options 5V/18W adapter that connects to a USB-C port on the phone.

Related links

Avaya Vantage K100 Installation Overview on page 136

Chapter 26: Vantage installation

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

Related links

Pre-Upgrading the Vantage phone firmware

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

Process	Refer to
Download and unpack the Vantage firmware onto an HTTP file server. This must be the same version of firmware that will also be used at the customer site.	Downloading the Vantage Phone Software on page 144
Edit the K1xxSupgrade.txt file to either remove the GET 46xxsetting.txt line or comment it out with ##.	-
If you are able, configure a DHCP server to provide the file server address, that removes the following steps.	-
Unbox each Vantage phone and using a PoE connection, connect the phone to the same network as the HTTP file server.	-

Table continues…

Process	Refer to
Once the phone has stated with its pre-installed factory firmware (approximately 20-minutes), change the file server address to be the HTTP file server.	Changing the file server address on page 162
After downloading the k1xxSupgrade.txt file from the file server, the phone will eventually begin upgrading its firmware.	-
When completed, check the phone's software version.	Checking the firmware version on page 166
Power off and re-box the phone.	-

Related links

Vantage installation on page 143

Downloading the Vantage Phone Software

The Vantage software (firmware and application files) is not included as part of the IP Office administration software and are not automatically installed on the IP Office system. Vantage software can be downloaded from the Avaya Support website.

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

Related links

Vantage installation on page 143

Loading Vantage files onto the file server

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

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

- **File Location:**

  If using theIP Office systems auto-generated `K1xxSupgrade.txt` and `K1xxBSupgrade.txt` files, the Vantage files need to be located in the root directory of the file server. For example on an IIS server, in the `wwwroot` folder.

  - To use a sub-folder requires you to switch to using a static files, see Using a static K1xxSupgrade.txt file (V1/V2) on page 149. That allows you to add the necessary sub-folder path to the file names that the phone's will be instructed to request.

- **MIME Types:**

  The file extensions used by the Vantage files are not supported as standard by some file servers. If that is the case, you need to add additional MIME types to the file server configuration. See Adding additional MIME file types on page 59.

Related links

Vantage installation on page 143

Adding additional MIME file types

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

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

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

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

Related links

File (Provisioning) server settings on page 52
Adding a MIME type to an IIS server on page 59
Adding a MIME type to an IIS sever configuration file on page 60
Adding a MIME type to an apache server on page 60
Vantage installation on page 143

Configuring the settings files (V1/V2)

For Vantage V1/V2 phones, the `K1xxSupgrade.txt` file that the phone requests needs to specify which dialer application the phone should support and also the specific file name (and if necessary path) for the installation file for that dialer application. It should also define a time server for the phone.

Related links

Vantage installation on page 143
Using the auto-generated files (V1/V2) on page 146
Setting the default Vantage dialer (V1/V2 only) on page 147
Modifying the auto-generated files (V1/V2) on page 148
Using a static K1xxSupgrade.txt file (V1/V2) on page 149
Other Vantage settings (V1/V2) on page 149

Using the auto-generated files (V1/V2)

The IP Office system can auto-generate the `K1xxSupgrade.txt` and `K1xxBSupgrade.txt` files. To view the file, browser to `https://<IPOffice>/<filename>.txt`

- The contents of the auto-generated file will match the firmware and dialer applications tested and supported with the release of IP Office. If necessary, settings within the IP Office configuration can be used to change the firmware versions specified in the auto-generated `K1xxSupgrade.txt` settings file. See Modifying the auto-generated files (V1/V2) on page 148
- For V1/V2 phones, the auto-generated `K1xxSupgrade.txt` file uses the default Vantage client setting configured on the system (see Setting the default Vantage dialer (V1/V2 only) on page 147) to create a file suitable for either Vantage Connect or Avaya Workplace Client clients on all Vantage phones. To support a mix of clients on the Vantage phones, a static `K1xxSupgrade.txt` file should be used. See Using a static K1xxSupgrade.txt file (V1/V2) on page 149

Vantage Connect K1xxSupgrade.txt File

The following is an example file from a system configured for Vantage Connect client support.

```
## IPOFFICE/11.1.0.1.0 build 34 192.168.0.180 AUTOGENERATED
IF $MODEL4 SEQ K175 GOTO K165_K175_SW
IF $MODEL4 SEQ K165 GOTO K165_K175_SW
IF $MODEL4 SEQ K155 GOTO K155_SW
GOTO END
# K165_K175_SW
SET APPNAME K1xx_SIP-R2_2_0_2_7042.tar
GOTO GETSET
# K155_SW
SET APPNAME K1xx_SIP-R2_2_0_2_7542.tar
GOTO GETSET
# GETSET
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"
GOTO GETSET
# GETSET
SET PUSH_APPLICATION VantageConnect_2.2.0.2.0003_300120_07d4558.apk,
AvayaConnectExpansionModule_2.2.0.1.0002_GET 46xxsettings.txt
# END
```

Avaya Workplace Client K1xxSupgrade.txt File

The following is an example file from a system configured for default Avaya Workplace Client support.

```
## IPOFFICE/11.1.0.1.0 build 35 192.168.0.36 AUTOGENERATED
IF $MODEL4 SEQ K175 GOTO K165_K175_SW
IF $MODEL4 SEQ K165 GOTO K165_K175_SW
IF $MODEL4 SEQ K155 GOTO K155_SW
GOTO END
# K165_K175_SW
SET APPNAME K1xx_SIP-R2_2_0_2_7042.tar
GOTO GETSET
# K155_SW
SET APPNAME K1xx_SIP-R2_2_0_2_7542.tar
GOTO GETSET
# GETSET
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.flare"
SET PUSH_APPLICATION "workplace-gaRelease-3.7.4.21.FA-RELEASE41-BUILD.2.apk"
GET 46xxsettings.txt
# END
```

K1xxBSupgrade.txt File

```
## IPOFFICE/11.1.1.0.0 build 151 192.168.0.180 AUTOGENERATED
IF $HWVERS SEQ 2 GOTO K1XXB_SW_EVT2
IF $HWVERS SEQ 3 GOTO K1XXB_SW_EVT2
# K1XXB_SW
SET APPNAME K1xxB_SIP-R3_0_0_0_0138.tar
GOTO GETSET
# K1XXB_SW_EVT2
SET APPNAME K1xxB_SIP-R3_0_0_0_0138_evt2.tar
# GETSET
GET 46xxsettings.txt
# END
```

Related links

Configuring the settings files (V1/V2) on page 145

Setting the default Vantage dialer (V1/V2 only)

About this task

This setting controls which Vantage dialer application, Vantage Connect or Avaya Workplace Client, should be specified in the system's auto-generated `K1xxSupgrade.txt` file for use by V1/V2 K165 and K175 phones.

Procedure

1. Open the system configuration and select **System** > **Telephony**.
2. Select the **TUI** settings.
3. Under **SIP Phone Options**, select the required **Application for Vantage**:
   - Vantage Basic/Connect: Specify the Vantage Connect client in the system's auto-generated `K1xxSupgrade.txt` file.
   - Equinox on Vantage: Specify the Avaya Workplace Client in the system's auto-generated `K1xxSupgrade.txt` file.
4. Save the settings and reboot the system.

Related links

Configuring the settings files (V1/V2) on page 145

Modifying the auto-generated files (V1/V2)

If the auto-generated `K1xxSupgrade.txt` file requires modification, this can be done through a number of NoUser source numbers. Changes can also be made to the contents of the `46xxsettings.txt` file.

K1xxSupgrade.txt

	NoUser Source Number
To set the dialer version:	This can be done using a NoUser source number to change the dialer application specified in the auto-generated `K1xxSupgrade.txt` file. • For Vantage Connect: Add **SET_VANTAGE_APK_VER=nnnn** where **nnnn** is the version that should be inserted into `Avaya_Vantage_Connect_playstore_nnnn.apk` • For example, use **SET_VANTAGE_APK_VER=1.1.0.1.0000_060318_99535a2** to change the autogenerated output to `SET PUSH_APPLICATION Avaya_Vantage_Connect_playstore_1.1.0.1.0000_060318_99535a2.apk`.
To set the firmware version:	This can be done using a NoUser source number to change the firmware specified in the auto-generated `K1xxSupgrade.txt` file: **For K165/K175 Phones:** • Add **SET_VANTAGE_FW_VER=nnnn** where **nnnn** is the version suffix that should be added to the `K1xx_SIP-Rnnnn.tar` file name. - For example, use **SET_VANTAGE_FW_VER=1_1_0_1_3119** to change the auto-generated output to `SET APPNAME K1xx_SIP-R1_1_0_1_3119.tar`. **For K155 Phones:** • Add **SET_K155_FW_VER=nnnn** where **nnnn** is the version suffix that should be added to the `K1xx_SIPRnnnn. tar` file name. - For example, use **SET_K155_FW_VER=2_0_0_0_4524** to change the auto-generated output section for the K155 to `SET APPNAME K1xx_SIP-R2_0_0_0_4524.tar`.

46xxsettings.txt

	NoUser Source Number
To set the time server:	Add **SET_VANTAGE_SNTP_SERVER=nnnn** where **nnnn** is the address of the SNTP time server. For example, `SET_VANTAGE_SNTP_SERVER=time2.google.com`
To set the Vantage administrator password:	The following NoUser source code can be used to set the Vantage phone administrator password specified in the auto-generated `46xxsettings.txt` file • Add **SET_ADMINPSWD=abcde** where **abcde** is the password required.

Related links

Configuring the settings files (V1/V2) on page 145

Using a static K1xxSupgrade.txt file (V1/V2)

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

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

In the example static `K1xxSupgrade.txt` file below, the group setting on the phones is used to select either Vantage Connect (0) or Avaya Workplace Client (1) support (see Changing the Phone's Group Setting

- Group 0 is the default group ID for new and defaulted phones. Therefore, the group 0 options in the file will act as the default dialer application selection all Vantage phones.
- However, phones configured with group 1 will load

```
## IP OFFICE K100 STATIC EXAMPLE
IF $MODEL4 SEQ K175 GOTO K165_K175_FW
IF $MODEL4 SEQ K165 GOTO K165_K175_FW
IF $MODEL4 SEQ K155 GOTO K155_FW
GOTO END
# K165_K175_FW
SET APPNAME K1xx_SIP-R2_0_0_0_4002.tar
GOTO GETAPP
# K155_FW
SET APPNAME K1xx_SIP-R2_0_0_0_4524.tar
GOTO GETAPP
# GETAPP
IF $GROUP SEQ 0 GOTO BASIC_CONNECT
IF $GROUP SEQ 1 GOTO EQUINOX
GOTO GETSET
# BASIC_CONNECT
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"
SET PUSH_APPLICATION VantageConnect_2.2.0.0.0014_101019_e833e21.apk
GOTO GETSET
# EQUINOX
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.flare"
SET PUSH_APPLICATION equinox-gaRelease-3.6.4.40.FA-RELEASE29-BUILD.22.apk
GOTO GETSET
# GETSET
GET 46xxsettings.txt
# END
```

Related links

Configuring the settings files (V1/V2) on page 145

Other Vantage settings (V1/V2)

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

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

Additional settings can be added in several ways:

- Add them to a static `46xxspecials.txt` file if using the auto-generated `K1xxSupgrade.txt` and `46xxsettings.txt` files. See 46xxspecials.txt on page 23.
- Add them to the `46xxsettings.txt` file if a static file is being used. Note however that those may be overwritten by any similar setting in a `46xxspecials.txt` file.
- Add them to the end of the `K1xxSupgrade.txt` file if a static file is being used. This has the advantage of keeping Vantage specific settings in a Vantage specific. However it risks those settings be overwritten by any similar setting in the `46xxsettings.txt` or `46xxspecials.txt` files.

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

Command	Description
GROUP	Set the group value used by the phone. The default is 0.
BRANDING_VOLUME	Sets the volume level of the Avaya connection sound. The range is 1 (low) to 8 (loud). The default is 5.
CLICKS	Sets whether the audio clicks function is on or off. The default is on (1).
USER_INSTALL_APPS_GOOGLE_PLAY_STORE	Sets whether the user can install applications from the Google Play Store. The default is off (0).
PIN_APP	Sets the name of the application locked on the screen. When an application is pinned, the user cannot switch to another application or the home or settings screens. See Application Pinning on page 168. To select the Avaya dialing application, use the same name as set for the **`ACTIVE_CSDK_BASED_PHONE_APP`** command.
UPGRADE_POLLING_PERIOD	Sets the frequency in minutes, that the phone polls its file server. The range is 0 (off) to 10080 (weekly). Additional settings can also be used to control when the phone downloads new files and when it installs those files. The default is hourly (60).
BRANDING_FILE	Specifies the URL of the branding image. When set, the image replace the Avaya log shown top-left of the dialer application screen. The image must be 142x56 pixels and in PNG, JPEG, GIF or BMP format. If using the IP Office as the file server this needs to be the full URL to the files location as this request is not redirected by the IP Office unless the file is uploaded to the IP Office.
ADMIN_PASSWORD	Set the phone administrator password. If set, this overrides any password specified by the **PROCPSWD** command.
PHNEMERGNUM	Set an emergency call number. Enter a number of up to 30 telephone dialing digits. If set, the phone's lock screen includes an **Emergency call** button. This number is the number auto-dialled from the emergency call screen. You must ensure that the number specified is correctly routed as an emergency number (using **Dial Emergency** short codes) by the IP Office system.

Table continues…

Command	Description
PHNMOREEMERGNUMS	Sets a set of emergency call numbers. Multiple numbers, separated by , commas can be entered. These numbers can then be manually dialed from the emergency calls screen. If **PHNEMERGNUM** has not been specified, then the first number in the list is also used for that function. Dialing of numbers not in this list is blocked. You must ensure that the numbers specified are correctly routed as emergency numbers (using **Dial Emergency** short codes) by the IP Office system.
TIMEZONE	Sets the phone's timezone for time and date operation. The value should be in Olson name format, for example **SET TIMEZONE Europe/London, America/Chicago or Europe/Zurich**. If not specified, the phone defaults to GMT timezone (with no Daylight Saving). The default is GMT. When set, the user can still manually change the timezone (**Settings** > **Date & time** > **Select time zone**) using the phone menus. The setting specified by the settings file appears in the user menu under the name **Default**.
WIFISTAT	Sets whether the phone user can configure WiFi settings or not. The default is on (1).

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

```
## Vantage settings
IF $MODEL4 SEQ K155 GOTO VANTAGE_COMMON
IF $MODEL4 SEQ K165 GOTO VANTAGE_COMMON
IF $MODEL4 SEQ K175 GOTO VANTAGE_COMMON
GOTO END_VANTAGE
# VANTAGE_COMMON
SET TIMEZONE Europe/London
SET CLICKS 0
SET PHNEMERGNUM 999
SET PHNMOREEMRGNUMS 911,112,9999, 9911, 99112
SET WIFISTAT 0
SET USER_INSTALL_APPS_GOOGLE_PLAY_STORE 0
SET BRANDING_FILE http://192.168.0.50/logo.png
# END_VANTAGE
```

Related links

Configuring the settings files (V1/V2) on page 145

Configuring the settings files (V3)

For Vantage V3 phones, the `K1xxBSupgrade.txt` file that the phone requests needs to specify the version of the dialer and firmware that the phone should request.

Related links

Vantage installation on page 143
Modifying the auto-generated files (V3) on page 152
Using a static K1xxBSupgrade.txt file (V3) on page 152

Modifying the auto-generated files (V3)

If the auto-generated `K1xxBSupgrade.txt` file requires modification, this can be done through a number of NoUser source numbers. Changes can also be made to the contents of the `46xxsettings.txt` file.

K1xxBSupgrade.txt

	noUser Source Number
To set the dialer version:	This can be done using a NoUser source number to change the dialer application version specified in the auto-generated `K1xxBSupgrade.txt` file. • Add **SET_VANTAGE_3_0_APK_VER=nnnn** where **nnnn** is the version that should used.
To set the firmware version:	This can be done using a NoUser source number to change the firmware specified in the auto-generated `K1xxBSupgrade.txt` file: • Add **SET_VANTAGE_3_0_FW_VER=nnnn** where **nnnn** is the version suffix that should be added to the `K1xx_SIP-Rnnnn.tar` file name.

46xxsettings.txt

	NoUser Source Number
To set the time server:	Add **SET_VANTAGE_SNTP_SERVER=nnnn** where **nnnn** is the address of the SNTP time server. For example, `SET_VANTAGE_SNTP_SERVER=time2.google.com`
To set the Vantage administrator password:	The following NoUser source code can be used to set the Vantage phone administrator password specified in the auto-generated `46xxsettings.txt` file • Add **SET_ADMINPSWD=abcde** where **abcde** is the password required.

Related links

Configuring the settings files (V3) on page 151

Using a static K1xxBSupgrade.txt file (V3)

If necessary, a static `K1xxBSupgrade.txt` file can be used. For example, when the Vantage files are located in a sub-folder on the file server rather than the file server's root folder.

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

Related links

Configuring the settings files (V3) on page 151

Initial phone startup (V1/V2 only)

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

- After applying power to a new or defaulted phone, it will go through a start-up process. This takes approximately between 4 to 20 minutes.
- When completed, the phone displays the "Avaya Vantage" logo and time/date.
- Wait a couple of minutes. This is important as the phone may still have further downloads to complete.
- If the ⤓ icon appears in the status bar, the phone is downloading additional files. This may include downloading the configured phone dialer application and/or downloading updated firmware.
    - Dialer Application: If a new dialer application is downloaded, the phone displays a message prompting you whether to install the application now or later.
        1. Allow the application to be installed now. After installing it the phone will reboot.
        2. After the reboot completes, again wait a couple of minutes and then check that there are no further downloads in progress. If there are further downloads in progress, it indicates that the phone is downloading updated firmware.
    - System Update: An update of the phone's firmware can take up to 2 hours. Do not power off the phone during this process.
- Once all application and firmware updates have been completed, you can continue with the initial phone start-up. The screen background varies depending on whether the phone was able to obtain its configuration files
    - **Blurred Office Workers Background:** The phone has obtained the settings file and installed the dialer application. See Blurred office workers background (V1/V2 only) on page 153.
    - **Grey or Blue Background:** The phone has not automatically obtained the settings file. It needs to be manually configured with the address of the file server. See Manually configure a new phone (V1/V2) on page 154.

Related links

Vantage installation on page 143

Blurred office workers background (V1/V2 only)

This screen usually indicates that the phone has downloaded the required settings and application files from the file server. This may occur automatically if the address is provided via DHCP. address.

Proceed to logging in. See:

- Logging in with Vantage Connect (V1/V2 only) on page 157
- Logging in with Avaya Workplace Client (V1/V2 only) on page 157

Related links

Vantage installation on page 143

Manually configure a new phone (V1/V2)

About this task

This task is required on a new or factory defaulted (see Factory defaulting a connected phone on page 164) phone. It sets basic details, how the phone should connect to the network and the file server address for the `K1xxSupgrade.txt` file.

Procedure

1. Swipe up on the padlock icon on the screen. The Android setup menu **Welcome** screen is displayed.
2. If required, click on **English (United States)** and select the language required.
3. Click **START**.
4. Select how the phone should connect to the network.
    - **To use the network cable connection:** Leave **Ethernet Mode** selected and click **Next**.
    - **To use Wi-Fi:** Click **Wi-Fi Mode** and click **Next**. The phone searches for available wireless networks.
        a. Click on the wireless network that the phone should use.
        b. Enter the network password and click **CONNECT**.
5. From the **Copy apps & data** menu click **Set up as new**.
6. Enter details of the user's Google email account. This is optional. However, if an account is not entered, various features are disable. To skip entry click **Skip**.
7. Scroll through the Google services, changing any settings if required and then click **ACCEPT**.
8. Add any other email accounts that you want associated with the phone. This can include non-Google accounts.
9. Click **DONE FOR NOW**.
10. Enter the file server address and click **Next**. The address to enter depends on how you configured the file server options. See Phone files on page 138.
    - Prefix the address with `https://`. If not specified or if `http://` is used, the phone's will not be able to obtain contacts and directory information from the IP Office unless HTTP Directory Read is enabled in the IP Office system's security settings.

- **Dual File Servers: (IP Office and 3rd-Party File Server)**
    - If using `K1xxSupgrade.txt`/`K1xxBSupgrade.txt` and `46xxsettings.txt` files from the IP Office system, enter the system's address prefixed with `https://`. This method requires that system has a its HTTP Server IP Address set to the address of the 3rd-party HTTP file server that is hosting the other Vantage firmware files. Not prefixing the address with `https://` will cause the phone to not be able to obtain directory contacts (see Error syncing IP Office Contacts on page 173).
- **Single File Server: (3rd-Party File Server)**
    - If all the files for the Vantage phones are on the same server, enter the address of that server. This requires the `46xxsettings.txt` file on that server to be manually configured with setting that match the IP Office system's SIP configuration and set the IP Office as the SIP Proxy for the Vantage phones.

11. The phone may need to restart several times as it loads updated firmware files and then the Avaya dialer application.

Next steps

When completed, the phone should restart with the blurred office workers background. See Blurred office workers background (V1/V2 only) on page 153.

Related links

Vantage installation on page 143

Manually configure a new phone (V3)

About this task

This task is required on a new or factory defaulted (see Factory defaulting a connected phone on page 164) phone. It sets basic details, how the phone should connect to the network and the file server address for the `K1xxBSupgrade.txt` file.

Procedure

1. If required, click on **English (United States)** and select the language required.
2. Click **Next**.
3. Select how the phone should connect to the network.
    - **To use the network cable connection:** Leave **Ethernet Mode** selected and click **Next**.
    - **To use Wi-Fi:** Click **Wi-Fi Mode** and click **Next**. The phone searches for available wireless networks.
        a. Click on the wireless network that the phone should use.
        b. Enter the network password and click **CONNECT**.
4. Click **Skip**.

5. Select **Manual Configuration** and click **Next**.
6. Enter the file server address and click **Next**. The address to enter depends on how you configured the file server options. See Phone files on page 138.
    - Prefix the address with `https://`. If not specified or if `http://` is used, the phone's will not be able to obtain contacts and directory information from the IP Office unless HTTP Directory Read is enabled in the IP Office system's security settings.
    - **Dual File Servers: (IP Office and 3rd-Party File Server)**
        - If using `K1xxSupgrade.txt`/`K1xxBSupgrade.txt` and `46xxsettings.txt` files from the IP Office system, enter the system's address prefixed with `https://`. This method requires that system has a its HTTP Server IP Address set to the address of the 3rd-party HTTP file server that is hosting the other Vantage firmware files. Not prefixing the address with `https://` will cause the phone to not be able to obtain directory contacts (see Error syncing IP Office Contacts on page 173).
    - **Single File Server: (3rd-Party File Server)**
        - If all the files for the Vantage phones are on the same server, enter the address of that server. This requires the `46xxsettings.txt` file on that server to be manually configured with setting that match the IP Office system's SIP configuration and set the IP Office as the SIP Proxy for the Vantage phones.
7. The phone may need to restart as it loads any updated files from the file server.

Next steps

When completed, the phone should restart. You can now sign in to the dialer. See Logging in the Vantage Connect (V3 only) on page 156.

Related links

Vantage installation on page 143

Logging in the Vantage Connect (V3 only)

Procedure

1. Click on the **Sign In** icon shown on the main screen.
2. For the **Username**, enter the user's extension number.
3. For the **Password**, enter the user's password.
4. The first time you login, a software license screen is displayed. Click **Accept**.
5. The first time you log in, you will be prompted to allow access to various services. Allow this.

Result

The Vantage Connect dial pad screen is displayed.

Related links

Vantage installation on page 143

Logging in with Vantage Connect (V1/V2 only)

Procedure

1. Swipe the padlock icon up the screen.
2. For the **Username**, enter the user's extension number.
3. For the **Password**, enter the user's password.
4. The first time you login, a software license screen is displayed. Click **Accept**.
5. The first time you log in, you will be prompted to allow access to various services. Allow this.

Result

The Vantage Connect dial pad screen is displayed.

Related links

Vantage installation on page 143

Logging in with Avaya Workplace Client (V1/V2 only)

Procedure

1. Swipe the padlock icon up the screen.
2. For the **Username**, enter the user's extension number.
3. For the **Password**, enter the user's password.
4. The first time you login, a software license screen is displayed. Click **Accept**.
5. The first time you log in, you will be prompted to allow access to various services. Allow this.
6. Click **Next** to move through the screens and then **Done** when finished or press **Skip** to exit the introduction.

Result

The Avaya Workplace Client home screen is displayed.

Related links

Vantage installation on page 143

Chapter 27: Bluetooth handset operation

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

- The handset has integrated power, mute, volume up and volume down buttons.
- The nominal range is 10m in clear-air.
- The handset automatically powers off if out of range or unable to detect the Vantage phone for over 20 minutes.
- The handset charges using contactless charging when placed in its cradle.
- Full charging takes approximately 3 hours. When fully charged the handset has a talk time of 12 hours and and standby time of 60 hours.
- The handset cradle includes a magnetic hook switch that can be used to start, end and answer calls.
- The handset includes a status lamp. See Handset lamp on page 159.

Related links

Pairing the bluetooth handset on page 158
Associating the Bluetooth handset on page 159
Handset lamp on page 159

Pairing the bluetooth handset

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

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

Related links

Bluetooth handset operation on page 158

Associating the Bluetooth handset

Procedure

1. Access the phone settings using the ⚙ icon if visible. Otherwise:
   a. Swipe down from the top of the display to show the status bar.
   b. Swipe down again to show the quick settings menu.
   c. Click on the ⚙ icon.
2. On the handset, press and hold the power button. Keep it pressed until the handset lamp flashes regularly. This indicate it is in pairing mode.
3. Select **Bluetooth**.
4. Change the setting to **On**. The phone scans for available Bluetooth devices.
5. When the handset is shown in the list of Bluetooth devices (**Avaya J100-02AE11** or similar), click on it and select **Connect**.
6. The 🔋 icon appears in the status bar, showing that the handset is connected and its charge level.

Related links

Bluetooth handset operation on page 158

Handset lamp

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

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

Related links

Bluetooth handset operation on page 158

Chapter 28: Additional Vantage Phone Processes

The following additional processes can be used with Vantage phones.

Related links

Switching to wireless connection on page 161
Rebooting a Vantage phone on page 162
Changing the file server address on page 162
Changing the phone's group setting on page 163
Clearing the user data on page 164
Factory defaulting a connected phone on page 164
Factory defaulting an unconnected phone on page 165
Checking the firmware version on page 166
Checking the dialer application version on page 166
Starting an immediate upgrade on page 167
Application Pinning on page 168
Vantage Headsets (V1/V2) on page 168
Vantage Headsets (V3) on page 169

Switching to wireless connection

About this task

The Vantage phone can be connected to the network using a wireless Wi-Fi connection.

Procedure

1. Access the phone settings using the ⚙ icon if visible. Otherwise:
    a. Swipe down from the top of the display to show the status bar.
    b. Swipe down again to show the quick settings menu.
    c. Click on the ⚙ icon.
2. Click **Network & Internet**.
3. The current mode is displayed under **Network Mode**.

4. To change mode, click **Network Mode** and select the mode required. The phone displays a VoIP services error message until you complete the network configuration.
5. Click **Wi-Fi** once the option is no longer grayed out, this may take a couple of seconds.
6. Select the require wireless network.
7. Enter the network password and click **CONNECT**.

Related links

Additional Vantage Phone Processes on page 161

Rebooting a Vantage phone

About this task

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

Procedure

1. Access the phone settings using the ⚙ icon if visible. Otherwise:
   a. Swipe down from the top of the display to show the status bar.
   b. Swipe down again to show the quick settings menu.
   c. Click on the ⚙ icon.
2. Select **System**.
3. Select **Reset options**.
4. Select **Reboot**.
5. Select **Yes**. The phone restarts.

Related links

Additional Vantage Phone Processes on page 161

Changing the file server address

About this task

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

Procedure

1. Access the phone settings using the ⚙ icon if visible. Otherwise:
   a. Swipe down from the top of the display to show the status bar.
   b. Swipe down again to show the quick settings menu.

c. Click on the ⚙ icon.

2. Select **Network & Internet**.
3. Select **More**.
4. Click on **File Server** and enter file server address.

   This should be the server configured to provide files for the phone. In most scenarios that will be the IP Office system.

   - Prefix the address with `https://`
   - For cloud based systems include **:411** as a suffix.
5. Click **OK**.
6. Exit the settings.

Result

The new value is used the next time the phone polls for software or is rebooted. See Rebooting a Vantage phone on page 162.

Related links

Additional Vantage Phone Processes on page 161

Changing the phone's group setting

About this task

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

For example, see the example static `K1xxSupgrade.txt` file which uses group values to select either Vantage Connect or Avaya Workplace Client.

Note:

The new setting will not take effect until the phone polls for software (by default once per hour) or is rebooted

Procedure

1. Access the phone settings using the ⚙ icon if visible. Otherwise:
   a. Swipe down from the top of the display to show the status bar.
   b. Swipe down again to show the quick settings menu.
   c. Click on the ⚙ icon.
2. Select **Network & Internet**.
3. Select **More**.

4. Click on **Group** and enter group number that the phone should use.
5. Click **OK**.
6. Exit the settings.

Result

The new value is used the next time the phone polls for software or is rebooted. See Rebooting a Vantage phone on page 162.

Related links

Additional Vantage Phone Processes on page 161

Clearing the user data

About this task

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

Procedure

1. Access the phone settings using the ⚙ icon if visible. Otherwise:
   a. Swipe down from the top of the display to show the status bar.
   b. Swipe down again to show the quick settings menu.
   c. Click on the ⚙ icon.
2. Click on the ⋮ icon.
   a. Select **Admin login**.
   b. Enter the administrator password (see The Administrator Password on page 141) set for Vantage phones on the IP Office system and click **OK**.
3. Select ☁ **Backup & reset**.
4. Select **Clear user data**.
5. Click **Yes**.

Related links

Additional Vantage Phone Processes on page 161

Factory defaulting a connected phone

About this task

This process can be used with a phone that is still connected to a system. It returns the phone state similar to a new out-of-the box device.

It removes all user data and settings. It also removes any applications and certificates not loaded as part of phone firmware. If you just want to clear the existing user data and applications, select Clear user data instead.

This process takes approximately 20 minutes to complete.

Procedure

1. Access the phone settings using the ⚙ icon if visible. Otherwise:
    a. Swipe down from the top of the display to show the status bar.
    b. Swipe down again to show the quick settings menu.
    c. Click on the ⚙ icon.
2. Click on the ⋮ icon.
    a. Select **Admin login**.
    b. Enter the administrator password (see The Administrator Password on page 141) set for Vantage phones on the IP Office system and click **OK**.
3. Select **System**.
4. Select **Reset options**.
5. Select **Factory data reset**.
6. Select **RESET DEVICE**.
7. Select **ERASE EVERYTHING**.

Result

The phone will power off and then restart.

Related links

Additional Vantage Phone Processes on page 161

Factory defaulting an unconnected phone

About this task

This process can be used with a phone that is no longer connected to a system. It returns the phone state similar to a new out-of-the box device.

It removes all user data and settings. It also removes any applications and certificates not loaded as part of phone firmware. If you just want to clear the existing user data and applications, select **Clear user data** instead.

This process takes approximately 20 minutes to complete.

Procedure

1. Connect an external USB keyboard to the device.

If the keyboard is USB Type-A, then you require a USB Type-A to Type-C adapter to connect to the USB Type-C port on the phone.

2. Reboot the device.
3. Press and hold the volume Up key whilst the phone reboots. After the boot, the phone displays its **Recovery** menu.
4. Select **BRM** to navigate to boot recovery menu options.
5. Enter the administrator password using the external USB keyboard connected to the device.
6. Select **Wipe data/factory reset**.

Related links

Additional Vantage Phone Processes on page 161

Checking the firmware version

Procedure

1. Access the phone settings using the ⚙ icon if visible. Otherwise:
   a. Swipe down from the top of the display to show the status bar.
   b. Swipe down again to show the quick settings menu.
   c. Click on the ⚙ icon.
2. Scroll down to the **System** section.
3. Select **About Avaya Vantage**.

Result

The information displayed includes the software version and build number.

Related links

Additional Vantage Phone Processes on page 161

Checking the dialer application version

Procedure

1. Within the application, click on the user name and extension number.
2. Select **Support** and then **About**.

Result

Details of the dialer application version are displayed.

Related links

[Additional Vantage Phone Processes](#) on page 161

Starting an immediate upgrade

About this task

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

Important:

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

Procedure

1. Access the phone settings using the ⚙ icon if visible. Otherwise:
    a. Swipe down from the top of the display to show the status bar.
    b. Swipe down again to show the quick settings menu.
    c. Click on the ⚙ icon.
2. Click on the ⋮ icon.
    a. Select **Admin login**.
    b. Enter the administrator password (see [The Administrator Password](#) on page 141) set for Vantage phones on the IP Office system and click **OK**.
3. Scroll down to the **System** section.
4. Select **About Avaya Vantage**.
5. Select **Software information**.
6. The information under **Update now** shows when the phone last checked for updated firmware.
7. If updated firmware is available, click **Update now** option to start an immediate upgrade.

Related links

[Additional Vantage Phone Processes](#) on page 161

Application Pinning

About this task

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

You can turn application pinning on or off through the dialer applications own settings using the Vantage administrator password. The settings command `SET PIN_APP` can also be used to pin the application by default.

Procedure

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

Related links

Additional Vantage Phone Processes on page 161

Vantage Headsets (V1/V2)

The Vantage phones support a range of methods for headset attachment.

In addition to the Avaya L100 range of headsets, the following headsets are tested and supported by Avaya. Refer to the release notes with the phone firmware for any updates.

Other headsets may also work but have not been tested by Avaya.

Headset Port	Support Headsets
RJ9 Telephony Headsets This is a standard telephony headset port. It is located on the back of phone and marked as **Ɔ**.	Plantronics HW251N \ HW261N (HIS), HW291N \ HW301N (HIS) Sennheiser SH 330\350, CC510\550 \ Circle TM SC 230\260 \ Century TM SC 630\660 (CAVA-31) Jabra BIZ TM 2400 (GN1216), GN2000 (GN1216) VXI CC PRO TM 4010V DC, CC PRO TM 4021V DC (OmniCord-V)

Table continues…

Headset Port	Support Headsets
3.5mm Audio Jack Headsets This is a headset port for traditional computer/audio headsets. The port is located on the right hand side of the Vantage phones	Apple Samsung Jabra Evolve Plantronics Blackwire 315/325 headset
Bluetooth Headsets The Vantage phones all support Bluetooth and the use of Bluetooth headsets	Jabra Speak 510 Jabra Extreme Jabra GO6400 Plantronics Pro Plantronics UC Pro Plantronics Blackwire C710

Related links

Additional Vantage Phone Processes on page 161

Vantage Headsets (V3)

The Vantage 3 phones support a range of methods for headset attachment.

In addition to the Avaya L100 range of headsets, the following headsets are tested and supported by Avaya. Refer to the release notes with the phone firmware for any updates.

Other headsets may also work but have not been tested by Avaya.

Headset Port	Support Headsets
USB Headsets	Avaya B109, B129, B199 Plantronics C3210 USB Plantronics C3210 USB Plantronics Encore pro 510,520 Plantronics Starset H31CD Plantronics Savi W710 Jabra Evolve

Table continues…

Headset Port	Support Headsets
RJ9 Telephony Headsets This is a standard telephony headset port. It is located on the back of phone and marked as **Ↄ**.	Jabra JN200 Plantronics HW251N \ HW261N (HIS), HW291N \ HW301N (HIS) Sennheiser SH 330\350, CC510\550 \ Circle TM SC 230\260 \ Century TM SC 630\660 (CAVA-31) Jabra BIZ TM 2400 (GN1216), GN2000 (GN1216) VXI CC PRO TM 4010V DC, CC PRO TM 4021V DC (OmniCord-V)
3.5mm Audio Jack Headsets This is a headset port for traditional computer/audio headsets. The port is located on the right hand side of the Vantage phones	Apple AKG Samsung Jabra Evolve Plantronics Blackwire 315/325 Plantronics 5220
Bluetooth Headsets The Vantage phones all support Bluetooth and the use of Bluetooth headsets	Avaya B109, B129, B199 Plantronics Savi W700 Jabra 510

Related links

Additional Vantage Phone Processes on page 161

Chapter 29: Vantage Phone Error Messages

The following error messages may appear.

Related links

"The configured phone application was not found" on page 171
"Please note Vantage is not functional ..." on page 171
BT handset is not paired on page 172
Red Screen/Enter PIN Code on page 172
Error syncing IP Office Contacts on page 173

"The configured phone application was not found"

Likely causes of this error message are:

- A mismatch between the name of the `.apk` file specified in the `46xxsettings.txt` file and the `.apk` file on the file server. See Configuring the settings files (V1/V2) on page 145.
- The specified file is not on the file server.
- The file server is not reachable.
- An error, such as a loop in the settings file, has caused the phone to timeout.

Related links

Vantage Phone Error Messages on page 171

"Please note Vantage is not functional ..."

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

Check that the settings files loaded by the phone:

- `K1xxSupgrade.txt`
- `K1xxBSupgrade.txt`

- `46xxsettings.txt`
- `46xxspecials.txt`

include the command **`SET ACTIVE_CSDK_BASED_PHONE_APP com.avaya.android.vantage.basic`**. See Configuring the settings files (V1/V2) on page 145.

Following any correction to the settings file reboots the phone

Related links

Vantage Phone Error Messages on page 171

BT handset is not paired

Likely causes of this error message are:

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

Related links

Vantage Phone Error Messages on page 171

Red Screen/Enter PIN Code

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

- For new/defaulted Vantage phones.
- For existing Vantage phones that have been working, the most likely cause is an error in the current settings files making the installed dialler application invalid. Login using the user's IP Office password. Then refer to "Please note Vantage is not functional ..." on page 171.

Related links

Vantage Phone Error Messages on page 171

Error syncing IP Office Contacts

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

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

Use the same procedure for IP Office contacts directory not available error.

Related links

Vantage Phone Error Messages on page 171

Chapter 30: The Vantage Connect Expansion Module Module App

The Vantage Connect Expansion Module application supports programmable button features configured for a user in the IP Office configuration.

- The application is only supported with the Vantage Connect dialer application. That includes V3 phones.
- The application is supported with IP Office R11.1 SP1 and higher when using Vantage™ 2.2 SP3 firmware or higher.
- The application can be run on the same Vantage™ device as the Vantage Connect dialer app and/or separately on up to 3 other Vantage™ devices.
  - On K165/K175 phones, the application can display up to 5 pages of 24 buttons per page.
  - On K155 phones, the application can display up to 5 pages of 8 buttons per page.

Related links

Vantage Connect Expansion Installation on page 174
Connecting to the Expansion Module Application on page 175
Supported IP Office Button Actions on page 177

Vantage Connect Expansion Installation

Installation of the Vantage Connect Expansion Module application onto a Vantage device is done by adding the expansion module APK file name to a `SET PUSH_APPLICATION` string in the same way as the Vantage Connect application. The `SET PUSH_APPLICATION` string for particular phones can be varied in order to install either both applications or just the Vantage Connect Expansion Module application.

Running just the Vantage Connect Expansion Module application on the Vantage device allows that device to be used without having to be logged in on the IP Office system using a user account. Instead the Vantage Connect Expansion Module application is associated with the logged in Vantage Connect application running on another Vantage device.

Example K1xxSupgrade.txt File

In the following example, Vantage devices can optionally be configured to load just the Vantage Connect Expansion Module application.

Vantage devices using the default Group value of 0, use the details in the `# GETCONNECT` section. That instructs them to load both the Vantage Connect and Vantage Connect Expansion Module applications. Note how the .apk files for both applications are defined as a single string with just a comma separating them.

The `# GETMODULEONLY` section is used by Vantage devices which have their Group value set to 1 (see Changing the phone's group setting on page 163). That section instructs those devices to only download the Vantage Connect Expansion Module application and can be used without requiring a IP Office login and therefore no user registration or license/subscription requirement. Note how the `SET ACTIVE_CSDK_BASED_PHONE_APP` string is still defined though with an empty "" value.

Example for V1/V2 Phones

```
IF $MODEL4 SEQ K175 GOTO K165_K175_SW
IF $MODEL4 SEQ K165 GOTO K165_K175_SW
IF $MODEL4 SEQ K155 GOTO K155_SW
GOTO END
# K155_SW
SET APPNAME K1xx_SIP-R2_2_0_3_7553.tar
GOTO GETBM
# K165_K175_SW
SET APPNAME K1xx_SIP-R2_2_0_3_7053.tar
GOTO GETBM
# GETBM
IF $GROUP SEQ 0 GOTO GETCONNECT
IF $GROUP SEQ 1 GOTO GETMODULEONLY
GOTO GETSET
# GETCONNECT
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"
SET PUSH_APPLICATION VantageConnect_2.2.apk,AvayaConnectExpansionModule_2.2.apk
GOTO END
# GETMODULEONLY
SET ACTIVE_CSDK_BASED_PHONE_APP ""
SET PUSH_APPLICATION AvayaConnectExpansionModule_2.2.apk
GOTO END
# END
GET 46xxsettings.txt
```

Related links

The Vantage Connect Expansion Module Module App on page 174

Connecting to the Expansion Module Application

Full details of using the Vantage Connect Expansion Module application, including connecting to the application running on another Vantage device, refer to the *"Using Avaya Vantage Connect"* user guide. The following is a simple summary for Vantage phones running on the same internal network.

Related links

The Vantage Connect Expansion Module Module App on page 174
Using the Expansion Module App on the same phone on page 176
Using Network Discovery to Connect an Expansion App on page 176
Connecting Using the Expansion Module IP Address on page 177

Using the Expansion Module App on the same phone

About this task

If both applications have been installed on the same Vantage device, they can both be run at the same time. This does not prevent the Vantage Connect device also connecting to Vantage Connect Expansion Module running on another device.

Procedure

1. Within Vantage Connect, click on the user name drop-down and select **User Settings**.
2. Select **Expansion Module**.
3. Enable **Expansion Module**.
4. Swipe up and access the desktop.
5. Click on the **Vantage Connect Expansion Module** app.
6. Select **CONNECT TO THIS DEVICE**.
7. Select **ALWAYS USE THIS DEVICE**.
8. The top-left icon in both applications shows a **<**, meaning it can now be clicked to switch between the Vantage Connect and Vantage Connect Expansion Module apps.

Related links

Connecting to the Expansion Module Application on page 175

Using Network Discovery to Connect an Expansion App

About this task

This method of connection can be used when both Vantage devices are on the same local network.

Before you begin

Procedure

1. Within Vantage Connect, click on the user name drop-down and select **User Settings**.
2. Select **Expansion Module**.
3. Enable **Expansion Module**.
4. Note the **Network Discovery Name**.
5. Click on **Network Discovery**. This allows the Vantage Connect device to be found by Vantage Connect Expansion Module devices on the same network for the next minute.
6. On the Vantage Connect Expansion Module device, click on the Vantage Connect Expansion Module app.
7. Click **CONNECT TO A NEARBY DEVICE**.
8. In the list of available devices, click on the one with the same network discovery name as Vantage Connect device above.

9. Select **ALWAYS USE THIS DEVICE**.
10. On the Vantage Connect device, select **Yes**.
11. The Vantage Connect Expansion Module application should now show the same user name and any supported programmable buttons in the user's IP Office configuration.

Related links

Connecting to the Expansion Module Application on page 175

Connecting Using the Expansion Module IP Address

About this task

This method of connection can be used when both Vantage devices are on the same local network or on networks between which there is appropriate routing.

Procedure

1. Within Vantage Connect, click on the user name drop-down and select **User Settings**.
2. Select **Expansion Module**.
3. Enable **Expansion Module**.
4. Note the **Network Discovery Name**.
5. Note the address shown under **Network Discovery**.
6. On the Vantage Connect Expansion Module device, enter the address in the address box and then click **CONNECT USING IP ADDRESS**.
7. Select **ALWAYS USE THIS DEVICE**.
8. On the Vantage Connect device, select **Yes**.
9. The Vantage Connect Expansion Module application should now show the same user name and any supported programmable buttons in the user's IP Office configuration.

Related links

Connecting to the Expansion Module Application on page 175

Supported IP Office Button Actions

The following table describes the IP Office button actions supported on a Vantage Connect Expansion Module.

- The buttons are applied in rows, top to bottom. This differs from the order used on other Avaya phones where buttons are applied in columns, left to right.
- Buttons configured for unsupported features are not displayed in the button layout shown by the Vantage Connect Expansion Module application.
- Within the Vantage Connect Expansion Module application, the Settings options are local to the device on which they are changed. In addition, the Edit Layout and Labels function can

only be used to edit the label displayed on a button and are also local to the device. However, they can be overwritten by IP Office configuration changes. All other actions to add, remove or change button settings should be done through a IP Office application.

- The operation of the buttons can differ from the same action on an Avaya phone. See the notes on the supported button actions below
- When the action data is indicated as optional, if no value is set for the button, the Vantage Connect Expansion Module prompt the user for a value when the button is pressed.

Button Actions

Action	Description
Call Record	This type of button allows the user to start/stop manual recording a call of which they are part. This is usable as long as no other user in the call has enables privacy. The button does not affect any automatic call recording of the same call or manual recording triggered by other party on call. • Path: **Advanced** > **Call** > **Call Record** • Action Data: None. • Default Label: `Record`
Cancel All Forwarding	This type of button cancels all active forwarding (on busy, on no answer and unconditional). It also cancels do not disturb. The button does not affect twinning. • Path: **Advanced** > **Call** > **Cancel All Forwarding** • Action Data: None. • Default Label: `FwdOff`
Conference Add	This type of button allows the user to add another party to an existing call. When answered, the other party is added to the call creating a conference. The button can then be used to add further parties to the conference. • Path: **Advanced** > **Call** > **Conference Add** • Action Data: None. • Default Label: `Conf.Add`
Dial	This type of button dials the stored number. It must be programmed with a complete number, partial or abbreviated dialing is not supported. The number can be matched to a user or system short codes to trigger other functions not specifically supported as Vantage Connect Expansion Module button action. • Path: **Dial** • Action Data: Telephone number. • Default Label: `Dial`

Table continues…

Action	Description
Dial Direct	This type of button allows the user to call an extension and have the call automatically answered on speaker phone after 3 beeps. If used to call a phone that is already on a call, or which does not support handsfree auto-answer, the call is presented as a normal call. • Path: **Advanced** > **Dial** > **Dial Direct** • Action Data: Extension number. • Default Label: `Dial Direct`
Dial Paging	This type of button allows the user to page an extension or group. The call is automatically connected to all phones that support handsfree auto-answer and are not already connected on another call. • Path: **Advanced** > **Dial** > **Dial Paging** • Action Data: Extension number. • Default Label: `Page`
Do Not Disturb On	This type of button puts the user into do not disturb (DND) mode. When on, all callers, except those from numbers in the user's DND exception list, either hear busy tone or are redirected to voicemail if available. • Path: **Advanced** > **Do Not Disturb** > **Do Not Disturb On** • Action Data: None. • Default Label: `DND`
Forward On Busy On	This type of button enables forwarding when the user's extension is busy. It uses their forward on busy number if set. Otherwise, it used the forward number if set. If the user has call appearance buttons programmed, the system does not treat them as busy until all their call appearance buttons are in use. • Path: **Advanced** > **Forward** > **Forward On Busy On** • Action Data: None. • Default Label: `FwdBusy`
Forward Busy Number	This type of button sets the number to which the user's calls are forwarded when either forward on busy or forward on no answer are enabled. If no forward on busy number is set, those functions use the forward number if set. Setting a number does not activate forwarding; that can be done using **Forward On Busy On** and **Forward On No Answer On** buttons. • Path: **Advanced** > **Forward** > **Forward Busy Number** • Action Data: Telephone number. • Default Label: `FwbNo`

Table continues…

Action	Description
Forward On No Answer On	This type of button enables forwarding when the user's extension is not answered within their no answer time. It uses their forward on busy number if set. Otherwise it used the forward number if set. Control of whether internal calls are forwarded is configurable through the user's system settings or through the phone menus on some Avaya phones. • Path: **Advanced** > **Forward** > **Forward On No Answer On** • Action Data: None. • Default Label: `FwdNoA`
Forward Number	This type of button is used to sets the number to which the user's calls are redirected when forward unconditional is enabled. The number can be an internal or external number. Setting a number does not activate forwarding; that is done using a **Forward Unconditional On** button (see below). The number is also used for forward on busy and forward on no answer (when enabled) if no separate forward on busy number is set. • Path: **Advanced** > **Forward** > **Forward Number** • Action Data: Telephone number. • Default Label: `FwdNo`
Forward Unconditional On	This type of button allows the user to switch the forwarding of all calls on/off. In order to use this feature a forwarding number must be set (see above). Control of whether internal/hunt group calls are forwarded and use of forwarding to voicemail are configurable through the user's system settings or through the phone menus on some Avaya phones. • Path: **Advanced** > **Forward** > **Forward Unconditional On** • Action Data: None. • Default Label: `FwdUnc`
Hunt Group Enable	This type of button allows the user to enable/disable their membership of the configured hunt group. • The user must be a member of the hunt group and be allowed to change their membership status for the group through the system's **User** > **Menu Programming** > **Huntgroup** settings. • The Vantage Connect Expansion Module does not support using the button to enable/disable member of all groups. • Path: **Advanced** > **Hunt Group** > **Hunt Group Enable** • Action Data: Hunt group extension number. • Default Label: `HGEna`

Table continues…

Action	Description
Extn Logout	This type of button logs the user off the phone Vantage device. • Path: **Advanced** > **Extension** > **Extn Logout** • Action Data: None. • Default Label: `Logout`
Priority Call	This type of button allows the user to call another user even when that other user has 'do not disturb' set. Priority calls still follow the forwarding and twinning settings of the target extension but do not go to voicemail. That is, at the target user's no answer timeout, the call continues alerting unless forward on no answer is set. • Path: **Advanced** > **Call** > **Priority Call** • Action Data: Extension number (Optional). • Default Label: `PCall`
Ringback When Free	This type of button can be used during a call to set an automatic callback on another extension that has been called whilst that extension is alerting. Once set, when that extension next ends a call or call attempt, the system will ring the Vantage user. When answered, it makes a new call to the original target extension. This feature is also called 'ringback when free' and 'ringback when next used'. When pressed at other times, a list of any currently set ringback numbers is shown and individual numbers can be deleted from that list. • Path: **Advanced** > **Miscellaneous** > **Ringback When Free** • Action Data: None. • Default Label: `AutoCB`
Send All Calls	This type of button works the same as a DND button. See the description above. • Path: **Emulation** > **Send All Calls** • Action Data: None. • Default Label: `DND`
Twinning	This type of button allows the user to turn on/off mobile twinning and to set the twinning destination number. To use this type of button the user must be configure for Mobile Twinning in the IP Office configuration. • During number entry, the Vantage Connect Expansion Module menu allows entry of characters other than 0 to 9, * and #. Use of those other characters can cause the twinning number not to work. • The Vantage Connect Expansion Module does not support using this type of button to transfer a current call to the twinning number or retrieve a call from the twinning number. • Path: **Emulation** > **Twinning** • Action Data: None. • Default Label: `Twin`

Table continues…

Action	Description
Voicemail On	This type of button enables the use of voicemail to answer calls which ring unanswered or arrive when the user is busy (has no further call appearances available). • Path: **Advanced** > **Voicemail** > **Voicemail On** • Action Data: None. • Default Label: `VMOn`

Related links

The Vantage Connect Expansion Module Module App on page 174

Part 6: Other Phones

Chapter 31: Other Avaya SIP Phones

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

Related links

1010/1040 Telephones on page 184
1100/1200 Series on page 184
D100 Series (D160) on page 185
H100 Series (H715) on page 185
H200 Series (H229/H239/H249) on page 185

1010/1040 Telephones

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

This series of phones is not supported in IP Office Subscription mode.

Related links

Other Avaya SIP Phones on page 184

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.

This series of phones is not supported in IP Office Subscription mode.

Related links

[Other Avaya SIP Phones](#) on page 184

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.

This series of phones is not supported in IP Office Subscription mode.

Related links

[Other Avaya SIP Phones](#) on page 184

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.

Related links

[Other Avaya SIP Phones](#) on page 184

H200 Series (H229/H239/H249)

The H200 Series are supported with IP Office from R11.0 SP1. The series includes the H229, H239 and H249 SIP telephones. The installation and administration of these phones is covered in the separate *"Installing and Administering the Avaya H239 and H249 Phones*" manual and "*Installing and Administering the Avaya H229 Phone*".

Related links

[Other Avaya SIP Phones](#) on page 184

Chapter 32: Third-Party SIP Phones

Through the Solutions & Interoperability Lab, Avaya issues application notes for non-Avaya product integration with Avaya products. These include application notes for particular models of third-party SIP telephones. You can search and download those application notes the Avaya DevConnect web site (https://www.devconnectprogram.com/).

Beyond basic call handling through the IP Office as listed below, the features available will vary between SIP devices and Avaya cannot make any commitments as to which features will work or how to configure the features.

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

Related links

General Notes on page 186

Third-party SIP phone call capacity on page 187

General Notes

Feature	Description
Multiple Line SIP Devices:	Some SIP devices can support multiple lines or user accounts, each configured separately. If used with an IP Office each SIP line requires a separate IP Office SIP extension, user and license. Note this refers to a SIP device that can handle multiple simultaneous calls itself and not one that is handling multiple calls by holding them on the IP Office/receiving call waiting indication for waiting calls on the IP Office. For the later, the IP Office limits third-party SIP devices to a maximum of 6 concurrent calls.
The IP Office is the SIP Registrar and SIP Proxy:	SIP extension devices are configured with separate SIP registrar and SIP proxy settings. When connecting to an IP Office, the LAN1 or LAN2 IP address on which the SIP registrar is enabled, is used for both settings.

Table continues…

Feature	Description
SIP Codec Selection:	Unlike H.323 IP devices which always support at least one G711 codec, SIP devices do not support a single common audio codec. Therefore, it is important to ensure that any SIP device is configured to match at least one system codec configured on the system.
G.723/G.729b:	These codecs are not available on Linux-based IP Office systems. They are supported on IP500 V2 systems with VCM channels.
Simultaneous Calls:	Third-party SIP extensions are limited by default to 6 simultaneous calls. However this can be changed if required by associating additional third-party endpoint licenses with the extension. See Third-party SIP phone call capacity on page 187.

Related links

Third-Party SIP Phones on page 186

Third-party SIP phone call capacity

By default, third-party SIP phones support up to 6 simultaneous calls. However, using a user source number, you can increase this to 30 calls.

- The user **Source Number** of **ULI=***N* allows a third-party SIP extension to consume multiple third-party endpoint licenses, where *N* is the number of additional licenses from 1 to 4.
- Each additional license enables another 6 calls, up to a maximum of 30 calls total (4 additional licenses).
- For subscription systems, the source number consumes additional user subscriptions.
- Changes to the user **Source Number** require a system restart.

Related links

Third-Party SIP Phones on page 186

Part 7: Miscellaneous

Chapter 33: Sample Settings Files

The following pages show examples of the `46xxsettings.txt` and `46xxspecials.txt` files that the IP Office auto-generates for use by SIP and H.323 extensions.

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

How the phones/clients use the settings:

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

Related links

The 46xxsettings.txt File on page 190
The 46xxspecials.txt File on page 197

The 46xxsettings.txt File

Below is an example auto-generated `46xxsettings.txt` file from an IP Office R11.1.3 system.

- The **AUTOGENERATEDSETTINGS** sections contain settings whose values have been automatically adjusted to match the current IP Office system configuration settings.
- The **NONAUTOGENERATEDSETTINGS** sections contain settings which have fixed values for IP Office operation.
- Note that the settings are also adjusted by the IP Office based on whether the client is local or remote.

If you need to add or change settings it is recommended that you do this using a separate `46xxspecials.txt` file. See The 46xxspecials.txt File on page 197.

- The `46xxspecials.txt` file is supported for the Avaya Workplace Client for IP Office R11.1.2.4 and higher.

Note: This is an example file with settings specific to the system which generated it.

```
## IPOFFICE/11.1.3.1.0 build 28 192.168.0.76 AUTOGENERATED
IF $MODEL4 SEQ 1603 GOTO 16XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 1608 GOTO 16XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 1616 GOTO 16XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9620 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9630 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9640 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9650 GOTO 96XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9608 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9611 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9621 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9641 GOTO 96X1AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J129 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J139 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J169 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J179 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J159 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J189 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K175 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K165 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K155 GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aca GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aci GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acm GOTO SIPXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acw GOTO SIPXAUTOGENERATEDSETTINGS
GOTO NONAUTOGENERATEDSETTINGS
# SIPXAUTOGENERATEDSETTINGS
IF $SIG_IN_USE SEQ H323 GOTO 96X1AUTOGENERATEDSETTINGS
SET RTP_PORT_LOW 46750
SET RTP_PORT_RANGE 4002
SET TLSSRVRID 0
SET ENABLE_OPUS 1
SET ENABLE_G722 1
SET ENABLE_G711A 1
SET ENABLE_G711U 1
SET ENABLE_G729 1
SET ENABLE_G726 0
SET DTMF_PAYLOAD_TYPE 101
SET SIPDOMAIN example.com
SET ENFORCE_SIPS_URI 0
SET DSCPAUD 46
SET DSCPSIG 34
SET HTTPPORT 80
SET TRUSTCERTS WebRootCA.pem
SET COUNTRY UK
SET ISO_SYSTEM_LANGUAGE en_GB
IF $MODEL4 SEQ J129 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J139 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J169 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J179 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J159 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J189 GOTO J1X9AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K175 GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K165 GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K155 GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aca GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aci GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acm GOTO K1EXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acw GOTO K1EXAUTOGENERATEDSETTINGS
# J1X9AUTOGENERATEDSETTINGS
SET RTCPMON 192.168.0.76
SET RTCPMONPORT 5005
IF $MODEL4 SEQ J129 GOTO J129AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J139 GOTO STIMULUSPHONECOMMONSETTINGS
IF $MODEL4 SEQ J169 GOTO STIMULUSPHONECOMMONSETTINGS
IF $MODEL4 SEQ J179 GOTO STIMULUSPHONECOMMONSETTINGS
IF $MODEL4 SEQ J159 GOTO STIMULUSPHONECOMMONSETTINGS
IF $MODEL4 SEQ J189 GOTO STIMULUSPHONECOMMONSETTINGS
GOTO NONAUTOGENERATEDSETTINGS
# J129AUTOGENERATEDSETTINGS
SET USER_STORE_URI "http://192.168.0.76:80/user"
SET MWISRVR "192.168.0.76"
SET SIP_CONTROLLER_LIST 192.168.0.76:5060;transport=tcp
SET CONFERENCE_FACTORY_URI "ConfServer@example.com"
SET FQDN_IP_MAP "sip.example.com=192.168.0.76"
SET AUTH 0
SET ENCRYPT_SRTCP 0
SET GMTOFFSET -6:00
SET SNTPSRVR ""
SET DSTOFFSET 0
SET DAYLIGHT_SAVING_SETTING_MODE 2
SET DSTSTART 1WedSep2L
SET DSTSTOP 2TueFeb2L
SET PHNMOREEMERGNUMS "999,112"
SET PHNEMERGNUM "999"
SET LANGUAGES
Mlf_J129_CastilianSpanish.xml,Mlf_J129_ParisianFrench.xml,Mlf_J129_Dutch.xml,Mlf_J129_Ge
rman.xml
SET MEDIAENCRYPTION 9
GOTO NONAUTOGENERATEDSETTINGS
# STIMULUSPHONECOMMONSETTINGS
SET SIP_CONTROLLER_LIST 192.168.0.76:5060;transport=tcp
SET FQDN_IP_MAP "sip.example.com=192.168.0.76"
SET AUTH 0
SET MEDIA_PRESERVATION 1
SET PRESERVED_CONNECTION_DURATION 120
SET MEDIAENCRYPTION 9
IF $MODEL4 SEQ J139 GOTO J139AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J169 GOTO J169J179AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J179 GOTO J169J179AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J159 GOTO J159AUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J189 GOTO J189AUTOGENERATEDSETTINGS
GOTO NONAUTOGENERATEDSETTINGS
# J139AUTOGENERATEDSETTINGS
SET LANGUAGES
Mlf_J139_CastilianSpanish.xml,Mlf_J139_ParisianFrench.xml,Mlf_J139_Dutch.xml,Mlf_J139_Ge
```

```
rman.xml
GOTO NONAUTOGENERATEDSETTINGS
# J169J179AUTOGENERATEDSETTINGS
SET LANGUAGES
Mlf_J169_J179_CastilianSpanish.xml,Mlf_J169_J179_ParisianFrench.xml,Mlf_J169_J179_Dutch.
xml,Mlf_J169_J179_German.xml
GOTO NONAUTOGENERATEDSETTINGS
# J159AUTOGENERATEDSETTINGS
SET LANGUAGES
Mlf_J159_CastilianSpanish.xml,Mlf_J159_ParisianFrench.xml,Mlf_J159_Dutch.xml,Mlf_J159_Ge
rman.xml
GOTO NONAUTOGENERATEDSETTINGS
# J189AUTOGENERATEDSETTINGS
SET LANGUAGES
Mlf_J189_CastilianSpanish.xml,Mlf_J189_ParisianFrench.xml,Mlf_J189_Dutch.xml,Mlf_J189_Ge
rman.xml
GOTO NONAUTOGENERATEDSETTINGS
# K1EXAUTOGENERATEDSETTINGS
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 1
SET ENABLE_IPO_PORTAL_MESSAGING  1
SET ENABLE_IM 1
SET SIP_CONTROLLER_LIST sip.example.com:5060;transport=tcp
SET CONFERENCE_FACTORY_URI "ConfServer@example.com"
SET PSTN_VM_NUM "VM.user@example.com"
SET SETTINGS_FILE_URL "http://sip.example.com:80/46xxsettings.txt"
SET FQDN_IP_MAP "sip.example.com=192.168.0.76"
SET MEDIAENCRYPTION 9
SET ENCRYPT_SRTCP 0
SET DSCPVID 46
SET TLS_VERSION 1
IF $MODEL4 SEQ acm GOTO EQNXCOMMONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acw GOTO EQNXCOMMONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aci GOTO EQNXCOMMONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aca GOTO EQNXCOMMONAUTOGENERATEDSETTINGS
# EQNXCOMMONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K175 GOTO K1XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K165 GOTO K1XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ K155 GOTO K1XXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acm GOTO EQNXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ acw GOTO EQNXAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ aci GOTO EQNXIOSSPECIFICSETTINGS
GOTO NONAUTOGENERATEDSETTINGS
# K1XXAUTOGENERATEDSETTINGS
SET USER_STORE_URI "http://192.168.0.76:80"
SET SNTPSRVR "192.168.0.76"
SET INTER_DIGIT_TIMEOUT 4
SET NO_DIGITS_TIMEOUT 30
SET ENABLE_PUBLIC_CA_CERTS 1
SET AUDIO_DEVICE_CALL_CONTROL_ENABLED 1
SET BUTTON_MODULE_ENABLE 2
GOTO NONAUTOGENERATEDSETTINGS
# EQNXAUTOGENERATEDSETTINGS
SET APPCAST_ENABLED 1
SET APPCAST_URL "https://storage.googleapis.com/avaya-subscription-eap-update/Vantage/
appcast.xml"
SET APPCAST_CHECK_INTERVAL 1
SET AUDIO_DEVICE_CALL_CONTROL_ENABLED 1
GOTO NONAUTOGENERATEDSETTINGS
# EQNXIOSSPECIFICSETTINGS
SET PUSH_NOTIFICATION_ENABLED 0
GOTO NONAUTOGENERATEDSETTINGS
# 16XXAUTOGENERATEDSETTINGS
SET LANG1FILE "mlf_Sage_v502_spanish.txt"
SET LANG2FILE "mlf_Sage_v502_french_paris.txt"
SET LANG3FILE "mlf_Sage_v502_dutch.txt"
SET LANG4FILE "mlf_Sage_v502_german.txt"
SET BRURI "http://192.168.0.76:80/user/backuprestore/"
SET HTTPPORT "80"
GOTO NONAUTOGENERATEDSETTINGS
# 96XXAUTOGENERATEDSETTINGS
IF $SIG SEQ 2 GOTO NONAUTOGENERATEDSETTINGS
SET SCREENSAVERON 240
SET SCREENSAVER 96xxscr.jpg
SET BRURI "http://192.168.0.76:80/user/backuprestore/"
SET HTTPPORT "80"
GOTO NONAUTOGENERATEDSETTINGS
# 96X1AUTOGENERATEDSETTINGS
SET TRUSTCERTS "Root-CA-020900DC.pem"
SET TLSSRVRVERIFYID 1
IF $SIG SEQ 2 GOTO NONAUTOGENERATEDSETTINGS
SET BRURI "http://192.168.0.76:80/user/backuprestore/"
SET HTTPPORT "80"
SET SCREENSAVERON 240
IF $MODEL4 SEQ 9608 GOTO BRANDINGSCR9608
SET SCREENSAVER 96xxscr.jpg
GOTO BRANDINGSCREND
# BRANDINGSCR9608
SET SCREENSAVER 9608scr.jpg
GOTO BRANDINGSCREND
# BRANDINGSCREND
SET LANG1FILE "mlf_96x1_v224_spanish.txt"
SET LANG2FILE "mlf_96x1_v224_french_paris.txt"
SET LANG3FILE "mlf_96x1_v224_dutch.txt"
SET LANG4FILE "mlf_96x1_v224_german.txt"
IF $MODEL4 SEQ 9608 GOTO NONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ 9611 GOTO NONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J169 GOTO NONAUTOGENERATEDSETTINGS
IF $MODEL4 SEQ J179 GOTO NONAUTOGENERATEDSETTINGS
SET WEATHERAPP ""
SET WORLDCLOCKAPP ""
SET WMLHELPSTAT 0
GOTO NONAUTOGENERATEDSETTINGS
# NONAUTOGENERATEDSETTINGS
SET USBLOGINSTAT 0
SET ENHDIALSTAT 0
# PRODUCT_LINE_SETTINGS
IF $MODEL4 SEQ 1603 GOTO SETTINGS16XX
IF $MODEL4 SEQ 1608 GOTO SETTINGS16XX
IF $MODEL4 SEQ 1616 GOTO SETTINGS16XX
IF $MODEL4 SEQ 9620 GOTO SETTINGS96X0
IF $MODEL4 SEQ 9630 GOTO SETTINGS96X0
IF $MODEL4 SEQ 9640 GOTO SETTINGS96X0
IF $MODEL4 SEQ 9650 GOTO SETTINGS96X0
IF $MODEL4 SEQ 9608 GOTO SETTINGS96X1
IF $MODEL4 SEQ 9611 GOTO SETTINGS96X1
IF $MODEL4 SEQ 9621 GOTO SETTINGS96X1
IF $MODEL4 SEQ 9641 GOTO SETTINGS96X1
IF $MODEL4 SEQ J129 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ J139 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ J169 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ J179 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ J159 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ J189 GOTO SETTINGSJ1X9
IF $MODEL4 SEQ K175 GOTO SETTINGSK1EX
IF $MODEL4 SEQ K165 GOTO SETTINGSK1EX
IF $MODEL4 SEQ K155 GOTO SETTINGSK1EX
IF $MODEL4 SEQ aca GOTO SETTINGSK1EX
IF $MODEL4 SEQ aci GOTO SETTINGSK1EX
IF $MODEL4 SEQ acm GOTO SETTINGSK1EX
IF $MODEL4 SEQ acw GOTO SETTINGSK1EX
```

```
GOTO PER_MODEL_SETTINGS
# SETTINGS96X1
SET UNNAMEDSTAT 0
IF $SIG_IN_USE SEQ H323 GOTO SETTINGS96X1H323
SET TLSSRVRID 0
SET SUBSCRIBE_SECURITY 0
SET ENFORCE_SIPS_URI 0
GOTO PER_MODEL_SETTINGS
# SETTINGS96X1H323
GOTO PER_MODEL_SETTINGS
# SETTINGS96X0
IF $SIG SEQ 2 GOTO SETTINGSSIP96xx
GOTO PER_MODEL_SETTINGS
# SETTINGSSIP96xx
SET TLSSRVRID 0
SET SUBSCRIBE_SECURITY 0
SET ENFORCE_SIPS_URI 0
GOTO PER_MODEL_SETTINGS
# SETTINGS16XX
GOTO PER_MODEL_SETTINGS
# SETTINGSJ1X9
IF $SIG_IN_USE SEQ H323 GOTO PER_MODEL_SETTINGS
SET SIMULTANEOUS_REGISTRATIONS 1
SET ENABLE_AVAYA_ENVIRONMENT 0
SET SIPREGPROXYPOLICY "alternate"
SET DISCOVER_AVAYA_ENVIRONMENT 0
SET FAILBACK_POLICY admin
SET SEND_DTMF_TYPE 2
SET SYMMETRIC_RTP 1
SET SIG_PORT_LOW 1024
SET SIG_PORT_RANGE 64511
SET TCP_KEEP_ALIVE_STATUS 1
SET ENABLE_PRESENCE 0
SET ENABLE_SHOW_EMERG_SK 0
SET ENABLE_SHOW_EMERG_SK_UNREG 0
SET TCP_KEEP_ALIVE_TIME 30
SET ENABLE_OOD_RESET_NOTIFY 1
SET IPV6STAT 0
IF $MODEL4 SEQ J139 GOTO STIMULUSSETTINGS
IF $MODEL4 SEQ J169 GOTO STIMULUSSETTINGS
IF $MODEL4 SEQ J179 GOTO STIMULUSSETTINGS
IF $MODEL4 SEQ J159 GOTO STIMULUSSETTINGS
IF $MODEL4 SEQ J189 GOTO STIMULUSSETTINGS
GOTO PER_MODEL_SETTINGS
# STIMULUSSETTINGS
SET ENABLE_IPOFFICE 2
SET SDPCAPNEG 1
SET CONNECTION_REUSE 1
SET ENCRYPT_SRTCP 0
SET INGRESS_DTMF_VOL_LEVEL -1
GOTO PER_MODEL_SETTINGS
# SETTINGSK1EX
SET SSOENABLED 0
SET EWSSSO 0
SET SIPREGPROXYPOLICY "alternate"
SET IPO_PRESENCE_ENABLED 1
SET IPO_CONTACTS_ENABLED 1
SET DND_SAC_LINK 1
SET POUND_KEY_AS_CALL_TRIGGER 0
SET OBSCURE_PREFERENCES
"ESMENABLED,ESMSRVR,ESMPORT,ESMREFRESH,ESMUSERNAME,ESMPASSWORD,ACSENABLED,ACSSRVR,ACSPOR
T,ACSUSERNAME,ACSPASSWORD,DIRENABLED,DIRSRVR,DIRSRVRPRT,DIRTOPDN,DIRSECURE,DIRUSERNAME,D
IRPASSWORD,SSOENABLED,WINDOWS_IMPROVIDER,AUTO_AWAY_TIME,PSTN_VM_NUM"
SET ENABLE_PPM 0
SET ENABLE_OPUS 1
SET SIMULTANEOUS_REGISTRATIONS 1
SET ENABLE_AVAYA_ENVIRONMENT 0
SET DISCOVER_AVAYA_ENVIRONMENT 0
SET ENABLE_IPOFFICE 1
SET ENABLE_IPO_CALL_LOG 1
SET SUBSCRIBE_LIST_NON_AVAYA "reg,message-summary,avaya-ccs-profile"
SET SDPCAPNEG 1
SET SIPENABLED 1
IF $MODEL4 SEQ K175 GOTO SETTINGSK1XX
IF $MODEL4 SEQ K165 GOTO SETTINGSK1XX
IF $MODEL4 SEQ K155 GOTO SETTINGSK1XX
IF $MODEL4 SEQ aca GOTO SETTINGSEQNX
IF $MODEL4 SEQ aci GOTO SETTINGSEQNX
IF $MODEL4 SEQ acm GOTO SETTINGSEQNX
IF $MODEL4 SEQ acw GOTO SETTINGSEQNX
GOTO PER_MODEL_SETTINGS
# SETTINGSK1XX
SET UPGRADE_POLICY 0
SET REGISTERWAIT 300
SET ENABLE_PHONE_LOCK 0
SET ENABLE_PRESENCE 1
GOTO END
# PER_MODEL_SETTINGS
IF $MODEL4 SEQ 1603 GOTO SETTINGS1603
IF $MODEL4 SEQ 1608 GOTO SETTINGS1608
IF $MODEL4 SEQ 1616 GOTO SETTINGS1616
IF $MODEL4 SEQ 9608 GOTO SETTINGS9608
IF $MODEL4 SEQ 9611 GOTO SETTINGS9611
IF $MODEL4 SEQ 9621 GOTO SETTINGS9621
IF $MODEL4 SEQ 9641 GOTO SETTINGS9641
IF $MODEL4 SEQ J129 GOTO SETTINGSJ129
IF $MODEL4 SEQ J169 GOTO SETTINGSJ169
IF $MODEL4 SEQ J179 GOTO SETTINGSJ179
IF $MODEL4 SEQ J159 GOTO SETTINGSJ159
IF $MODEL4 SEQ J189 GOTO SETTINGSJ189
GOTO END
# SETTINGSEQNX
SET SETTINGS_CHECK_INTERVAL 1
SET ENABLE_BROWSER_EXTENSION 0
SET WINDOWS_IMPROVIDER 0
SET ENABLE_OUTLOOK_ADDON 1
SET OUTLOOK_CALL_CONTACT 1
SET IPO_CONFERENCE_CONTROLS_ENABLED 1
SET CALL_DECLINE_POLICY 2
SET IPO_ADHOC_CONFERENCE_NAME "Conf fa"
SET IPO_OTHER_PHONE_MODE_ENABLED 1
SET IPO_CALL_RECORDING_ENABLED 1
SET IPO_SHARE_CONTROLLED_SOFTPHONE_ENABLED 1
SET AUTO_ANSWER 1
SET IPO_CALL_HANDOVER_ENABLED 1
GOTO END
# SETTINGS1603
GOTO END
# SETTINGS1608
GOTO END
# SETTINGS1616
GOTO END
# SETTINGS9608
GOTO END
# SETTINGS9611
GOTO END
# SETTINGS9621
GOTO END
# SETTINGS9641
GOTO END
```

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

```
GOTO END
# SETTINGSJ169
GOTO END
# SETTINGSJ179
GOTO END
# SETTINGSJ159
GOTO END
# SETTINGSJ189
GOTO END
# END
GET 46xxspecials.txt
```

Related links

Sample Settings Files on page 189

The 46xxspecials.txt File

You can use the `46xxspecials.txt` file to provide SIP and H.323 extensions with settings not included in the auto-generated `46xxsettings.txt`, and to override settings in that file.

- When a `46xxspecials.txt` file is loaded onto an IP Office system, the system automatically adds the `GET 46xxspecials.txt` command to the auto-generated `46xxsettings.txt` file.
- The `46xxspecials.txt` file is supported for the Avaya Workplace Client for IP Office R11.1.2.4 and higher.

Important:

- For extensions operating with IP Office, Avaya only supports settings specifically listed for IP Office use. Using any other settings is not supported.

Sample file

The IP Office can auto-generate a sample `46xxspecials.txt` file. The sample file contains the structure to apply different commands to different phones and clients. To obtain the sample file, browse to `https://<IPOffice>/46xxspecials.txt`. Save and edit that file before uploading it back to the IP Office system.

```
## IPOFFICE/11.1.2.4.0 build 3 192.168.0.76 AUTOGENERATED
IF $MODEL4 SEQ 1603 GOTO 16XXSPECIALS
IF $MODEL4 SEQ 1608 GOTO 16XXSPECIALS
IF $MODEL4 SEQ 1616 GOTO 16XXSPECIALS
IF $MODEL4 SEQ 9620 GOTO 96XXSPECIALS
IF $MODEL4 SEQ 9630 GOTO 96XXSPECIALS
IF $MODEL4 SEQ 9640 GOTO 96XXSPECIALS
IF $MODEL4 SEQ 9650 GOTO 96XXSPECIALS
IF $MODEL4 SEQ 9608 GOTO 96X1SPECIALS
IF $MODEL4 SEQ 9611 GOTO 96X1SPECIALS
IF $MODEL4 SEQ 9621 GOTO 96X1SPECIALS
IF $MODEL4 SEQ 9641 GOTO 96X1SPECIALS
IF $MODEL4 SEQ J129 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J139 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J169 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J179 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J159 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J189 GOTO J1X9SPECIALS
IF $MODEL4 SEQ K165 GOTO K1XXSPECIALS
IF $MODEL4 SEQ K175 GOTO K1XXSPECIALS
IF $MODEL4 SEQ aca GOTO SETTINGSEQNX
IF $MODEL4 SEQ aci GOTO SETTINGSEQNX
IF $MODEL4 SEQ acm GOTO SETTINGSEQNX
IF $MODEL4 SEQ acw GOTO SETTINGSEQNX
GOTO GENERALSPECIALS
# 16XXSPECIALS
GOTO GENERALSPECIALS
# 96XXSPECIALS
GOTO GENERALSPECIALS
# 96X1SPECIALS
GOTO GENERALSPECIALS
# J1X9SPECIALS
IF $SIG_IN_USE SEQ H323 GOTO J1X9H323SPECIALS
GOTO GENERALSPECIALS
# J1X9H323SPECIALS
GOTO GENERALSPECIALS
# K1XXSPECIALS
GOTO GENERALSPECIALS
# SETTINGSEQNX
GOTO GENERALSPECIALS
# GENERALSPECIALS
# GROUP_SETTINGS
IF $GROUP SEQ 1 GOTO GROUP_1
IF $GROUP SEQ 2 GOTO GROUP_2
IF $GROUP SEQ 3 GOTO GROUP_3
IF $GROUP SEQ 4 GOTO GROUP_4
IF $GROUP SEQ 5 GOTO GROUP_5
GOTO END
# GROUP_1
GOTO END
# GROUP_2
GOTO END
# GROUP_3
GOTO END
# GROUP_4
GOTO END
# GROUP_5
GOTO END
# END
```

Related links

Sample Settings Files on page 189

Part 8: Further Help

Chapter 34: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

Additional Manuals and User Guides on page 200
Getting Help on page 200
Finding an Avaya Business Partner on page 201
Additional IP Office resources on page 201
Training on page 202

Additional Manuals and User Guides

The Avaya Documentation Center website contains user guides and manuals for Avaya products including IP Office.

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

For other types of documents and other resources, visit the various Avaya websites (see Additional IP Office resources on page 201).

Related links

Additional Help and Documentation on page 200

Getting Help

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

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See Finding an Avaya Business Partner on page 201.

Related links

Additional Help and Documentation on page 200

Finding an Avaya Business Partner

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

Procedure

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

Related links

Additional Help and Documentation on page 200

Additional IP Office resources

In addition to the documentation website (see Additional Manuals and User Guides on page 200), there are a range of website that provide information about Avaya products and services including IP Office.

- Avaya Website (https://www.avaya.com)

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

- **Avaya Sales & Partner Portal** *(*https://sales.avaya.com*)*

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

- **Avaya IP Office Knowledgebase** *(*https://ipofficekb.avaya.com*)*

  This site provides access to an online, regularly updated version of IP Office user guides and technical manual.

- **Avaya Support** *(*https://support.avaya.com*)*

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

- **Avaya Support Forums** (https://support.avaya.com/forums/index.php)

  This site provides forums for discussing product issues.

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

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

- **Avaya DevConnect** (https://www.devconnectprogram.com/)

  This site provides details on APIs and SDKs for Avaya products, including IP Office. The site also provides application notes for third-party non-Avaya products that interoperate with IP Office using those APIs and SDKs.

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

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

Related links

Additional Help and Documentation on page 200

Training

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

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

Credential maps are available on the Avaya Learning website.

Related links

Additional Help and Documentation on page 200

Index