Installing and Administering the IP Office B179 SIP Conference Phone

September 2013

© 2013 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

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

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

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

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

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

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the

authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, 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 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 Inc.

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: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: B179 SIP conference phone

Description

The B179 SIP conference phone is a simple, sophisticated, conference phone solution that extends crystal-clear sound and smart productivity features to board rooms and large conference rooms alike. The B179 helps improve employee productivity and collaboration between customers, partners and suppliers. Use the instructions in this manual to operate and administer your B179 device with ease.

The Avaya B179 offers a host of innovative features:

- OmniSound® audio technology
- IP telephony for flexible and affordable telephony
- The option to use two accounts simultaneously
- IP Office-based conference support for 128 conferencing channels on the IP500 and IP500 V2 (each conference has a capacity of 3 to 64 parties)
- Support for check-sync message to trigger software upgrades via IP Office
- Support for IP Office centralized personal directory and centralized system directory
- Active call management (dialing new parties, splitting a multi-party call)
- Recorder capability
- Resiliency; the Avaya B179 is a future-proof product that is constantly evolving with smart new features
- (Optional) Extra microphone connection for wider reception
- (Optional) Connection for wireless headset or PA system

Maintenance

Clean the equipment with a soft, dry cloth. Never use liquids. Cleaning your B179 device is that simple. Just try to store the device in a friendly and secure environment, away from potential hazards.

Related topics:

Minimum requirements on page 8
B179 phone detail on page 8
Keypad on page 10

Minimum requirements

Before you proceed, ensure that you have the minimum required components:

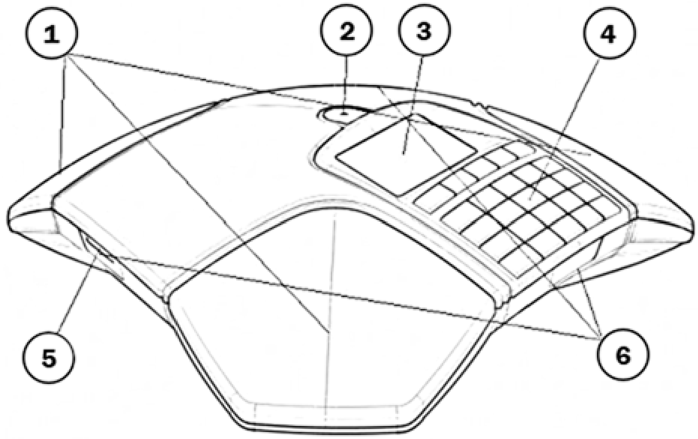
- a working B179 device
- a power cable and AC adapter (for each device you install)
- an Ethernet network cable (for each device you install)
- a memory card (min. 2GB)

Optional components

You might incorporate any of the optional components during or following installation, such as a PA interface box, security lock and cable, or wall-mounting bracket. Expansion microphones are also supported, which can extend the voice pickup range from 320 sq. ft. to up to 750 sq. ft. We advise that you refer to the appropriate documentation when installing these components.

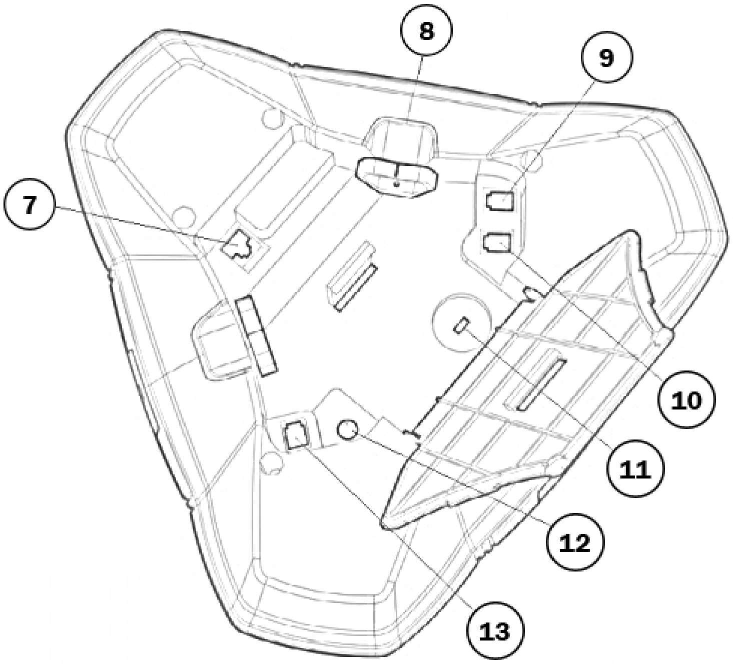
The images that follow illustrate the B179 design and device interface. All the relevant ports, indicators, and feature/dial buttons are identified.

B179 phone detail



Label	Description
1	Three speakers
2	Microphone
3	Display screen

Label	Description
4	Keypad
5	SD memory card port
6	LEDs — **Flashing blue light:** Incoming call — **Steady blue light:** Call in progress — **Flashing red light:** Hold (microphone and speaker turned OFF) — **Steady red light:** Microphone turned OFF



Label	Description
7	Network cable port
8	SD memory card port
9	Expansion microphone port
10	AUX port
11	Security lock port
12	Power supply port
13	Expansion microphone port

Keypad

The buttons located around the perimeter of the button display are explained in the table below. The alphanumeric buttons are identified in the following section.

Note:

You can hold any button for two (2) seconds in order to open the phone book.

Button	Description	Button	Description
REC C	**C button** • No/End/Back/Cancel • Start/Stop recording	▲	**Up arrow** • Navigation in menus • Display of call list
MENU	**Menu button** • Settings menu	▼	**Down arrow** • Navigation in menus • Display of call list
OK	**OK button** • Yes/Confirm choice	☎	**Off-hook button** • Answer/connect new line • During a call: Press to make a new call
☎	**On-hook button** • Hang up/End line	✱	**Conference button** • Automatic dialing of conference groups • Press to call and connect all members of a selected conference group
LINE	**Line button** • Line selection	HOLD	**Hold button** • Hold call
Ø	**Mute button** • Mute call	◢ -	**Volume down button** • Decrease volume level
◢ +	**Volume up button** • Increase volume level		

Entering text

Each alphanumeric button contains letters and characters - more than those shown on the button (see the table below). Press the same button repeatedly to change to another character.

If there are two letters under the same button that you want to enter one after the other, you need to pause momentarily between each letter.

Press **C** to delete the last character you entered.

Button	Options	Button	Options
1 ␣.	(blank) . - 1	2 ABC	A B C Ä Á À Ǻ 2
3 DE	D E F É È 3	4 GHI	G H I 4
5 JKL	J K L 5	6 MN	M N O Ö Ø Ň 6
7 PQRS	P Q R S 7	8 TUV	T U V Ü Ú 8
9 WXY	W X Y Z 9	*	
0	0	#	

Chapter 2: B179 display information

Display screens

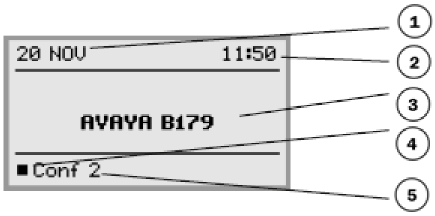
The display screens allow you to view line statuses and menu items. Line statuses will appear on the main screen with different icons to indicate each status. The following sections illustrate the main displays, their icons, and their functions. When you press the **MENU** button, the display screen will change so that you can view the menu options. Refer to the section Navigating the menus on page 16 for more information on the menu options. Note also that the display screen changes depending on whether or not your phone is on the hook.

Related topics:

On hook display on page 13
Off hook display on page 14
Information text on page 14
Line status table on page 15
Line menu on page 15

On hook display

When the phone is on the hook, press the ☎ button to display the following screen:

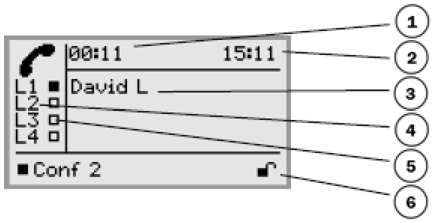


Label	Description
1	Date
2	Time
3	Display text

Label	Description
4	■ Registered □ Not registered
5	Account name

Off hook display

When the phone is off the hook, press the button to display the following screen:



Label	Description
1	Call duration
2	Time
3	information text
4	Phone lines (L1–L4)
5	Line status
6	Secure connection

Information text

The display screen contains important textual elements known as “information text” that relate to one of the following:

- the full number, extension number, or name of the phone line user (the name will be displayed if the user's number is in the phone book)
- an explanation of what to do (for example, **ENTER NUMBER**)
- an explanation of your status (for example, **HOLD** when you place all calls on hold)

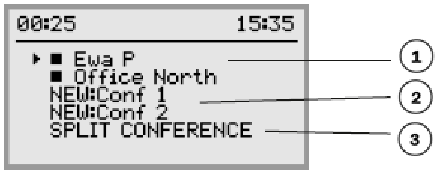
Line status table

As mentioned above, the display screen also indicates line statuses via square-shaped icons. The following table identifies all of the line status icons and what they represent.

Line status icon	Description
□	Line free (before account name – telephone not registered)
■	Line connected (before account name – telephone registered)
■	Line on hold (**HOLD** displayed on the screen – all calls on hold)
✕	Line (called party) busy
◪	Own line put on hold by other party
●	Recording call
🔒	Secure connection

Line menu

When you press the **LINE** button, the following Line menu screen appears:

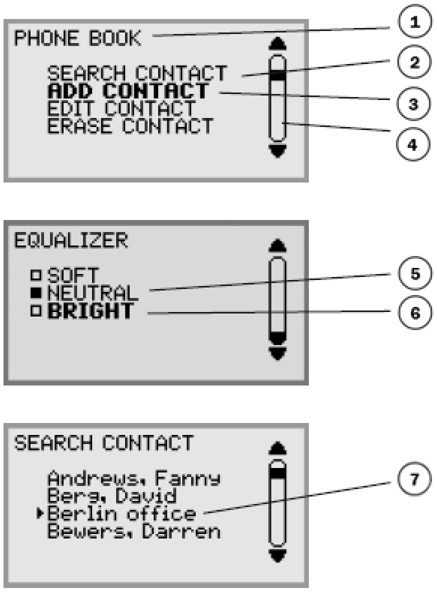


```
00:25          15:35
 ▸ ■ Ewa P
   ■ Office North
   NEW:Conf 1
   NEW:Conf 2
   SPLIT CONFERENCE
```

Label	Description
1	Line/number/name
2	New line (two lines if two accounts are registered)
3	Option for creating or splitting conference calls

Navigating the menus

You can access the menu screen by pressing the **MENU** button. Use the same button to switch to and from a menu. Your options and actions will vary from menu to menu. The images and the table that follow identify the menu types and their various indicators.



Label	Description
1	Current menu
2	Submenu
3	Marked option — select by pressing the OK button
4	Scrolling list — indicates the location of the marked option in the menu list
5	Existing settings
6	Marked option — select by pressing the OK button
7	Marked name — select by pressing the OK button

Navigation and selection in menus

Button	When pressed
MENU button	Open and close the default menu screen.

Button	When pressed
C button	Cancel the setting or return to the previous menu.
OK button	Selects the marked option. This button is also used as a confirmation button; after you have made changes to a setting, you must press **OK** to activate the new setting.
Arrow buttons	Navigate to an option in the menu.
Numerical buttons	Navigate to a corresponding option in the menu (see the menu trees below). For example, press **2** to open **PHONE BOOK** and then press **3** to select **EDIT CONTACT**.

Using the web interface

You can use the web browser of a PC connected to the network to manage the B179 contacts, conference groups, and settings. For security reasons, recordings can only be managed directly on the Avaya B179. All other settings that can be made directly on the Avaya B179 can also be made via the web interface.

It is also possible to import and export contacts and conference groups, name user profiles, and change PIN codes, which can be done via the web interface or through the IP Office configuration file. The administrator can also view logs, update software and create a configuration file.

The default setting for the PIN code is **0000** for the user account (Default, Profile 1, Profile 2, Profile 3 and Profile 4) and **1234** for the administrator's account (Admin). We recommend that you change the PIN codes in order to protect the settings. The code may consist of eight digits. The administrator can always view and change the PIN codes to the user accounts. The administrator's PIN code can only be reset with a complete reset to factory settings. Refer to Reset configuration on page 55 for more information.

Checking the IP address

The following procedure allows you to check the network address that you will use to log into the web server for the conference phone.

Procedure

1. Press **MENU**.
2. Select the sub menu **STATUS** > **NETWORK** (or press **8**, **2** from the main menu).
   The Network screen appears.

3. Check and make note of the conference phone's network address listed under the heading **IP ADDRESS**.

Logging into the web server

Using the information you retained from the previous procedure, you can access the web server to which the conference phone connects. Note that you will require a profile and PIN code in order to access the web server.

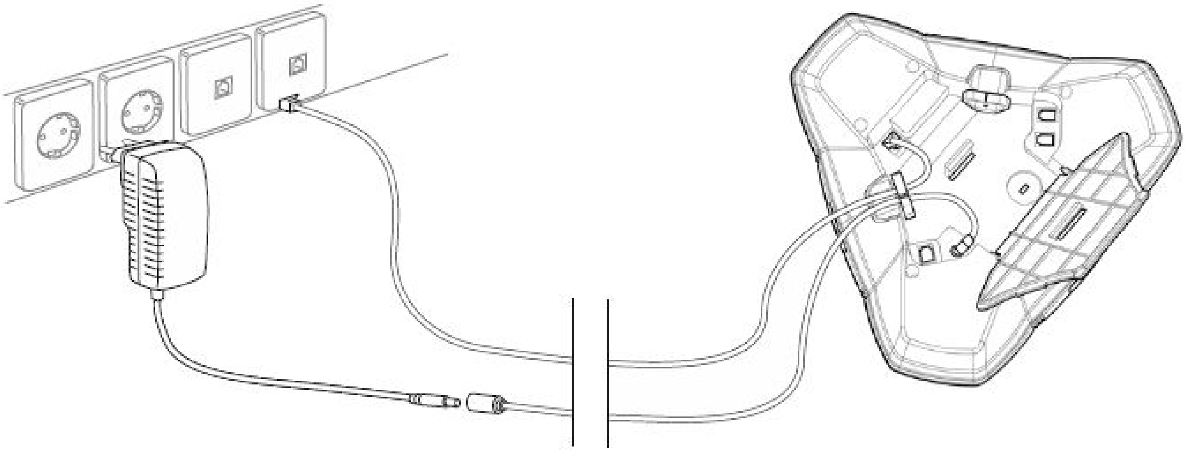
Procedure

1. Type the conference phone IP address into your web browser and press **Enter** in order to access the web server login page. If you are not sure of your conference phone network address, refer to the section Checking the IP address on page 17.
2. On the web server login page, select the appropriate profile, enter the correct PIN code, and click the **Login** button.

Chapter 3: Installing your B179

Connecting the B179

Connect the Avaya B179 to the network as illustrated below. Plug the Avaya B179 into the mains using the power adapter as illustrated.



Once the connections are secure, place the conference phone in the middle of the table.

Note:

The Avaya B179 can be driven directly from the network if the network supports Power over Ethernet (PoE).

Registering the B179

The Avaya B179 must obtain a network address and be registered in a SIP PBX before it can be used. The easiest way to register an account and configure the settings in the Avaya B179 is to use a computer connected to the same network and access the integrated web server. Refer to the following section Obtaining a network address on page 20 for more information.

Obtaining a network address

***To connect to a network using DHCP*:** See the section Checking the IP address on page 17.

***To connect to a network with static IP addresses*:** Use the following procedure.

Before you begin

You will need the IP address, host name, domain, netmask, gateway, DNS 1, and DNS 2. The host name can be set freely. The domain and secondary DNS can be left blank.

Procedure

1. Press **MENU**.
2. Select the sub menu **SETTINGS** > **ADVANCED** (or press **6**, **2** from the main menu).
3. Enter the PIN code. The default is **1234**.
4. Select **NETWORK** (**2**).
5. Select **STATIC IP**.
6. Enter values for the **IP ADDRESS**; enter three digits (begin with 0 if necessary), press **OK**, enter three digits, and so on.
7. Enter the **HOST NAME** (default is 'Avaya'), **DOMAIN**, **NETMASK**, **GATEWAY**, **DNS1**, and **DNS2**.
   When you are finished, the display shows 'DONE.'

Registering an account

The conference phone can be registered in a company SIP PBX or with a public IP telephony service provider. You can store settings for two accounts in the Avaya B179.

To register your phone, you must have access to the account information and all necessary settings that the SIP PBX or service provider requires.

For more information, refer to Account settings on page 39.

Procedure

1. From the web interface, select **Settings** > **SIP**.

2. Click **Yes** at “Enable account” under Account 1.
3. Enter the account information you have received.
   The account name can be chosen freely and is the name or phone number you want to appear on the phone display. Leave the default values if you have no other information.
4. Select a method of NAT traversal if you have received this information.
5. Select a different transport protocol if you have received this information.
6. Save the settings by clicking the **Save** button.
   The Avaya B179 responds by showing “REGISTERING.” If registration is successful, your selected account name will appear at the bottom of the display screen next to a shaded square.

Next steps

Configure your desired media settings. Refer to Media settings on page 45 for more information.

Software upgrades and basic settings

The following settings should be made during installation. Note that all settings on the Basic tab also affect the Default user profile. Other user profiles can be changed individually. The settings on the Basic tab, except the name and PIN for Admin, can be modified by any user. Other settings require a login as Admin.

Note also that these configurations are set in the web interface only.

Related topics:

Upgrading the B179 software on page 21
Setting the time and region on page 22
Setting the language on page 22
Setting the PIN code on page 23

Upgrading the B179 software

Use the following procedure to upgrade the B179 software to the latest version.

Procedure

1. From the web interface, select **Settings** > **Provisioning**.
2. Click the **Check now** button.

3. Compare the latest software version with the current version (shown on the web page).
4. If you want to upgrade, select the desired version in the list box and click the **Upgrade** button.
   The browser window and the display on the Avaya B179 shows that the upgrade has begun.

   > **Note:**
   >
   > The download and installation of the new software can take several minutes. Do not interrupt the upgrade and do not disconnect plugs to the Avaya B179 during the upgrade. Doing so may render the conference phone inoperable.

5. When installation is complete, the text “Upgrade Complete. The unit will be rebooted.” is shown in your browser.
   After a short while, you should hear the Avaya music signature that indicates the reinitiation of the conference phone.

Setting the time and region

Using the procedure below you can set the time and region of the device. You can also set the daylight savings time (DST) and fixed start/stop dates.

Procedure

1. From the web interface, select **Settings** > **Time & Region**.
2. Select the time zone from the drop down menu and, if you wish, select the correction for DST. It is also possible to set the time and date manually or choose a different time server.
3. Select the region where you are. This setting affects the signalling.
4. Click the **Save** button.
   The Avaya B179 reboots with the new settings.

Setting the language

The B179 includes support for various languages. Use the following procedure to configure the language set for the device.

Procedure

1. From the web interface, select **Settings** > **Basic**.
2. Select the desired language using the drop down menu next to “Phone Language” (in the “Preferences” section).
3. When you are satisfied with the setting, click the **Save** button.

Setting the PIN code

We recommend that you change the Admin PIN code from the default configuration to protect the system settings. Make a note of the new PIN code and keep it in a safe place. The administrator’s PIN code can only be reset by a full factory reset!

Procedure

1. From the web interface, select **Settings** > **Basic**.
2. Under the “Profiles” section click the **Edit** button on the Admin line.
3. Enter a new PIN (must consist of eight [8] digits).
4. When you are satisfied, click **Set** and then **Save**.

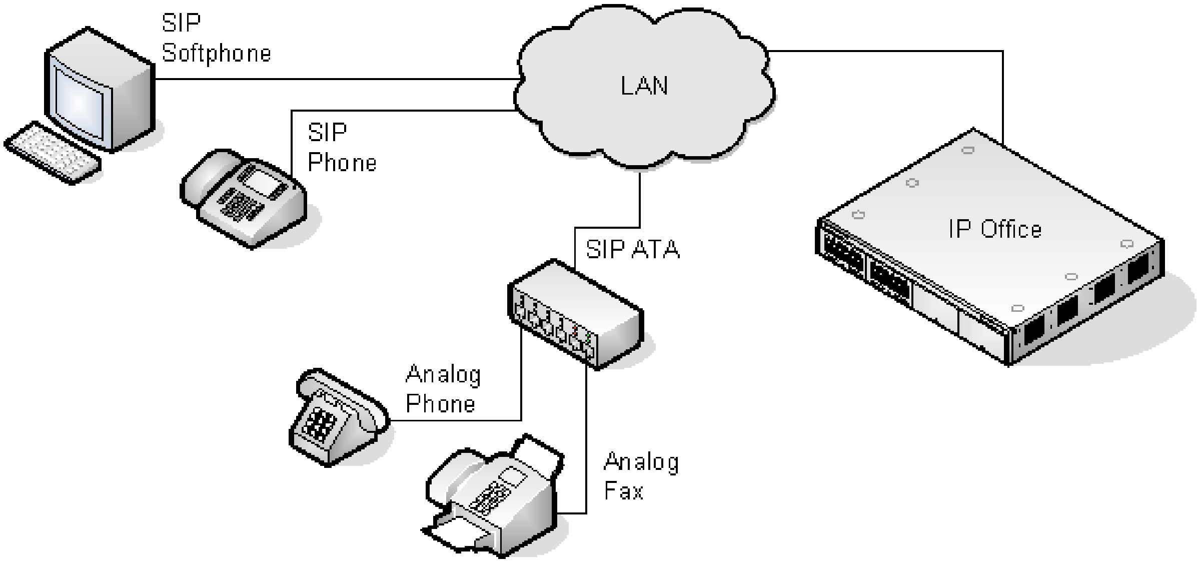
Chapter 4: Configuring your B179 in IP Office

IP Office SIP extensions

SIP stands for Session Initiation Protocol and is a standardized protocol (communication regulations) for connecting phone calls via networks – in most cases via the Internet too. To make and receive calls, the phone has to be registered to a SIP switch. The switch can be a company PBX or can be located with an IP telephony service provider. The SIP switch ensures that the call is connected to the right address within the network or sends the call to the public telephone network if the recipient is not registered as an IP telephone in the same switch.

IP Office 5.0 and higher supports the B179 within the IP Office system. In IP Office, the B179 is licensed using an **Avaya IP Endpoint** license. The number of extensions supported is subject to available licenses and to the normal extension limits of the IP Office control unit being used. This document only covers basic registration with IP Office.

This section of the document provides notes on registering a B179 device with the IP Office system. It assumes that you are familiar with IP Office configuration using IP Office Manager, System Status Application, and System Monitor.



SIP configuration features

- **No NAT**

  Connection of B179 devices from locations where Network Address Translation (NAT) is applied to the connection is not supported. The IP Office does not provide NAT traversal services (for example STUN or TURN) for SIP extension devices.

- **Multiple line SIP devices**

  If used with an IP Office, each SIP line requires a separate IP Office SIP extension, user, and license. Note that 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 or by receiving call waiting indication for waiting calls on the IP Office.

- **IP Office as the SIP registrar and SIP proxy**

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

- **Codec selection**

  Unlike H323 IP devices which always support at least one G711 codec, the B179 does not support a single common audio codec. It is therefore important to ensure that the IP Office SIP extension codecs are configured to match a codec for which the B179 device is configured.

- **IP Office Call Waiting = SIP 'REFER'**

  For the IP Office user associated with a B179 extension, Call Waiting should be enabled. This is required for functions such as transferring a call.

- **Phone features**

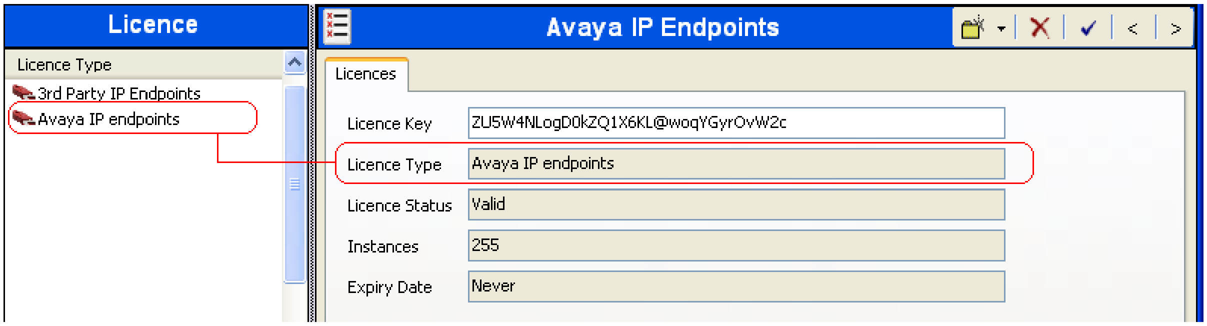
  Beyond basic call handling via the IP Office (see the features listed below), Avaya cannot make any commitments as to which features will or will not work, nor how features are configured on the device.

  - Answer calls
  - Make calls
  - Hang up
  - Hold
  - Supervised transfer
  - Unsupervised transfer
  - Voicemail collect
  - Set forwarding / DND
  - Park / Unpark

B179 licensing information

B179 devices that are handled within the IP Office configuration use **Avaya IP Endpoint** licenses. Successful registration consumes one (1) license count.

There must be sufficient licenses to match the required number of extensions.



Licence

Licence Type

3rd Party IP Endpoints

Avaya IP endpoints

Avaya IP Endpoints

Licences

Licence Key: ZU5W4NLogD0kZQ1X6KL@woqYGyrOvW2c

Licence Type: Avaya IP endpoints

Licence Status: Valid

Instances: 255

Expiry Date: Never

Enabling SIP extension support

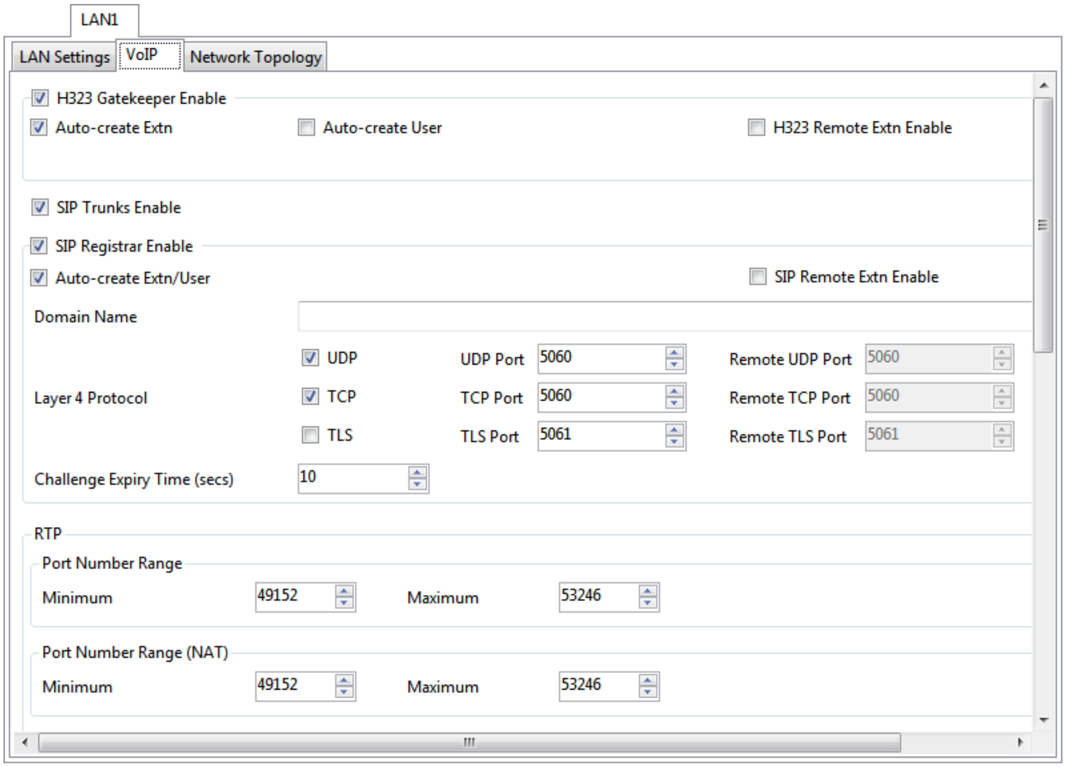
Once the IP Office system has valid Avaya IP Endpoint licenses, it will allow Avaya SIP IP devices, such as the B179, to be connected.

Note:

Changing the SIP registrar settings of an IP Office system requires the IP Office system to be rebooted.

Procedure

1. Using IP Office Manager, retrieve the IP Office system configuration.
2. Select **System**.
3. Select either the **LAN1** or **LAN2** tab as required.
4. Select the **VoIP** sub-tab.



☑ H323 Gatekeeper Enable
☑ Auto-create Extn □ Auto-create User □ H323 Remote Extn Enable

☑ SIP Trunks Enable

☑ SIP Registrar Enable
☑ Auto-create Extn/User □ SIP Remote Extn Enable

Domain Name

Layer 4 Protocol

☑ UDP	UDP Port	5060	Remote UDP Port	5060
☑ TCP	TCP Port	5060	Remote TCP Port	5060
□ TLS	TLS Port	5061	Remote TLS Port	5061

Challenge Expiry Time (secs) 10

RTP

Port Number Range
Minimum 49152 Maximum 53246

Port Number Range (NAT)
Minimum 49152 Maximum 53246

- **SIP Registrar Enable**: Check that **SIP Registrar Enable** is selected.
- **Domain Name**: Default = Blank

  This is the local SIP registrar domain name that will be needed by the B179 in order to register the device with IP Office. If this field is left blank, registration is against the LAN IP address. The examples in this documentation all use registration against the LAN IP address.
- **Layer 4 Protocol**: Default = Both TCP & UDP

  The transport protocol for SIP traffic between IP Office and the B179. Both TCP and/or UDP can be used.
- **TCP Port**: Default = 5060

  The SIP port if using TCP. The default is 5060.
- **UDP Port**: Default = 5060

  The SIP port if using UDP. The default is 5060.
- **Challenge Expiry Time (sec)**: Default = 10

  The challenge expiry time is used during SIP extension registration. When you register the B179, the IP Office SIP Registrar sends a challenge back to the device and then waits for an appropriate response. If the response is not received within this timeout the registration is failed.

- **Auto-create Extn/User**: Default = On

  If this option is selected, the IP Office will automatically create user and SIP extension entries in its configuration based on SIP extension registration. If this method is being used for installation, it is important to check that the settings created match those of the B179. It is also important to deselect this option after installation of the device.

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

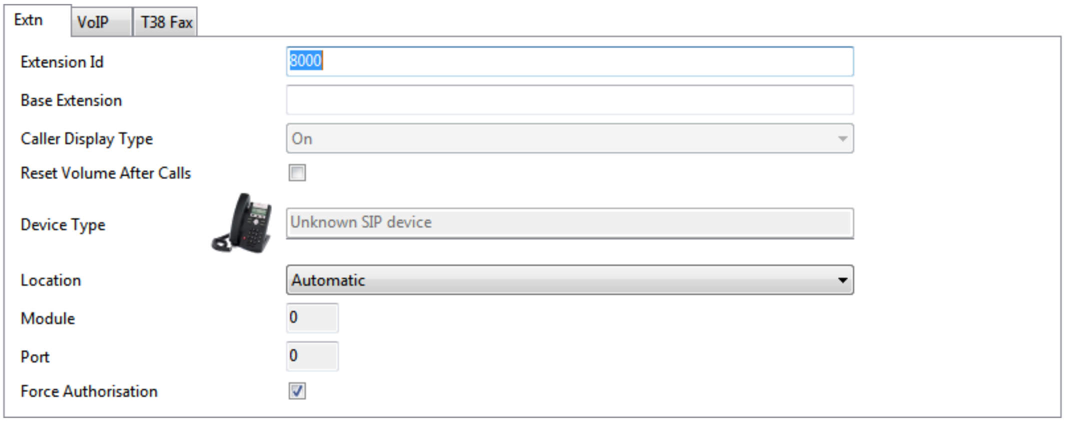
B179 extension settings

Extensions for the B179 can be created manually using | **SIP Extension** or automatically created during registration of the SIP device. Even if auto-created, the extension settings created in IP Office should be checked after installation.

This section looks just at the key configuration settings that affect B179 device extensions. For full details of all the fields shown, refer to the IP Office Manager manual.

Procedure

1. Select **Extensions** and locate the B179 SIP extension. Select the **Extn** tab.



Extension Id	8000
Base Extension	
Caller Display Type	On
Reset Volume After Calls	☐
Device Type	Unknown SIP device
Location	Automatic
Module	0
Port	0
Force Authorisation	☑

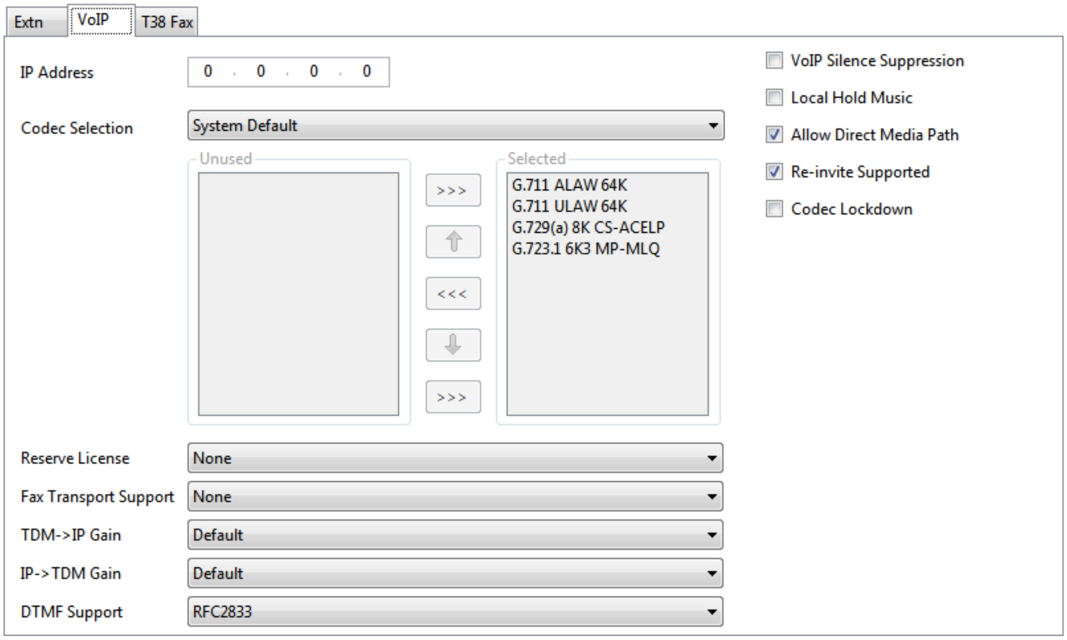
- **Base Extension**

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

- **Force Authorization**: *Default = On*

If enabled, SIP devices are required to register with the IP Office system using the **Name** and **Login Code** configured for the user within the IP Office configuration.

2. Select the **VoIP** tab.



IP Address: 0 . 0 . 0 . 0

Codec Selection: System Default

Selected: G.711 ALAW 64K, G.711 ULAW 64K, G.729(a) 8K CS-ACELP, G.723.1 6K3 MP-MLQ

Reserve License: None

Fax Transport Support: None

TDM->IP Gain: Default

IP->TDM Gain: Default

DTMF Support: RFC2833

□ VoIP Silence Suppression

□ Local Hold Music

☑ Allow Direct Media Path

☑ Re-invite Supported

□ Codec Lockdown

- **Reserve License**

  Each Avaya IP phone requires an Avaya IP Endpoint license. Normally the available licenses are issued in the order that devices register. This option allows an extension to be pre-licensed before the device has been registered. For a B179 device, select **Reserve Avaya IP endpoint licence**.

- **Codec Selection**

  See below.

  - **Codec Lockdown**

    Supports RFC 3264 Section 10.2 when **RE-Invite Supported** is enabled. In response to a SIP offer with a list of codecs supported, some SIP user agents supply a SDP answer that also lists multiple codecs. This means that the user agent may switch to any of those codecs during the session without further negotiation. The system does not support multiple concurrent codecs for a session, so loss of speech path will occur if the codec is changed during the session. If codec lockdown is enabled, when the system receives an SDP answer with more than one codec from the list of offered codecs, it sends an extra re-INVITE using just a single codec from the list and resubmits a new SDP offer with just the single chosen codec.

- **DTMF Support**

  This can be set to one of the two common methods used by SIP devices; ***RFC2833*** or ***Inband***. If the method is not known or varies on a per call basis, deselecting **Allow Direct Media Path** allows a VCM channel to be used for DTMF support when necessary. The selection should be set to match the method used by the B179, otherwise you will be unable to access voicemail in IP Office via the B179 as a result of incompatible signalling tones. Refer to Media settings on page 45 for B179 configuration.

- **Local Hold Music**

  Select this option if you want the B179 to support its own Hold Music source.

- **Re-invite Supported**

  Select this option if you want the B179 to receive REINVITE messages.

Codec selection

The setting you choose for codec selection in IP Office **must match** the codec selection on the B179 itself (as described Media settings on page 45). When the codec settings do not match, calls between certain devices will fail to initiate and you may experience other issues.

The following codecs are supported:

Codec	Explanation
G.722	G.722 is an ITU-T standard codec that provides 7 kHz wideband audio at a data rate within 64 kbit/s. It offers greatly improved speech quality compared with older narrowband codecs such as G.711, but requires a high quality network connection between the devices.
G.723	G.723 is an ITU-T standard codec that provides 300Hz to 3400Hz wideband audio using ADPCM.
G.729	G.729 is an ITU-T standard codec that operates at 8 kbit/s. It is mostly used in VoIP applications with low bandwidth requirements.
G.711 A-law G.711 µ-law	G.711 is an ITU-T standard codec that uses audio companding. Companding algorithms reduce the dynamic range of an audio signal. In analog systems, this can increase the signal-to-noise ratio achieved during transmission and, in the digital domain, can reduce the quantization error. Two main compression algorithms are defined in the standard; the µ-law algorithm (used in North America and Japan) and A-law algorithm (used in Europe and the rest of the world).

If **Codec Selection** is left set to ***System Default***, the extension will use the system codec preferences. In most cases this is preferred and any changes required should be made at the system level to ensure consistency for all IP trunks and extensions.

If required, the **Codec Selection** of each individual trunk and extension can be adjusted to differ from the system defaults, although this is not recommended.

Procedure

1. Using IP Office Manager, retrieve the system's configuration.
2. To display the extension's settings, click ☎ **Extension** in the left-hand panel.
3. Select the **VoIP** tab.
4. Change the **Codec Selection** to ***Custom***.
5. The **Unused** and **Selected** lists can be used to select which codecs the B179 uses and their order of preference.
6. Save the configuration changes back to the system.

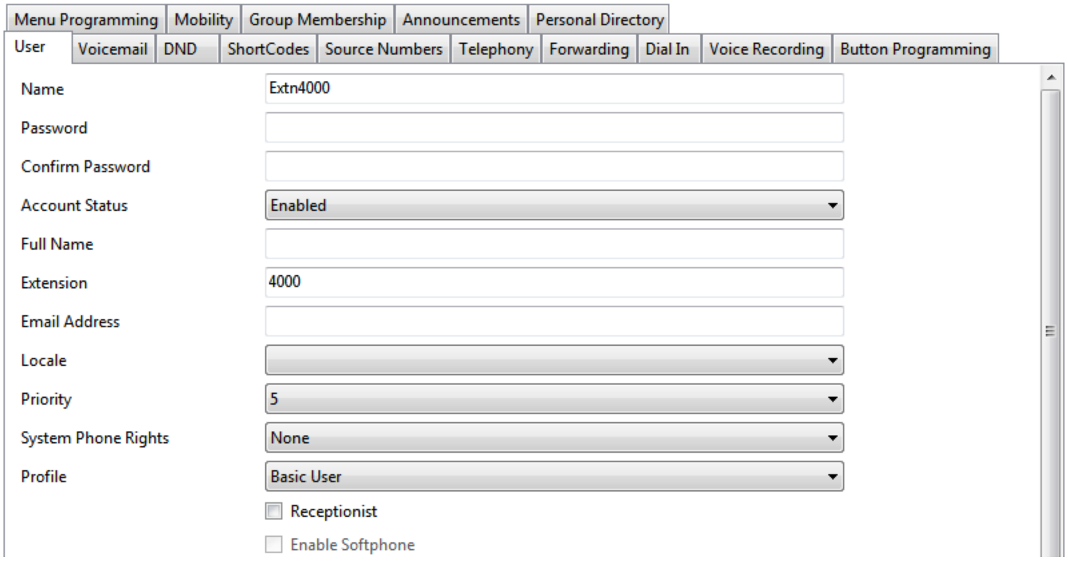
B179 user settings

B179 users can be created manually using 🗀 | **User** or automatically created during device registration. Even if auto-created, the user settings created in the IP Office configuration should be checked during installation.

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

Procedure

1. Select 👤 **User**, locate the B179 extension user, and select the **User** tab.



Name	Extn4000
Password	
Confirm Password	
Account Status	Enabled
Full Name	
Extension	4000
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Basic User

□ Receptionist

□ Enable Softphone

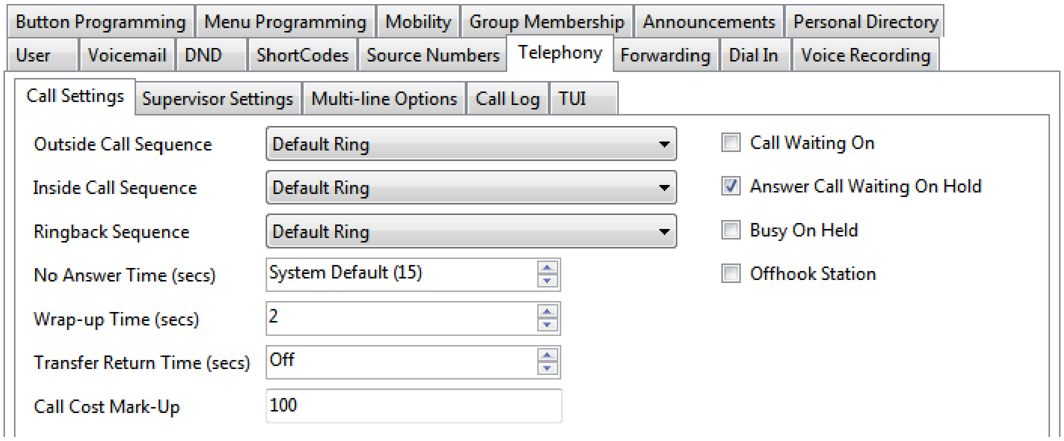
- **Name**

  If the SIP extension is set to **Force Authorization** (the default). This field is used as the ***Authorization Name*** that must be set in the B179 device's configuration.

- **Extension**

  This should match the SIP ID of the B179 device and the Base Extension setting in IP Office.

2. Select the **Telephony** | **Call Settings** tab.



Outside Call Sequence	Default Ring
Inside Call Sequence	Default Ring
Ringback Sequence	Default Ring
No Answer Time (secs)	System Default (15)
Wrap-up Time (secs)	2
Transfer Return Time (secs)	Off
Call Cost Mark-Up	100

□ Call Waiting On

☑ Answer Call Waiting On Hold

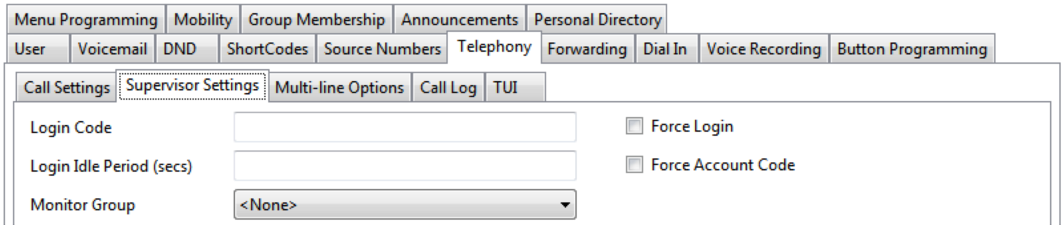
□ Busy On Held

□ Offhook Station

- **Call Waiting On**

  This setting must be enabled in order to allow features such as transferring calls.

3. Select the **Telephony** | **Supervisor Settings** tab.



Login Code

Login Idle Period (secs)

Monitor Group <None>

□ Force Login

□ Force Account Code

- **Login Code**

  If the SIP extension is set to **Force Authorization** (the default), this field is used as the ***Authorization Password*** that must be set in the B179 device's configuration.

Related topics:

[Configuring a Conference Add Shortcode](#) on page 34

Configuring a Conference Add Shortcode

About this task

A Conference add shortcode can be used to place the user, their current call and any calls they have on hold into a conference. When used to start a new conference, the system automatically assigns a conference ID to the call. This is termed ad-hoc (impromptu) conferencing. If the call on hold is an existing conference, the user and any current call are added to that conference. This can be used to add additional calls to an ad-hoc conference or to a meet-me conference.

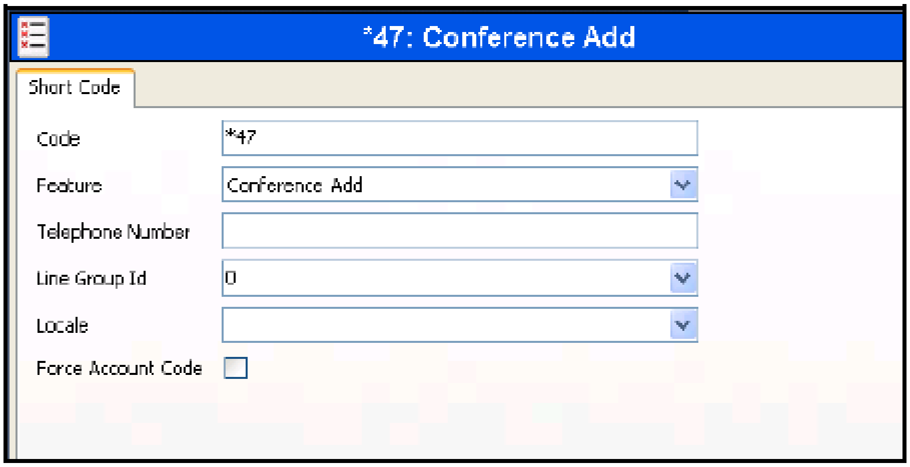
Note:

The Conference Add feature differs from the Conference button on the B179 unit, which is used to call and connect all members of a selected conference group. For information on managing conference groups, see [Managing Contacts and Conference Groups](#)

To configure a Conference Add shortcode, use the following procedure.

Procedure

1. Using IP Office Manager, retrieve the IP Office system configuration.
2. Select the **Short Code** icon.



Code	*47
Feature	Conference Add
Telephone Number	
Line Group Id	0
Locale	
Force Account Code	□

3. Create the short code for the appropriate feature.
4. Send the configuration back to the IP Office.

Allowing Extn/User Auto-creation

The IP Office system can be set to automatically create extension and user entries in its own configuration as each B179 device registers with the system. It can speed up installation to enable this setting when installing several devices and then disable the setting once the installation has been completed.

Note:

Changing the SIP registrar settings of an IP Office system requires the IP Office system to be rebooted.

Procedure

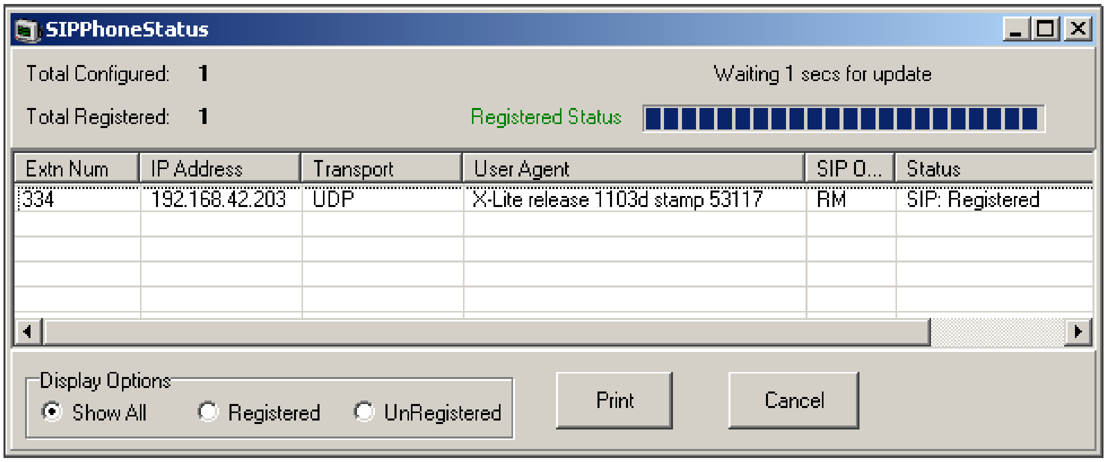
1. Using IP Office Manager, retrieve the IP Office system configuration.
2. Select **System**.
3. Select either the **LAN1** or **LAN2** tab as required.
4. Select the **VoIP** sub-tab.
5. Change the **Auto-create Extn/User** settings to the state required.
6. Send the configuration back to the IP Office.

Checking the B179 extension status

You can view the status of the B179 extensions in the IP Office configuration using the IP Office System Monitor application.

Procedure

Select **Status | SIP Phone Status** to display the SIP extension list.



Total Configured: 1

Total Registered: 1

Waiting 1 secs for update

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

Chapter 5: B179 settings configuration

Basic settings

Almost all settings can be done directly on the Avaya B179. For safety reasons, recordings can *only* be managed directly on the B179. As an administrator, you can also study logs, upgrade the software, and create an XML-based configuration file for easier management of a set of phones.

To configure these settings in the web interface, select **Settings** > **Basic**.

Basic settings include the following:

- Default account
- Language
- Key tone
- Ring level
- Recording/recording tone
- External equipment (Aux)
- Time format
- Equalizer
- Screen text

Default account

This setting determines which account will be used as default.

1. On the phone, press **MENU** > **SETTINGS** > **BASIC** > **ACCOUNT** (or press **6**,**1**,**1** from the main menu).

   Note:

   Press **LINE** before dialing a number to choose the alternative account for the call.

2. Select the desired account and press **OK** to confirm your choice.

Language

1. On the phone, press **MENU** > **SETTINGS** > **BASIC** > **LANGUAGE** (or press **6**,**1**,**2** from the main menu).
2. Select the desired language and press **OK** to confirm your choice.

Key tone

Configure this setting to determine whether or not a tone is heard when you press a button.

1. On the phone, press **MENU** > **SETTINGS** > **BASIC** > **KEY TONE** (or press **6**,**1**,**3** from the main menu).
2. Select the desired volume and press **OK** to confirm your choice.

Ring level

There are six volume levels plus a silent mode. You will hear the ring tone for each level you select. If you select silent mode, only the blue LEDs on the phone flash when an incoming call is received.

1. On the phone, press **MENU** > **SETTINGS** > **BASIC** > **RING LEVEL** (or press **6**,**1**,**4** from the main menu).
2. Select the desired volume and press **OK** to confirm your choice.

Recording

It is possible to turn off the recording feature. This setting can only be done by the administrator, (through the web interface or configuration .xml file during IP Office provisioning) and affects all profiles.

1. From the web interface, select **Settings** > **Basic**.
2. Enable or disable the recording feature by selecting the appropriate radial button next to 'Recording' under the “Preferences” section.
3. When you are satisfied, click on the **Save** button.

Recording tone

When a call is being recorded, all parties are informed every 20 seconds by a short beep. This default feature can be turned off.

1. On the phone, press **MENU** > **RECORDING** > **SETTINGS** (or press **5**,**5** from the main menu).
2. Select the desired volume and press **OK** to confirm your choice.

Settings when connecting external equipment (Aux)

The Avaya B179 can be connected to a wireless headset or an external PA system, although a PA interface box (not included with the Avaya B179) is required for PA system connection. You can configure the settings for the external equipment through the **PA** menu.

⚠ **Warning:**

Do not select the PA option unless a PA system is connected. This option turns off the internal microphone and internal speakers as default. On the contrary, you may select the HEADSET option whether or not a headset is connected.

1. On the phone, press **MENU** > **SETTINGS** > **BASIC** > **PA** (or press **6**,**1**,**7** from the main menu).
2. Activate or deactivate features for your external microphone mixer and PA system as desired.
3. Press **OK** to confirm your choice.

Time format

1. On the phone, press **MENU** > **SETTINGS** > **BASIC** > **TIME FORMAT** (or press **6**,**1**,**8** from the main menu).
2. Select the desired time format (12 or 24 hour) and press **OK** to confirm your choice.

Equalizer

You can adjust sound reproduction to the required or desired pitch (SOFT, NEUTRAL, or BRIGHT).

1. On the phone, press **MENU** > **SETTINGS** > **BASIC** > **EQUALIZER** (or press **6**,**1**,**5** from the main menu).
2. Select Soft, Neutral, or Bright, and press **OK** to confirm your choice.

Screen text

The text on the display screen is shown when the Avaya B179 is in stand-by mode (on hook). You can enter your own text to replace the default text.

1. On the phone, press **MENU** > **SETTINGS** > **BASIC** > **SCREEN TEXT** (or press **6**,**1**,**9** from the main menu).
2. Enter your new text in the text box and press **OK** to confirm your choice.

Account settings

You may wish to register a second account to the extension, especially if the IP Office control unit and the phone are located in separate countries. Otherwise, local calls using the telephone network, connected through the ordinary PBX or SIP server, would be connected as international calls. To configure account settings, you must access the advanced menu, which requires you to enter an administrator's PIN code.

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **ACCOUNTS** (or press **6**,**2**,**1** from the main menu—you will be asked to enter the PIN).
2. Configure the account settings and press **OK** when you are satisfied. Refer to the table below for a brief description of the account setting options.

Account setting	Description
Enable account	It is possible to store account information for future use, but temporarily disable it.
Account name	This is the name displayed on the screen. It can be set according to company standards.
User	The account (customer) name.
Registrar	Shall contain the IP address or the public name of the IP Office unit to which the account is registered (e.g. 10.10.1.100 for a local SIP server)
Proxy	Shall contain the proxy server used for Internet communication, if any.

Account setting	Description
	Can be left blank.
Realm	The protection domain where the SIP authentication (name and password) is valid. This is usually the same as the registrar. If left blank, or marked with a "*", the phone will respond to any realm. If specified, the phone will only respond to the specific realm when asked for credentials.
Authentication name	The name used for the Realm authentication. This may be the same as the user name, but must be filled in.
Password	The password used for the Realm authentication.
Registration interval	This is a request to IP Office for when the registration should expire. Avaya B179 automatically renews the registration within the time interval if the phone is still on and connected to the server. The default value is 1800 seconds.

Network settings

You can configure network settings only if you have proper authorization. You must access the advanced menu, which requires an administrator's PIN code. However, you can also access network settings through the web interface, via **Settings** > **Network**.

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **NETWORK** (or press **6**,**2**,**2** from the main menu—you will be asked to enter the PIN).
2. Configure the network settings and press **OK** when you are satisfied. Refer to the table below for a brief description of the network setting options.

Network setting	Description
DHCP	*Dynamic Host Configuration Protocol* is used by network devices (clients) to obtain the parameters necessary for operation in the IP network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration. DHCP should be set to On if no other information is given. When set to On, all information on this page will be set automatically.
IP address	IP address of the B179. The address is provided by the network administrator or service provider if DHCP is not in use.
Hostname	Set to avaya as default. Can be changed to suitable name.

Network setting	Description
Netmask	Usually set to 255.255.255.0 to limit network traffic to the subnet.
Domain	The domain where the device is located. Can be left blank.
Gateway	The device or server used for Internet communication.
Primary DNS	The address to the primary DNS (Domain Name System) server —a program or computer that maps a human-recognizable name to its computer-recognizable identifier (IP address).
Secondary DNS	The address of an optional secondary DNS server.

NAT traversal settings

NAT (*Network Address Translation*) is a firewall or router function that operates by rewriting the IP addresses in the IP headers as packets pass from one interface to the other. When a packet, for example, is sent from the inside, the source IP address and port are rewritten from the private IP address space into the address space on the outside (Internet).

NAT rewrites the addresses but leaves the packets themselves untouched. This kind of translation works fine for many protocols, but causes a lot of trouble for SIP packets that contain address information in their content (for example an INVITE request from one IP address to another).

NAT traversal solves this problem, providing a “view from the outside” that makes it possible to replace the IP address in the SIP requests with the address shown on the other side of the firewall.

Note that in some cases NAT traversal is not necessary. Some public service providers of IP telephony keep track of the actual IP address used to register a phone, and the one used in the SIP requests from the same phone, and then replaces the addresses in the SIP messages.

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **NAT TRAVERSAL** (or press **6**,**2**,**3** from the main menu—you will be asked to enter the PIN).
2. Configure the NAT traversal settings and press **OK** when you are satisfied. Refer to the table below for a brief description of the setting options.

Setting	Detail
STUN	STUN (*Simple Traversal of UDP through NATs*) is a protocol that assists devices behind a NAT firewall or router with their packet routing. STUN is commonly used in real-time voice, video, messaging, and other interactive IP communication applications. The protocol allows applications operating through a NAT to discover the presence and specific type of NAT and obtain the mapped (public) IP address (NAT address) and port number that the NAT has allocated for the application's UDP (*User Datagram Protocol*) connections to remote hosts. The protocol requires assistance from a 3rd-party network server (STUN server). STUN should be activated if an external SIP server cannot connect to the Avaya B179 behind a firewall NAT function and the SIP server supports STUN. A suitable STUN server is usually provided by the VoIP service provider. **Note:** STUN might also be referred to as *Session Traversal Utilities for NAT*.
STUN host	The IP address or public name of the STUN server.
Offer ICE	ICE (*Interactive Connectivity Establishment*), is a STUN addition that provides various techniques to allow SIP-based VoIP devices to successfully traverse the variety of firewalls that may exist between the devices. The protocol provides a mechanism for both endpoints to identify the most optimal path for the media traffic to follow.
TURN	TURN (*Traversal Using Relay NAT*) TURN is an extension of the STUN protocol that enables NAT traversal when both endpoints are behind symmetric NAT. With TURN, media traffic for the session will have to go to a relay server. Since relaying is expensive, in terms of bandwidth that must be provided by the provider, and additional delay for the media traffic, TURN is normally used as a last resort when endpoints cannot communicate directly.
TURN User	User authentication name on the TURN server.
TURN host	The IP address or public name of the TURN server.
Password	User authentication password on the TURN server.

Transport settings

The transport setting only concerns the protocol to be used for SIP messages between the devices involved. These settings do not include the media (the actual call). The settings on the Media tab should be set accordingly.

Note that if you choose to use a secure connection, both units must support it. Otherwise they cannot negotiate a connection. If an incoming call demands a secure TLS or SIPS connection, the Avaya B179 uses the appropriate protocol even if you have set the phone to use UDP.

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **ACCOUNTS** > **TRANSPORT** (or press **6**,**2**,**1**,**3** from the main menu—you will be asked to enter the PIN).
2. Configure the transport settings and press **OK** when you are satisfied. Refer to the table below for a brief description of the protocols.

   Note:

   Even if Transport is set to TLS or SIPS, the Avaya B179 still accepts incoming UDP or TCP signalling.

Protocol	Detail
UDP	**UDP** (*User Datagram Protocol*) is a protocol on the transport layer in the Internet Protocol Suite. It is a stateless protocol for short messages – datagrams. Stateless implies that it does not establish any connection between sender and receiver in advance. UDP does not guarantee reliability or ordering in the way that TCP does. Datagrams may arrive out of order or go missing without notice. The advantages it offers are speed and efficiency. UDP is the default protocol for SIP.
TCP	**TCP** (*Transmission Control Protocol*) is a protocol on the transport layer in the Internet Protocol Suite. TCP is the standard protocol for Internet communication. TCP keeps track of all individual packets of data, ensuring that they reach the receiver and are put together properly. TCP is not the default protocol for SIP, because it is slower and uses more bandwidth than UDP.
TLS	With UDP and TCP, SIP packets travel in plain text. **TLS** (*Transport Layer Security*) is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks. TLS encrypts the datagrams of the transport layer protocol in use. The secure connection may

Protocol	Detail
	be to the end device or to the first server (usually the SIP server where the phone is registered). There is no guarantee that there is a secure channel to the end point, but because the SIP server is the only part receiving the user authentication, this is still a rather secure solution.
SIPS	**SIPS** (*Secure SIP*) is a security measure that uses TLS to provide an encrypted end-to-end channel for the SIP messages. To use SIPS, however, both VoIP devices and the SIP server must support it.

TLS settings

If you select TLS or SIPS under the transport setting, this additional setting appears on the page.

It may be possible to use secure communication without a certificate and make changes to these settings. In some cases, if you choose TLS or SIPS, the SIP server requires a certificate for user/client verification. This should be specified in the account information.

You can further increase security by requiring verification of the server, or the client when the Avaya B179 acts as a server for incoming calls.

TLS Setting	Detail
Method	The TLS includes a variety of security measures. The methods are defined in the versions of the standard (SSL, SSL v2, SSL v3, TLS v1, TLS v2). The default method is SSLv23, which accepts both SSL v2 and v3.
Negotiation timeout	The TLS settings are negotiated during a call setup (both incoming and outgoing). If this negotiation does not succeed within the specified time (seconds) the negotiation is aborted. Timeout is disabled with 0 (zero).
Verify client	When set to On, the Avaya B179 will activate peer verification for incoming secure SIP connections (TLS or SIPS).
Require client certificate	When set to On, the Avaya B179 rejects incoming secure SIP connections (TLS or SIPS) if the client does not have a valid certificate.
Verify server	When the Avaya B179 is acting as a client (outgoing connections) using secure SIP (TLS or SIPS) it will always receive a certificate from the peer. If Verify server is set to On, the Avaya B179 closes the connection if the server certificate is not valid.

TLS Setting	Detail
Certificate	Here you can upload a certificate to the Avaya B179 to be used for TLS or SIPS communication. A certificate is a file that combines a *public key* with information about the *owner* of the public key, all signed by a trusted third party. If you trust the third party, then you can be sure that the public key belongs to the person/organization named in that file. You can also be sure that everything you decrypt with that public key is encrypted by the person/organization named in the certificate.
Root certificate	The public key in the root certificate is used to verify other certificates. A root certificate is only needed if you have selected client or server verification. A root certificate is signed by the same public key that is in the certificate, a so-called “self-signed” certificate. A typical root certificate is one received from a *Certificate Authority*.
Private key	Here you can upload a private key to the Avaya B179 to be used for TLS or SIPS communication. A private key is one of the keys in a key-pair used in *asymmetric cryptography*. Messages encrypted using the public key can only be decrypted using the private key.
Private key password	The password used for encryption of the private key, if it is encrypted.

Media settings

The media settings determine how audio is sent between the devices. The devices negotiate via SIP before a call is connected. All devices must support the same media types, codecs, and security settings.

Codec

Codecs are used to convert an analog voice signal to a digitally encoded version and vice versa. Codecs vary in the sound quality they deliver and the bandwidth required. The Avaya B179 supports the most common codecs and each codec can be given a precedence depending on your requirements for high quality audio or low bandwidth use. Ensure that you configure IP Office to use the same codec and codec priority. Refer to Codec selection on page 29 for more information.

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **MEDIA** > **CODEC** (or press **6**,**2**,**4**,**1** from the main menu—you will be asked to enter the PIN).
2. Set the codec priority and press **OK** when you are satisfied.

The priority can be set from 4 (high) to 1 (low) or 0 (disabled), and must match that of IP Office.

Security

The media in VoIP calls is usually sent using the RTP protocol (*Real-time Transport Protocol*). RTP is a standardized packet format for delivering audio and video over the Internet.

SRTP (*Secure Real-time Transport Protocol*) is an extension of RTP to provide encryption, message authentication and integrity for the audio and video streams.

All devices must support SRTP to establish a connection. It is therefore possible to set SRTP as disabled, optional or mandatory.

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **MEDIA** > **SECURITY** (or press **6**,**2**,**4**,**4** from the main menu—you will be asked to enter the PIN).
2. Configure SRTP and secure signalling and press **OK**. Refer to the table below for a brief description of each option.

SRTP	If set to disabled, the media is sent using RTP. Note that despite this setting, the Avaya B179 will still use a secure channel if the opposite device demands it. If set to optional or mandatory, a padlock will be shown in the bottom right-hand corner of the screen. If the other devices support SRTP, the padlock will be locked. Otherwise, an open padlock will be displayed. If set to mandatory, the call will not be connected if the other devices do not support SRTP.
Secure signalling	The SIP messages (signalling) and the SRTP cipher key are sent on a different channel than the media and are not affected by the RTP/SRTP setting. To ensure a secure connection, the signalling must be secured using **TLS** or **SIPS**. Note that the SIP transport setting must be set accordingly.

VAD

Voice Activity Detection (speech detection) is a technique used in speech processing to detect the presence or absence of human speech in regions of audio. In VoIP applications, VAD is mainly used to avoid unnecessary coding and transmission of silence packets, saving on computation and network bandwidth.

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **MEDIA** > **VAD** (or press **6**,**2**,**4**,**2** from the main menu—you will be asked to enter the PIN).
2. Configure speech detection and press **OK** when you are satisfied.

DTMF

DTMF (*Dual-tone Multi-Frequency*) signalling is used for telephone signalling over the line to the phone switch or PBX.

If the device itself generates the tones and they are sent in the voice-frequency band, the method is called **Inband**. This is not the best method when using VoIP. Low bit rate codecs may corrupt the signalling tones and make it difficult for the switch to identify them.

RFC 2833 is a method of carrying DTMF signals in RTP packets using a separate RTP payload format. With this method a PSTN gateway reproduces the DTMF tones sent from the end device.

With **SIP Info**, the DTMF signals are sent as SIP requests. The SIP switch creates the tones if the call is transferred to the PSTN.

Use RFC 2833 or SIP Info as preferred methods. Switch to inband only if you encounter problems using DTMF signalling with your PBX/SIP switch.

Ensure that the DTMF configuration on the phone matches the DTMF configuration in IP Office. Otherwise, you will be unable to access voicemail in IP Office via the B179 as a result of incompatible signalling tones. Refer to B179 extension settings on page 29 for IP Office configuration.

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **MEDIA** > **DTMF SIGNALLING** (or press **6**,**2**,**4**,**3** from the main menu—you will be asked to enter the PIN).
2. Configure the desired signalling settings and press **OK** when you are satisfied.

Advanced

First RTP port— If the RTP packets must be directed to a specific port series, the first port number is set here.

LDAP settings

Avaya B179 has support for an external phone book, which means it can communicate with a directory server using LDAP (*Lightweight Directory Access Protocol*). The built in search function dynamically filters the content from the LDAP database, based on the search characters the user enter.

Note:

Once this feature is enabled, the B179 will be able to download the IP Office centralized personal directory and centralized system directory .

To make the LDAP phone book available, the administrator has to activate and configure the LDAP feature.

Procedure

From the web interface, select **Settings** > **LDAP**.
The following table identifies the settings available for configuration:

Setting	Detail
Enable LDAP	The LDAP feature is disabled by default because it has to be configured.
Name filter	Defines how the entered search characters are used. The filter is designed conforming to the string representation of LDAP search filters described in *RFC2254*. The character % in the filter string will be replaced with the search character entered by the user. Example: **(|(sn=%*)(cn=%*))** - All entries with the search characters in the beginning of the **sn** OR **cn** attribute are presented to the user.
Server URL	The IP address of the LDAP server host. Supports *ldap* and *ldaps*.
Search base	The DN (*distinguished name*) of the search base. Example: **dc=domain**, **dc=com**.
Username	Leave this field blank if the LDAP server does not require a username.
Password	Leave this field blank if the LDAP server does not require a password.
Max hits	The maximum number of hits to return for each LDAP search.
Display name	Specifies how the search hits shall be presented on the display in Avaya B179. Example: **%cn** - shows the **cn** attribute. **%givenName %sn** - shows the **givenName** attribute and the **sn** attribute with a space in between.
Sort results	Sorts the search hits based on the Display name.
Number attributes	Here you define the attributes that shall be displayed for a selected search hit. Example: **mobile telephoneNumber** - shows the mobile phone number and office phone number on separate rows for the selected Display name.
Country code	By entering the country code where the phone is located, the country code in any phone number attribute is ignored, if it is identical.
Area code	By entering the area code where the phone is located, the area code in any phone number attribute is ignored, if it is identical.

Setting	Detail
External prefix	If a special prefix is needed to dial external numbers, it should be added here. Use this if you for example need to dial 0 to get a dialing tone.
Min length for external prefix	Restricts the external prefix to be added only if the phone number is longer than the min length. This makes it possible to use short internal numbers.
Exact length for no external prefix	The external prefix in not added if the phone number has exactly the entered length.
Number prefix for no external prefix	All numbers that starts with this number will not have the external prefix added. Useful if you know that all internal numbers start with a certain number.

Web interface settings

The web server in the Avaya B179 supports secure connections using HTTPS.

Procedure

From the web interface, select **Settings** > **Web interface**.
You can also access web interface settings through the B179 via **MENU** > **SETTINGS** > **ADVANCED** > Enter your PIN > **WEB INTERFACE** (or press **6**, **2**, **7** from the main menu).

Option	Detail
Enable HTTPS	Set *Enable HTTPS* to **On** if you need a secure communication between the PC used for setup and the phone.
Certificate	You need to upload a certificate to the phone in order to use HTTPS.

Time settings

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **TIME** (or press **6**,**2**,**5** from the main menu—you will be asked to enter the PIN).
2. Configure the time settings and press **OK** when you are satisfied. Refer to the table below for a brief description of the time setting options.

Time setting	Description
Enable NTP	NTP (*Network Time Protocol*) is a protocol for distributing the *Coordinated Universal Time* (UTC) by means of synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. **Note:** The B179 will set the date and time according to the Date header field in the SIP REGISTER response if no NTP server is configured.
Time	This field shows the actual time if NTP is enabled. Otherwise enter the correct time (hh:mm:ss) and save the setting.
Date	This field shows the actual date if NTP is enabled. Otherwise enter the correct date (yyyy-mm-dd) and save the setting.
Time zone	Select the UTC time zone in your country.
Daylight saving	This setting only adjusts the time by one hour and does not change the time automatically when the DST starts and ends. You can configure the following options: • **Enable DST**: Activate this option if your country uses DST (*Daylight Saving Time* or *Summer Time*). • **DST Timezone**: Select the offset from UTC time when daylight saving is in use. • **DST Mode**: When set to Automatic, the B179 uses dates stored in the phone to adjust for DST. When set to Manual, you need to manually set the offset two times a year. • **Start/Stop Fixed Date**: — Set to **Yes** if DST changes the same date every year in your country. Then select the time and date that it changes. — Set to **No** if DST changes a specific week and day each year (for example, third Sunday in March). Then select the month, week, and time that it changes.
NTP server	The *NTP pool* is a dynamic collection of networked computers that volunteer to provide highly accurate time via NTP to clients worldwide. These computers are part of the pool.ntp.org domain and part of several subdomains divided by geographical zones. They are distributed to NTP clients via round robin DNS.

Region settings

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **REGION** (or press **6**,**2**,**6** from the main menu—you will be asked to enter the PIN).
2. Configure the region settings and press **OK** when you are satisfied.

System settings

You can access system settings via the B179 phone's main menu. You can access the following restart, reboot, and reset options:

Application restart

Restart the phone application using the procedure below.

1. On the phone, press **MENU** > **SYSTEM** > **RESTART** (or press **7**,**1** from the main menu).

The application takes less than 30 seconds to restart.

System reboot

Reboot the entire device using the procedure below.

1. On the phone, press **MENU** > **SYSTEM** > **REBOOT** (or press **7**,**2** from the main menu).

Rebooting the system may take about two minutes.

Factory reset

Use this option to reset the Avaya B179 to factory default settings. All personal settings, including account information, are erased.

1. On the phone, press **MENU** > **SYSTEM** > **FACTORY RESET** (or press **7**,**3** from the main menu).

Hard reset to factory settings

If you have forgotten your Admin PIN code and need to reset the B179 device to factory settings, refer to Hard system recovery on page 55.

Quality of service

Quality of service is used in IP networks to provide different priority to different applications, users, or to guarantee a certain level of performance to a critical data flow such as voice or video. *Differentiated Services* or *DiffServ* is a networking architecture that specifies a simple mechanism for classifying network traffic using a 6-bit field in the header of the IP packets. *VLAN* (*Virtual LAN*) is a technology to logically divide a physical network into several logical nets and thus to differentiate traffic.

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **NETWORK** > **ETHERNET** > **VLAN** (or press **6**,**2**,**2**,**2**,**1** from the main menu—you will be asked to enter the PIN).
2. Configure the DiffServ and VLAN settings and press **OK** when you are satisfied. Refer to the table below for a brief description of the setting options.

Ethernet setting	Description
SIP DiffServ	Enter a value between 0 and 63 to prioritize the SIP messages.
Media DiffServ	Enter a value between 0 and 63 to prioritize the media packets (voice).
VLAN	By enabling this option, all communication to and from the B179 is done via the VLAN specified under VLAN ID.
VLAN ID	The ID number to be used for the IP telephony VLAN.
VLAN map enable	Enabling VLAN priority mapping from the DiffServ setting.
VLAN prio SIP	Set a value between 0 and 7 to prioritize the SIP messages in the VLAN.
VLAN prio media	Set a value between 0 and 7 to prioritize the media packets in the VLAN.

802.1x

IEEE 802.1X is an IEEE Standard for port-based Network Access Control and is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

Procedure

1. On the phone, press **MENU** > **SETTINGS** > **ADVANCED** > enter your PIN > **NETWORK** > **ETHERNET** > **802.1x AUTH** (or press **6**,**2**,**2**,**2**,**2** from the main menu—you will be asked to enter the PIN).
2. Configure the protocol and press **OK** when you are satisfied. Refer to the table below for a brief description of the setting options.

Protocol setting	Description
Enable 802.1x	When you enable this option, the B179 asks an authentication server for permission when connected to the LAN.
EAP method	Select which EAP *(Extensible Authentication Protocol)* method to use: MD5 or TLS.
Username	The device identity in the network.
MD5 password	The password for the device identity when using MD5.
Certificate	Upload a certificate to the Avaya B179 to be used for authentication when using TLS.
Root certificate	The public key in the root certificate is used to verify other certificates when using TLS.
Private key	Upload a private key to the B179 to be used for authentication when using TLS.
TLS password	The password used for encryption of the private key when using TLS.

Chapter 6: Hard system recovery

Reset configuration

If you have forgotten the Admin PIN code, the only way to reset it to default is to do a hard factory reset. This is the same as the factory reset in the system menu (MENU > SYSTEM > FACTORY RESET).

✱ **Note:**

This erases all settings, including account information and contacts!

Procedure

1. Disconnect the power supply cable. Note that this is the same as the network cable if the phone uses Power over Ethernet (PoE).
2. Press and hold the **MENU** button while you connect the cable again (i.e. start the Avaya B179). Hold the button pressed until the SYSTEM RECOVERY menu is shown on the display.
   You can press any other button than **1**, **2**, or **3** to start the phone without resetting.
3. Press **1** to select **Reset Configuration** and confirm your selection by pressing **OK**.
4. When the phone starts, upgrade to the latest version of the software and re-configure account setup and other settings (see Basic settings on page 37 for more information).

Restore firmware

This replaces the current software with the one supplied with the phone.

✱ **Note:**

This erases all settings including account information and contacts!

Procedure

1. Disconnect the power supply cable. Note that this is the same as the network cable if the phone uses Power over Ethernet (PoE).
2. Press and hold the **MENU** button while you connect the cable again (i.e. start the Avaya B179). Hold the button until the SYSTEM RECOVERY menu is shown on the display.

   Note:

   If you are using POE and not the external power supply, you must wait for **Avaya** to appear on the display, then press and hold Menu until the SYSTEM RECOVERY menu appears.

   You can press any other button than **1**, **2**, or **3** to start the phone without restoring the firmware.
3. Press **3** to select **Restore Firmware** and confirm your selection by pressing **OK**. All content in the phone's memory is erased and the firmware supplied with the phone is written to the memory.
4. When the phone starts, upgrade to the latest version of the software and re-configure account setup and other settings (see Basic settings on page 37 for more information).

Chapter 7: Headset and PA installation and settings

Connecting a wireless headset

The microphones from the Avaya B179 and the wireless headset will work simultaneously and transmit the call to other participants in the phone conference. Please refer to your headset manual for further information.

Procedure

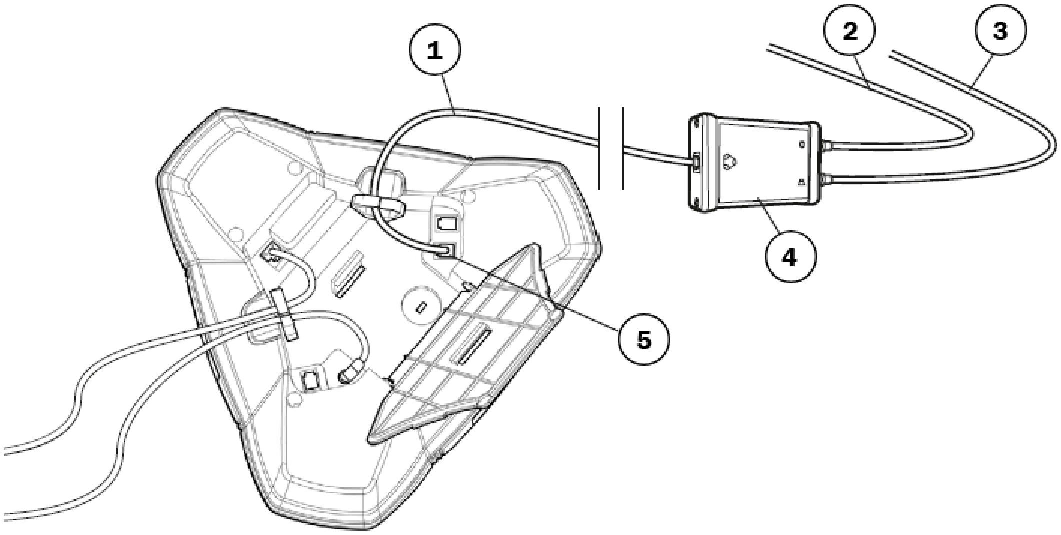
Connect the headset to the AUX port on the Avaya B179 device.

Connecting a PA interface box

The Avaya B179 can be connected to an external PA system using a PA interface box.

Note:

Always disconnect the power supply from the electrical outlet before disconnecting or connecting equipment to the Avaya B179.



1	2.5 meter connection cable
2	To mixer/microphone
3	To amplifier/speakers
4	PA interface box
5	AUX port

Procedure

1. Connect the PA box to the AUX port on the Avaya B179 with the included cable.
2. Connect the external amplifier to the RCA connector marked with a speaker.
3. Connect the microphone mixer to the RCA connector marked with a microphone.

PA settings

To match several types of situations and equipment, access the PA settings available in the Avaya B179 menu.

Related topics:

Activating internal microphone and speakers on page 59
Adjusting microphone volume from PA on page 59
Adjusting PA calibration manually on page 60

Activating internal microphone and speakers

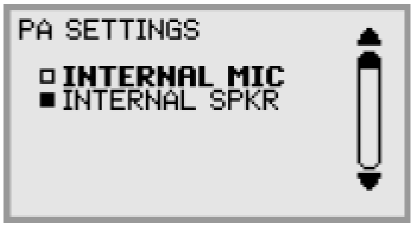
These settings can only be activated on the B179 device.

Note:

To ensure maximum audio quality, do not use the internal microphone and external microphones connected via the PA box at the same time.

Procedure

1. Select **MENU** > **SETTINGS** > **BASIC** > **PA** (or press **6**,**1**,**7** from the main menu).



PA SETTINGS

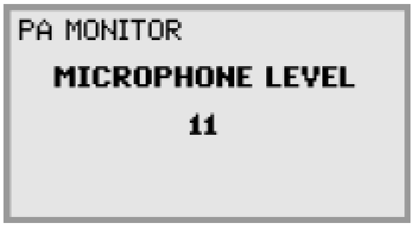
□ **INTERNAL MIC**
■ INTERNAL SPKR

2. Select **INTERNAL MIC** and press **OK** to switch between on (indicated by a shaded box) and off (indicated by an empty box).
   Only the internal microphone is turned off. Any external microphones connected to the B179 remain turned on.
3. Select **INTERNAL SPKR** and press **OK** to switch between on (indicated by a shaded box) and off (indicated by an empty box).

Adjusting microphone volume from PA

Procedure

1. During a call, select **MENU** > **PA** > **PA MONITOR**.



PA MONITOR

MICROPHONE LEVEL

11

2. Adjust the microphone volume from the mixer so that the level on the display screen is around 10–12 when speaking in a normal tone.

Adjusting PA calibration manually

It is possible to calibrate the duplex performance of the conference phone when it is connected to a PA system. The calibration level can be set automatically by the B179 device or adjusted manually to any value between 0 and 5 (0 being full duplex).

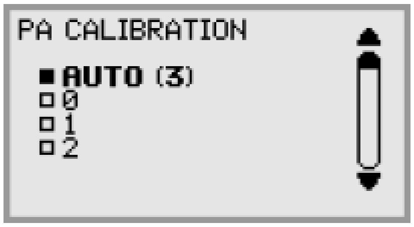
- Increase the calibration if the other party experiences disturbing echo.
- Decrease the calibration if the other party experiences low duplex, i.e. your voice is muted or clipped when the other party is speaking.

Note:

The position of the PA system's microphones and speakers and the amplifier's settings may affect full duplex performance.

Procedure

1. Select **MENU** > **PA** > **CALIBRATION**.



PA CALIBRATION

■ AUTO (3)
□ 0
□ 1
□ 2

AUTO is the default setting and is recommended in most cases. The figure shown in brackets ( ) is the measured calibration value.

2. Select different levels and compare the audio quality to achieve your preferred setting.

Next steps

Call someone and ask them to assess the effect(s) of any adjustment you make.

Chapter 8: Provisioning

Firmware upgrade on a single phone

The easiest way to upgrade the Avaya B179 is via a computer connected to the same network. Via the web interface, you can check for a more recent version and then automatically install it.

It is also possible to download the latest version, via the Avaya website (http://support.avaya.com), and then install the file via the web interface or using a SD card.

Related topics:

Upgrading firmware using the web interface on page 61
Upgrading firmware from a downloaded file on page 62
Firmware binary on page 62
Upgrading firmware from a SD card on page 63
Upgrading Firmware Using IP Office Check-Sync on page 63

Upgrading firmware using the web interface

✱ **Note:**

Download and installation can take several minutes. Do not interrupt the upgrade and do not disconnect plugs to the Avaya B179 during the upgrade. Interrupting the upgrade may render the conference phone inoperable.

Procedure

1. From the web interface, select **Settings** > **Provisioning**.
2. Click on the **Check Now** button.
3. Compare the latest software version with the current version (shown on the same page).
4. If you choose to upgrade, select a version in the list box and click on the **Upgrade** button.
   The browser window and the Avaya B179 display shows that the upgrading has begun.

When installation is complete, the text “`Upgrade Complete. The unit will be rebooted.`” is shown in your browser, and after a while you hear the Avaya music signature, which indicates that the conference phone has started.

> **Note:**
>
> If DHCP is used in the network, the IP address may have been changed. If the web browser loses contact with Avaya B179, check the IP address on the conference phone.

Upgrading firmware from a downloaded file

It is possible to download a firmware file from support.avaya.com and install it on the Avaya B179 from the local hard disk.

Procedure

1. Download the firmware file from support.avaya.com.
2. Click on the **Browse…** button and locate and select the downloaded file.
3. Click on the **Upgrade** button.

> **Note:**
>
> If DHCP is used in the network, the IP address may have been changed. If the web browser loses contact with Avaya B179, check the IP address on the conference phone.

Firmware binary

Procedure

1. Place the firmware binary file on the Provisioning server.
2. Create a Firmware metadata file and place it on the *File server address* specified above.
   Depending on the server used, and the security settings, there might be necessary to add the file type *.kt* to the MIME settings on the server. This is easily checked by trying to download the kt file from a web browser.

Upgrading firmware from a SD card

Upgrading from SD card may be suitable if you have many phones to upgrade. The phones do not have to be connected to the network.

Procedure

1. Download the latest firmware as above and save it on a SD card.
2. Put the SD card in the phone you want to upgrade.
3. Disconnect the power supply cable. Note that this is the same as the network cable if the phone uses Power over Ethernet (PoE).
4. Press and hold the **MENU** button while you connect the cable again (i.e. starts the Avaya B179). Hold the button pressed until the SYSTEM RECOVERY menu is shown on the display.
   You can press any other button than **1**, **2**, or **3** to start the phone without any change.
5. Press **2** to select **SD-card upgrade**.
   The Avaya B179 is upgraded with the firmware file on the SD card and starts when the upgrade is done.

   Note:

   If DHCP is used in the network, the IP address may have been changed. If the web browser loses contact with Avaya B179, check the IP address on the conference phone.

Upgrading Firmware Using IP Office Check-Sync

The B179 SIP phone can initiate a firmware upgrade by acquiring avayab179_fw_version.xml from file manager.

When the firmware version specified in avayab179_fw_version.xml is different from its current firmware, the B179 SIP phone downloads the new firmware from file manager.

The B179 SIP phone starts the firmware upgrade process:

- During boot up
- Upon receiving a check-sync notification message from IP Office
  - Check-sync with no xml body
  - Check-sync with xml body: file_ID=TR_IMG

The structure of the Check- Sync .xml file is as follows:

avayab179.xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<firmware_version>
   <version>2.2.7</version>
   <filename>AVAYA_B179_v2.2.7.kt</filename>
   <checksum></checksum>

</firmware_version>
```

Provisioning from a configuration file

It is possible to save a configuration xml file to be used as:

- Backup (i.e. if the system has been reset to factory default)
- Configuration interface (there are some settings that are not configurable via the web interface)
- Management tool (export, edit and import settings to a set of phones instead of doing the settings on each phone)
- Use with a Device Management server

The structure of the xml file is as follows:

`<locale>`
`    <region>`	

`<recording>`
`    <enabled>`	

`<logging>`	
`    <level>`	The phone application logs messages to log facility LOCAL0. Log level 1–5 (equivalent to Fatal–Trace)
`    <log_sip>`	Log SIP messages to log facility LOCAL1. Default is true.
`    <remote_log>`	Log messages to a remote log server. Default is false.
`    <remote_host />`	Remote log server.

`<network>`
`    <net>`	

`        <dhcp>`	Specify if DHCP should be used to obtain network settings. If so, the other network settings won't be used.

<ip>	Specify the IP address of the Avaya B179.
<netmask>	The netmask of the IP address.
<gateway>	Specify the default gateway to be used.
<dns> <dns>	Specify at most two Domain Name Servers to be used.
<hostname>	Specify host name.
<domain />	Specify domain name.
<vlan>	
<enable>	Virtual LAN enabled if set to true.
<id> <std_prio_map> <sip_priority> <media priority> <ether_8021x> <enable> <username /> <eap_md5> <enable> <password> <eap_tls> <enable> <password> <qos> <dscp_sip> <dscp_media> <time> <ntp> <timezone> <daylight_save> <ntps>	VLAN ID.
<sip>	
<udp_transport>	Specify if UDP shall be used as transport.
<udp_port>	Specify the UDP port to listen to.
<tcp_transport>	Specify if TCP shall be used as transport.
<tcp_port>	Specify the TCP port to listen to.
<tls_transport>	Specify if TLS shall be used as transport.
<sips_transport>	Specify if SIPS shall be used as transport.
<tls_port>	Specify the TLS port to listen to.
<rtp_port>	Specify the start port for RTP traffic.
<outbound_proxy />	Specify the URL of outbound proxies to visit for all outgoing requests. The outbound proxies will be used for all accounts and will be used to build the route set for outgoing requests. The final route set for outgoing

	requests will consist of the outbound proxies and the proxy configured in the account.
`<use_stun>`	Use Simple Traversal of UDP through NATs (STUN) for NAT traversal. Default is No.
`<stun_domain />`	Specify domain name to be resolved with DNS SRV resolution to get the address of the STUN servers. Alternatively, application may specify `stun_host` and `stun_relay_host` instead.
`<stun_host />`	Specify STUN server to be used in ”HOST[:PORT]” format. If port is not specified, default port 3478 will be used.
`<use_turn>`	Use Traversal Using Relay NAT (TURN) for NAT traversal. Default is no.
`<turn_host />`	Specify TURN relay server to be used.
`<turn_tcp>`	Use TCP connection to TURN server. Default is false.
`<turn_user />`	TURN username.
`<turn_passwd />`	TURN password.
`<nat_type_in_sdp>`	Support for adding and parsing NAT type in the SDP to assist troubleshooting. The valid values are: **0**: no information will be added in SDP and parsing is disabled **1**: only the NAT type number is added **2**: add both NAT type number and name
`<require_100rel>`	Specify whether support for reliable provisional response (100rel and PRACK) should be required by default. Note that this setting can be further customized in account configuration.
`<use_srtp>`	Specify default value of secure media transport usage. Note that this setting can be further customized in account configuration. **0**: SRTP will be disabled, and the transport will reject RTP/SAVP offer. **1**: SRTP will be advertised as optional and incoming SRTP offer will be accepted. **2**: The transport will require that RTP/SAVP media shall be used.
`<srtp_secure_signaling>`	Specify whether SRTP requires secure signalling. This option is only used when use_srtp option above is non-zero. Note that this setting can be further customized in account configuration. **0**: SRTP does not require secure signalling **1**: SRTP requires secure transport such as TLS

	2: SRTP requires secure end-to-end transport (SIPS)
<codec>	
<type> <name> <prio> <dtmf>	Codec type. Codec name. Codec priority (0–4) DTMF signalling. Default is 2. **0**: In-band **1**: SIP message **2**: RTP message
<no_vad>	Disable VAD. Default is VAD enabled.
<ec_tail>	Echo canceller tail length, in milliseconds.
<enable_ice>	Enable ICE?
<enable_relay>	Enable ICE relay?
<enable_presence>	Enable the use of presence signalling.
<tls>	
<tls_password />	Password for the private key.
<tls_method>	TLS protocol method from pjsip_ssl_method, which can be: **0**: Default (SSLv23) **1**: TLSv1 **2**: SSLv2 **3**: SSLv3 **23**: SSLv23
<tls_verify_server>	Verify server certificate.
<tls_verify_client>	Verify client certificate.
<tls_require_client_cert>	Require client certificate.
<tls_neg_timeout>	TLS negotiation timeout in seconds to be applied for both outgoing and incoming connections. If zero, no timeout is used.
<account>	
<valid>	If this account information is valid or not.
<name>	User-defined name of the account.
<id>	The full SIP URL for the account.
<registrar>	This is the URL to be put in the request URI for the registration.

<publish_enabled>	If this flag is set, the presence information of this account will be published to the server where the account belongs.
<initial_auth>	If this flag is set, the authentication client framework will send an empty Authorization header in each initial request.
<initial_algo />	Specify the algorithm to use when empty Authorization header is to be sent for each initial request (see above).
<pidf_tuple_id />	Optional PIDF tuple ID for outgoing PUBLISH and NOTIFY. If this value is not specified, a random string will be used.
<force_contact />	Optional URI to be put as Contact for this account. It is recommended that this field is left empty, so that the value will be calculated automatically based on the transport address.
<require_100rel>	Specify whether support for reliable provisional response (100rel and PRACK) should be required for all sessions of this account.
<proxy_uri />	Optional URI of the proxies to be visited for all outgoing requests that are using this account (REGISTER, INVITE, etc).
<reg_timeout>	Optional interval for registration, in seconds. If the value is zero, default interval will be used.
<cred>	Array of credentials. Normally, if registration is required, at least one credential should be specified to successfully authenticate the service provider. More credentials can be specified, for example when it is expected that requests will be challenged by the proxies in the route set.
<realm>	Realm. Use ”*” to make a credential that can be used to authenticate any challenges.
<scheme />	Scheme (e.g. ”digest”).
<username>	Authentication name.
<cred_data_type>	Type of data (0 for plaintext password).
<cred_data>	The data, which can be a plaintext password or a hashed digest.
<auto_update_nat>	This option is useful for keeping the UDP transport address up to date with the NAT public mapped address. When this option is enabled and STUN is configured, the library will keep track of the public IP address from the response of REGISTER request.

	Once it detects that the address has changed, it will unregister current Contact, update the UDP transport address and register a new Contact to the registrar.
`<ka_interval>`	Set the interval for periodic keep-alive transmission for this account. If this value is zero, keep-alive will be disabled for this account. The keep-alive transmission will be sent to the registrar's address after successful registration.
`<ka_data />`	Specify the data to be transmitted as keep-alive packets. Default: CR-LF.
`<use_srtp>`	Specify whether secure media transport should be used for this account. **0**: SRTP will be disabled and the transport will reject RTP/SAVP offer. **1**: SRTP will be advertised as optional and incoming SRTP offer will be accepted. **2**: The transport will require that RTP/SAVP media is used.
`<srtp_secure_signaling>`	Specify whether SRTP requires secure signalling. This option is only used when use_srtp option above is non-zero. **0**: SRTP does not require secure signalling **1**: SRTP requires secure transport such as TLS **2**: SRTP requires secure end-to-end transport (SIPS)
`<account>`	Same as above, but for account 2.

`<provisioning>`
`<upgrade>`	

`<url>`	Place to find software upgrades. The supported URL types are: HTTP, FTP, and TFTP.
`<dev_mgnt>`	
`<enable>`	Device management enabled, true or false.
`<use_dhcp_option>`	Use DHCP option for DM server address.
`<dhcp_option>`	Specification of which DHCP option to use.
`<file_server_address>`	DM server address if not provided by DHCP option.
`<pagename />`	Base name of configuration files to download.
`<type />`	Configuration file type specification.
`<update_interval>`	Timing for downloading files. Shall be entered in crontab format: * * * * * where the * stands for minute (0–59), hour (0–23), day of month (1–30), month (1–12), day of week (0–7) (Sunday =0 or 7)

	Example: 0 6 * * * = the files are downloaded daily at 6:00.
<https_check_srv_cert>	Controls server certificate, true or false.
<https_protocol>	Possibility to set https protocol if open-ssl auto detection fails.
<www>	
<enable_https>	Secure communication to the Avaya B179 web server. Default is false.
<pa>	
<enable_pa>	PA enabled, true or false.
<enable_internal_mic>	Internal mic enabled when PA set to true.
<enable_internal_spkr>	Internal speakers enabled when PA set to true.
<calibration>	Calibration value. Note that 0 is auto, 1 is calibration value 1, 2 is calibration value 1, etc.
<ldap>	
<enable>	LDAP enabled, true or false.
<name_filter>	Name filter according to RFC2254.
<server_url>	LDAP server address.
<search_base>	The DN (distinguished name) of the search base.
<username /> <password /> <max_hits> <country_code> <area_code> <external_prefix /> <min_length_for_ext_prefix /> <exact_length_for_no_ext_prefix /> <number_prefix_for_no_ext_prefix /> <number_attributes> <display_name> <sort_results>	

Related topics:

Exporting configuration on page 71

Importing configuration on page 71

Exporting configuration

Procedure

1. From the web interface, select **Settings** > **Provisioning**.
2. Click on the **Export** button under **Configuration**.
   The configuration file is shown in the web browser.
3. Choose to save the page as an xml file.
   The xml file is as default saved in your folder for downloaded files.
4. If necessary, edit the xml file in a suitable editor.

Importing configuration

Procedure

1. From the web interface, select **Settings** > **Provisioning**.
2. Select the xml file and choose to open it.
3. Click on the **Import** button.

Provisioning from a device management server

Using *Device management* facilitates the upgrading and configuration of multiple conference phones. To use this feature, the Device management needs to be enabled (default) and configured and the appropriate files must be located on a server reachable from all phones, here called a *device management server*.

The configuration and firmware download are controlled with a configurable frequency. The default value is once every 30 minutes.

✱ **Note:**

The interval can only be edited directly in the configuration file.

Configuration priorities

Because the same configuration parameters can be entered in multiple locations, there is a need for priorities. The local configuration files have the highest priority followed by the global configuration file. Configuration entered on the unit itself, via the web interface or directly on the phone, is overridden the next time the configuration files are downloaded.

Note:

The exception to this is any phone language entered on the unit, which will take precedence.

Files on the device management server

Global configuration file

The global configuration file contains the basic configuration – all settings that are common for all conference phones on your location. The easiest way to create this file is simply to configure one phone and export the configuration file or use the built in configuration file creator.

The default name for this file is *avaya.xml*, but it is possible to create a custom name by using the *pagename* element in the configuration file. It is also possible to refer to a cgi, php, asp, js or jsp file, instead of the xml file, if this is declared using the *type* element in the configuration file.

Avaya B179 searches for configuration files in the following order:

"	Type parameter value	Result
1	<nothing>	<pagename>.xml
2	cgi	<pagename>.cgi?phone_model=avaya_b179>
3	%"%	<pagename>.php?phone_model=avaya_b179>
4	asp	<pagename>.asp?phone_model=avaya_b179>
5	E	<pagename>.js?phone_model=avaya_b179>
6	E %	<pagename>.jsp?phone_model=avaya_b179>
:	<any name>	<pagename>.<any name>?phone_model=avaya_b179>
=	auto	1, 2, 3, 4, 5, and 6 will be tried in that order

Local configuration file

The local configuration file contains configuration parameters that are unique for every conference phone. The settings in this file takes precedence over the settings in the global configuration file.

The default name for this file is *avaya-<MAC>.xml*, where <MAC> is the MAC address of the specific conference phone. The MAC address should be written without colons.

It is possible to create a custom name by using the pagename element in the configuration file. It is also possible to refer to a cgi, php, asp, js or jsp file, instead of the xml file, if this is declared using the *type* element in the configuration file.

Avaya B179 searches for configuration files in the following order:

"	Type parameter value	Result
1	<nothing>	<pagename>-<MAC>.xml
2	cgi	<pagename>.cgi? phone_model=avaya_b179&eth=<MAC>
3	%"%	<pagename>.php? phone_model=avaya_b179&eth=<MAC>
4	asp	<pagename>.asp? phone_model=avaya_b179&eth=<MAC>
5	E	<pagename>.js? phone_model=avaya_b179&eth=<MAC>
6	E %	<pagename>.jsp? phone_model=avaya_b179&eth=<MAC>
:	<any name>	<pagename>.<any name>? phone_model=avaya_b179&eth=<MAC>
=	auto	1, 2, 3, 4, 5, and 6 will be tried in that order

Firmware binary

Contains the firmware binary that will be downloaded and installed by Avaya B179 if the metadata file shows that this is a newer version than the present installed. The binary file can be downloaded from support.avaya.com.

Firmware metadata file

A metadata file in xml format with information of the firmware version in the binary file. The file is used to check if the binary file should be downloaded to the phone or not.

The name of this file shall be *avaya_fw_version.xml*. The file shall contain the following elements in xml format:

`<firmware_version>`	
`<version>X.X.X</version>`	Eg. 2.0.7
`<filename>xxxx</filename>`	Eg. AVAYA_B179_v2.0.7.kt
`<checksum>XXXX</checksum>`	MD5 checksum of the firmware binary
`</firmware_version>`	

Related topics:

Configuring device management on page 74
Setting up a device management server on page 75

Configuring device management

As mentioned previously, you can configure device management options in the web interface only.

Procedure

1. From the web interface, select **Settings** > **Provisioning**.
2. Configure the options using the information below:

Device management option	Detail
Enable	**On** enables Device management.
Use DHCP option	Set to on if you want to use DHCP option for DM server address.
DHCP option	Select the DHCP option used for the DM server address: 43: Vendor specific 56: DHCP message 60: Class Id 61: Client Id 66: Server-name 67: Bootfile-name 242: Site-specific
File server address	DM server address if not provided by DHCP option.
HTTPS protocol	Default is auto, but can be set to SSLv2 or SSLv3 if open-ssl auto detection fails.
Check server cert.	Enable authentication with certificate.
Certificate	Here you can upload a certificate to the Avaya B179 to be used for authentication when using Device management.
Root certificate	The public key in the root certificate is used to verify other certificates when using Device management.
Private key	Here you can upload a private key to the Avaya B179 to be used for authentication when using Device management.

Setting up a device management server

This is a description of a manual method to create the configuration files.

Procedure

1. From the web interface, select **Settings** > **Provisioning**.
2. Enable device management and enter the server information.

Related topics:
Firmware binary on page 62
Creating a global configuration file on page 75
Creating a local configuration file on page 75

Creating a global configuration file

Procedure

1. Configure a phone with the basic configuration.
2. Click on **Export** to create a configuration file.
3. If necessary, edit the xml file in a suitable editor.

   ✱ **Note:**

   Some parameters can’t be entered via the web interface (update frequency, pagename, and filetype).

   To avoid confusion, it may be wise to delete the local information from the file (eg. account information).
4. Save the file with the name **avaya.xml** on the *File server address* specified above.

Creating a local configuration file

Procedure

1. Save a copy of the configuration file for each conference phone on your location with content only in the elements that shall be unique for each conference phone (eg. account information).
   The default name for each file is *avaya-<MAC>.xml* where <MAC> is the MAC address of the specific conference phone.
2. Place the configuration files on the *File server address* specified above.

Firmware binary

Procedure

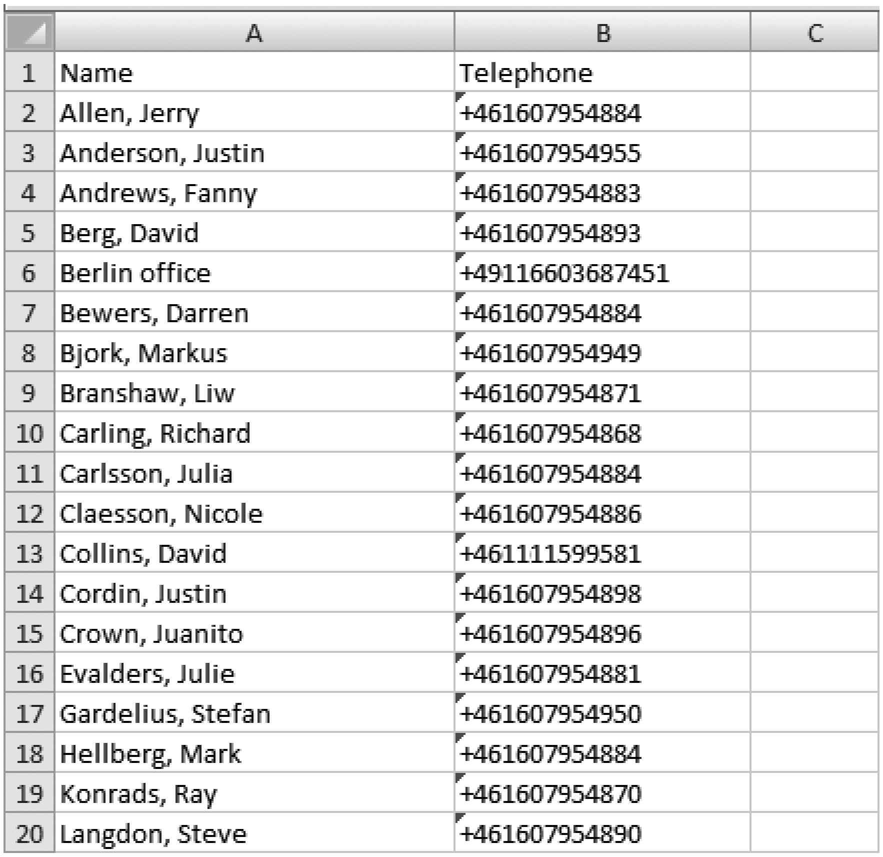
1. Place the firmware binary file on the Provisioning server.
2. Create a Firmware metadata file and place it on the *File server address* specified above.
   Depending on the server used, and the security settings, there might be necessary to add the file type *.kt* to the MIME settings on the server. This is easily checked by trying to download the kt file from a web browser.

Chapter 9: Managing contacts and conference groups

Importing and exporting contacts

You can import contacts from a comma separated values (.csv) file. One way of creating a .csv file is using Microsoft Excel and saving the file in .csv format.

Enter the names of the contacts in the first column and their phone numbers or URIs in the second. Do not use hyphens or spaces in the number. Note that Excel ignores zeros at the beginning of numbers. The cells must therefore be formatted as text.



	A	B	C
1	Name	Telephone	
2	Allen, Jerry	+461607954884	
3	Anderson, Justin	+461607954955	
4	Andrews, Fanny	+461607954883	
5	Berg, David	+461607954893	
6	Berlin office	+49116603687451	
7	Bewers, Darren	+461607954884	
8	Bjork, Markus	+461607954949	
9	Branshaw, Liw	+461607954871	
10	Carling, Richard	+461607954868	
11	Carlsson, Julia	+461607954884	
12	Claesson, Nicole	+461607954886	
13	Collins, David	+461111599581	
14	Cordin, Justin	+461607954898	
15	Crown, Juanito	+461607954896	
16	Evalders, Julie	+461607954881	
17	Gardelius, Stefan	+461607954950	
18	Hellberg, Mark	+461607954884	
19	Konrads, Ray	+461607954870	
20	Langdon, Steve	+461607954890	

Note:

It is normally possible to export contact books stored in your PC in CSV format.

The way the number can be written may depend on the SIP PBX being used, but normally you can use:

- Complete phone number, including country code
- Phone number, including area code
- Local phone number only
- Internal speed dial number (with company’s own PBX)
- URI, e.g. **sip:user@company.com**
- URI with IP address, e.g. **sip:10.10.1.100** (within a local network)

Importing contacts

Procedure

1. From the web interface, select **Phone Book**.
2. Click on the **Scroll…** button under the heading 'Import' in the web window.
3. Open your .csv file.
4. Click on **Import**.
   The name is limited to 15 characters, since the Avaya B179 screen cannot display more than 15 characters.

Exporting contacts

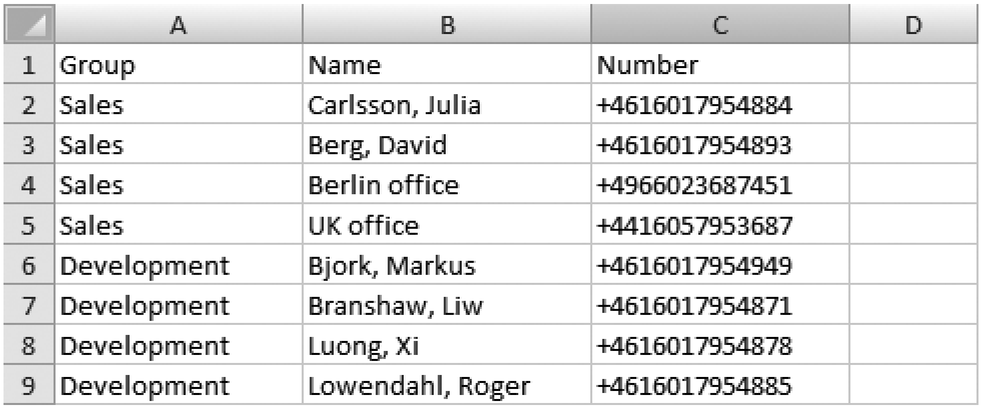
You can export your contacts as a .csv document in order to import them into another phone.

Procedure

1. Click on **Export**.
2. Save the document.

Importing and exporting conference groups

The conference groups can be imported and exported in the same way as the contacts in the phone book, but you must use a three-column csv instead of a two-column csv.



	A	B	C	D
1	Group	Name	Number	
2	Sales	Carlsson, Julia	+4616017954884	
3	Sales	Berg, David	+4616017954893	
4	Sales	Berlin office	+4966023687451	
5	Sales	UK office	+4416057953687	
6	Development	Bjork, Markus	+4616017954949	
7	Development	Branshaw, Liw	+4616017954871	
8	Development	Luong, Xi	+4616017954878	
9	Development	Lowendahl, Roger	+4616017954885	

Chapter 10: Checking status and logs

Checking device status

The Device menu lists phone information such as serial number, network port, and current software version.

Procedure

On the phone, press **MENU** > **STATUS** > **DEVICE** (or press **8**,**6** from the main menu).
You will be able to view the status of the following:

- Avaya B179 (software version and date)
- Serial number
- MAC address

Checking media status

You can check the status of the media settings, such as codec priority and media security, using the procedure below.

Procedure

On the phone, press **MENU** > **STATUS** > **MEDIA** (or press **8**,**4** from the main menu).
You will be able to view the status of the following:

- Codec priority
- VLAD
- DTMF signalling
- Security RTP
- Secure signalling

Checking network status

You can view your network information via the Network menu. You will find information including the IP address, the gateway, the quality of service, and more.

Procedure

On the phone, press **MENU** > **STATUS** > **NETWORK** (or press **8**,**2** from the main menu).
You will be able to view the status of the following:

- DHCP
- IP address
- Hostname
- Domain
- Network
- Gateway
- DNS 1
- DNS 2
- VLAN

Checking SIP status

You can check the status of the SIP settings in the web interface using the procedure below.

Procedure

From the web interface, select **STATUS** > **SIP**.

✳ **Note:**

From this screen you will also be able to view NAT traversal and transport settings, as well as the status of the active account(s).

Checking account status

You can check the status of either account registered to the device using the procedure below.

Procedure

On the phone, press **MENU** > **STATUS** > **ACCOUNTS** and select the desired account (alternatively, press either **8**,**1**,**1** from the main menu to view the status of Account 1 or press **8**,**1**,**2** from the main menu to view the status of Account 2).
You will be able to view the status of the following:

- Account name
- Registrar
- SIP ID
- Auth. name
- Realm
- Proxy

Checking NAT traversal status

It may be necessary to check the status of the NAT traversal if the phone is behind a firewall. You can check whether address conversion is activated using the following procedure.

Procedure

On the phone, press **MENU** > **STATUS** > **NAT TRAVERSAL** (alternatively, press **8**,**3** from the main menu).
You will be able to view the status of the following:

- STUN
- TURN
- ICE

Checking transport status

You can check the status of the transport setting using the following procedure.

Procedure

On the phone, press **MENU** > **STATUS** > **ACCOUNTS** > **TRANSPORT** (alternatively, press **8**,**1**,**3** from the main menu).

Checking time and region status

You can check the status of the time and region settings using the procedure below.

Procedure

On the phone, press **MENU** > **STATUS** > **TIME** (or press **8**,**5** from the main menu).
You will be able to view the status of the following:

- NTP
- NTP server
- Timezone

Obtaining logs

You can view and obtain logs using the web interface. There are five types of log messages that can be useful when troubleshooting. Read below the procedure for more information on the types of logs available.

Procedure

1. From the web interface, select **Status** > **Log**.
2. Select the log you want to review and click the **Change** button.

   Note:

   Clicking the **Refresh** button will add all the new messages sent since the present log was chosen.

Application log

This shows the phone application messages. The log can be filtered from “Fatal” (only the fatal error messages) to “Trace” (all messages).

The **Clear log** button erases all content in the log.

SIP Trace

The SIP Trace logs the communication between the phone and the SIP PBX.

The **Clear log** button erases all content in the log.

It is possible to disable the SIP trace log:

1. Select SIP logging **Off** and click on the **Set** button.

System log

Shows the phone system messages.

Device management log

Logs the device management activities.

Upgrade log

Logs the upgrade procedure.

Chapter 11: Technical data

DEVICE	
Size	Diameter 240 mm, height 77 mm
Weight	1kg
Colour	Liquorice black
Display screen	Illuminated graphics (LCD), 128x64
Keypad	Alphanumerical 0–9, *, on, off, mute, hold, volume up, volume down, 5 buttons for menu navigation, line mode, conference guide
Anti-theft protection	Kensington security slot
Memory	Support for SD memory cards up to 2 GB

CONNECTIVITY	
Network connection	Modular 8P8C (RJ45), Ethernet 10/100 Base T
Power supply	AC adapter 100–240 V AC/13.5 V DC IEEE 802.3af Power over Ethernet
Extra microphones	Two (2) modular 4P4C
Auxiliary	Modular 4P4C for wireless headset

NETWORK & COMMUNICATION	
Network addressing	DHCP and static IP
NAT traversal	STUN, ICE, and TURN
Connection protocol	SIP 2.0 (RFC 3261 and companion RFCs)
Transport	UDP, TCP, TLS and SIPS
Security	SRTP and TLS
Quality of service	DiffServ, VLAN and 802.1x

NETWORK & COMMUNICATION	
Audio support	Codecs: G.722, G.711 A-law, G.711 µ-law, G.729ab
DTMF tone generation	RFC, SIP INFO, In-band
Time servers	NTP and SNTP — Daylight saving: Configurable for automatic adjustments

DIRECTORY	
Internal phone book	1,000 entries per profile (4 password protected profiles) Export/import of directory Call list
External directory	Support for LDAP

SOUND	
Technology	OmniSound® 2.0 Wideband
Microphone	Omni-directional
Reception area	Up to 30 metres2, >10 people
Speaker	Frequency band 200–7000 Hz,
Volume	90 dB SPL 0.5 m
Equalizer	Three pitches: soft, neutral, bright

ENVIRONMENT	
Temperature	5°–40°C
Relative humidity	20-80% condensation free
Recommended acoustic conditions	Reverberation period: 0.5 S Rt 60 Background noise: 45 dBA

APPROVALS	
Electrical safety	EN 60950-1:2006, ANSI/UL 60950-1-2002, CAN/CSA-C22.2, No. 60950-1-03
EMC/Radio	EN 301 489-3 V1.4.1 (2002-08), EN 301 489-1 V1.6.1 (2005-09), FCC Part 15 subpart B class A, FCC Part 15 subpart C, EN 300220-1:2000, EN 300220-2:2000, RoHS

Index