SIP Software for Avaya 1100 Series IP Deskphones-Administration

Release 4.4
NN43170-600
Issue 06.06 Standard
December 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

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

License types

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions

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

Copyright

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya 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.

Contents

Chapter 1: New in this release

SIP Software for Avaya 1100 Series IP Deskphones- Administration , NN43170-600 supports SIP Software Release 4.4. This document contains administration information for the Avaya 1120E IP Deskphone, Avaya 1140E IP Deskphone, and Avaya 1165E IP Deskphone with SIP Software Release 4.4.

Supported platforms

SIP 4.4 supports the following platforms:

- Communication Server 1000 7.6
- B5800 Branch Gateway 6.2
- IP Office Release 8.1
- Avaya Aura® Communication Manager 6.2 FP2
- Avaya Aura® Messaging 6.2
- Avaya Aura® Presence Services 6.2
- Avaya Aura® Conferencing 7.0

Avaya Aura® support for 1100 Series IP Deskphones

The Avaya Aura® communications platform (solution comprised of Avaya Aura™ Communication Manager, Avaya Aura™ Session Manager, Avaya Modular Messaging) now supports the 1100 Series IP Deskphone with SIP 4.4 software. The 1100 Series IP Deskphones are directly registered to Session Manager and are supported by Communication Manager configured as an Evolution Server (CM-ES).

Supported platforms

The following Avaya Aura® platforms are supported:

- Avaya Aura® Communication Manager 6.2 FP2
- Avaya Aura® Session Manager 6.2 FP2
- Avaya Aura® Messaging 6.2

- Avaya Aura® Presence Services 6.1
- Avaya Aura® Conferencing 7.0

Telephony features

Some Communication Manager (CM) features can be invoked by dialing a Communication Manager Feature Name Extension (FNE). FNEs must be defined in Communication Manager for each of those features, subject to the existing dial plan.

Some CM features can be invoked by dialing a Communication Manager Feature Access Code (FAC). FACs must be defined in Communication Manager for each of those features, subject to the existing dial plan.

Note:

Most FNEs require first configuring the equivalent FAC.

Features

SIP Software Release 4.4 introduces support for the following :

Support for Auto Login parameters in server profiles

In SIP 4.4, a user can now have a different auto-login for each server.

If the IP Deskphone configuration parameter AUTOLOGIN_ENABLE is configured as 2 or USE_AUTOLOGIN_ID, then the UserID, AuthID, and Passwd values are extracted from the AUTOLOGIN[_ID_KEY|_AUTHID_KEY|_PASSWD_KEY] configuration parameters.

Server profiles support all configurations of the AUTOLOGIN_ENABLE parameter.

If the AUTOLOGIN_ENABLE parameter in a profile is configured as 0(or NO) or 1 (or YES), then the configuration file behaves as if there was no profile.

If the AUTOLOGIN_ENABLE parameter in the profile is configured as 2 (or USE_AUTOLOGIN_ID), the IP Deskphone performs a soft reset. After the soft reset, users specified by the AUTOLOGIN[_ID_KEY|_AUTHID_KEY|_PASSWD_KEY] configuration parameters are logged in.

If the profile does not contain the AUTOLOGIN_ENABLE parameter, the parameter from the System Configuration file is used.

Note:

Auto login user names and passwords are not printed using the *prtcfg* command as they are not stored in the system configuration file and are secure parameters which should not be displayed.

For more information, see Auto Login parameters in server profiles on page 242.

No soft reset for IPv6 address change

With SIP 4.4, the IP Deskphone no longer performs a soft reset if the phone's IPv6 address(es) changes.

Note:

The IP Deskphone still performs a soft reset if the phone's IPv4 address changes.

If the IP Deskphone receives a new IPv6 address and this address is the best address for any active SIP connection, the following occurs:

- All users associated with this connection are logged out.
- The new address is added to the list of SipApp's addresses.
- The connection is re-established using the new best IPv6 address.
- Users associated with this connection are logged in automatically.

If the IP Deskphone's IPv6 address becomes deprecated, and that IP address is currently in use for any active SIP connections, the following occurs:

- All users associated with this connection are logged out.
- The deprecated address is removed from the list of SipApp's addresses.
- The connection is re-established using some other IPv6 address (if there is one).
- Users associated with this connection are logged in automatically.

In the preceding situations, if there is an active call at the time when the new best IPv6 address is added or the current IPv6 address becomes deprecated, the following message is displayed on the IP Deskphone screen:

`Phone will reconnect`

instead of `SIP reset after call`.

Connection is re-established after the active call is completed.

If the IP Deskphone's IPv6 address is removed and the IP address is currently used for any active SIP connection, the following occurs:

- All SIP sessions and active calls associated with this connection are terminated.
- The IP address is removed from the list of SipApp's addresses.
- The connection is re-established using another IPv6 address (if one is available).

RTP/SRTP port changes

There are changes in the allowed values of the RTP_MIN_PORT and RTP_MAX_PORT parameters. (The changes are highlighted in bold font).

- RTP_MIN_PORT — The minimum RTP port value is an integer between **2048** and 65535, exclusive of the restricted SIP ports between 5059 and 5080. The default value is **16384**.
- RTP_MAX_PORT — The maximum RTP port value is an integer between **2048** and 65535, exclusive of the restricted SIP ports between 5059 and 5080. The default value is **32764**.

Address Book size

In the device configuration file, the MAX_ADDR_BOOK_ENTRIES parameter specifies the maximum number of entries in the Address Book. The default value has been increased from 100 to 1000. The default value is 1000 (allowed values: 0–1000).

SIP 4.4 introduces the new parameter MAX_DOWNLOAD_ADDR_BOOK_ENTRIES. This parameter specifies the maximum number of Address Book entries that can be downloaded from the network in LOCAL Address Book mode. The default value is 1000 (allowed values: 0–1000).

In LOCAL Address Book mode, if MAX_DOWNLOAD_ADDR_BOOK_ENTRIES is greater than MAX_ADDR_BOOK_ENTRIES, then only MAX_ADDR_BOOK_ENTRIES are downloaded from the network.

IP Deskphone users can add manual entries to the Address Book unless the size of the Address Book will exceed the MAX_ADDR_BOOK_ENTRIES parameter. The number of entries that can be added manually is the difference between MAX_ADDR_BOOK_ENTRIES and MAX_DOWNLOAD_ADDR_BOOK_ENTRIES.

For more information, see Address Book on page 192.

Case-insensitive Directory search

SIP Software Release 4.4 introduces the case-insensitive Directory search.

When a Directory search is initiated, the displayed Address Book entries are sorted based on the entered characters, no matter what case was used. When Name search or First Character search methods are used, the first item which fits the entered search criterion is selected. Navigation keys are used to view other items which fit the entered criterion

Note:

This enhancement is available for English only.

For more information, see the IP Deskphone User Guide for the desired model.

Additional supported redirect scenarios

SIP 4.4 introduces support for the following redirect scenarios:

- Redirect from IPv4 to IPv6 SIP proxy through UDP, TCP and TLS
- Redirect from IPv6 to IPv4 proxy through TCP and TLS
- Redirect from IPv6 to IPv6 SIP proxy with the IPv6 address belonging to a different IPv6 scope through UDP

IP Deskphone behavior when DHCPv4/DHCPv6 server is unreachable

If the DHCPv4/DHCPv6 server is unreachable due to the following scenarios:

- IP Deskphone starts and cannot get IPv4 address from DHCPv4 server (cached IP is disabled)
- IP Deskphone starts and cannot get IPv6 address from DHCPv6 server (cached IP is disabled)
- IPv4 address lease expires (cached IP is disabled)
- IPv6 address becomes deprecated and there are no active calls (cached IP is disabled)
- IPv6 address lease expires (cached IP is disabled)

then the following message is displayed on the IP Deskphone display screen:

```
DHCP server unreachable. Trying to contact...
```

Note:

If the IPv6 address becomes deprecated and there is an active call, the message is displayed on the IP Deskphone display screen after the active call is released.

When this message is displayed, the user can:

- wait until the IP Deskphone receives the required IP address from DHCP
- open the **Device Settings** menu (by double-pressing the **Services** key) and try to re-configure the IP Deskphone

The message window closes automatically when the IP Deskphone receives a new valid IPv4/IPv6 address.

For more information, see DHCP server unreachable on page 348.

Handling fixed keys for multiple calls

In SIP 4.4, the behaviour of the following fixed keys when there are multiple calls has been aligned:

- Line key
- Goodbye/Release button
- Mute
- Hold
- Handsfree
- Headset
- Hookswitch

If there is an active established call, the key action applies to this active call.

When there is no active call, the key action is applied to the call that is highlighted in the list of calls

Phone behavior after fixed key press

If there is one or more calls, the behavior of the IP Deskphone after pressing a fixed key is the following:

Goodbye/Release, Mute, Hold, Headset, Handsfree and Hookswitch:

If there is an active established call, the key action applies to this active call.

If there is no established call, the key action is applied to the call highlighted in the list of calls.

Note:

Some actions may be ignored in certain conditions, such as:

- pressing the Mute key for a call on hold
- pressing the Goodbye/Release key for a call on local hold
- pressing the Hold key for an incoming call

Line key:

If there is an incoming call, that call is answered.

If there is an active call, the key press is ignored.

If there are no incoming or active calls, the key action is applied to the call highlighted in the list of calls

Note:

If there is an active established call, and at the same time another call comes in, pressing the Line key puts the active call on hold and the incoming call is answered.

If there are several incoming calls at the same time, the newest call is answered. In order to answer a different call, the user must select the call and press the corresponding soft key.

Soft key:

Soft keys always perform actions on the highlighted call.

For more information, see the IP Deskphone User Guide for the desired model.

Duplicate IPv6 addresses

When the IP Deskphone receives an IP address from the DHCPv6 server and detects that this address is duplicated in the network,

`Duplicated IPv6 Address`

is displayed on the phone screen. There is an initial timeout of 10 seconds.

When the timeout expires,

`Starting DHCPv6`

is displayed on the phone screen and the IP Deskphone makes five attempts to contact the DHCP server.

If the DHCPv6 server sends a REPLY message in answer to the DECLINE message, the IP Deskphone removes the duplicate IP address from the list of IPv6 addresses, resources associated with the duplicate address are freed, and the DHCP process restarts.

If no reply is received, the duplicate address is removed, resources associated with the duplicate address are freed, and the DHCP process restarts.

For more information, see Duplicate IPv6 addresses from DHCPv6 server on page 347.

IP Deskphone behavior during a non-consultative transfer

When a user transfers a call, then the IP Deskphone prompts with the following question: "`Consult with party?`". Pressing the **No** soft key initiates a non-consultative transfer.

With SIP 4.4, a soft key with the caption "**Exit**" has been added to the transfer dialog for a non-consultative transfer. Pressing this soft key closes the "**Transferring....**" dialog . The IP Deskphone then displays any local calls, including the transferred call. The transferred call displays a state of "**Transferring**" until "**Transfer successful**" or "**Transfer failed**", is displayed, depending on the transfer results.

For more information, see the IP Deskphone User Guide for the appropriate model.

Debug port security

SIP 4.4 introduces a security change to prevent unauthorized access and intervention in IP Deskphone operation through the debug port (Accessory Expansion Module (AEM) port) when a dongle is used.

The debug port is now disabled by default; enabling the debug port requires access to the **Advanced Diag Tools** menu, which is always protected by the admin password.

The configuration option **Debug port** has been added to the **Advanced Diag Tools** menu. The default value is **disabled**.

For more information, see Debug port security on page 266.

HTTPS support in BootC mode

In SIP 4.4, the following functionality is introduced:

- When a firmware upgrade is performed and there is not enough memory for the upgrade, the IP Deskphone automatically reboots in BootC mode and upgrades in BootC. After the upgrade is completed, the IP Deskphone automatically reboots again and starts up in normal mode.
- Support of HTTPS protocol (for provisioning and firmware upgrades) is added to BootC mode.

Automatic firmware upgrade using BootC

When a firmware upgrade is performed and there is not enough memory to allocate a buffer for new firmware, the IP Deskphone automatically reboots and BootC is loaded.

BootC downloads the provisioning file (for example, 1120eSIP.cfg). Only the [FW] section of this file is processed. BootC uses the same settings (for example, Provisioning Server URL, protocol) that are used in normal mode.

BootC performs the firmware upgrade, and the IP Deskphone automatically reboots again.

The IP Deskphone starts up with new firmware in Normal mode.

Note:

Regardless of whether the firmware upgrade was successful or not, the [FW] section does not offer to update during the IP Deskphone reboot.

Support of HTTPS protocol in BootC

HTTPS is supported for downloading provisioning files (for example, 1120eSIP.cfg) and firmware images from the Provisioning Server. It uses the embedded and customer certificates that are installed on the IP Deskphone.

Important:

Customer certificates must be installed in Normal mode.

Both mutual authentication and server-only authentication methods are supported.

The TLS connection cipher is set according to the security policy configured on the IP Deskphone (the security policy must be configured in Normal mode). The default cipher is TLS_RSA_WITH_AES_256_CBC_SHA.

For more information, see HTTPS support in BootC mode on page 298.

Permanently disable Port Mirroring

SIP 4.4 introduces the ability to permanently disable Port Mirroring through provisioning. When Port Mirroring is permanently disabled, it cannot be enabled in the **Advanced Diag Tools** menu or by using the special key combination.

In SIP 4.4, when the existing PORT_MIRROR_ENABLE configuration parameter is set to NO, the Port Mirroring feature is permanently disabled. The Port Mirroring prompt in the **Advanced Diag Tools** menu is disabled and cannot be modified. This is the default.

If the PORT_MIRROR_ENABLE configuration parameter is set to YES, the Port Mirroring prompt in the **Advanced Diag Tools** menu is enabled and can be modified. If enabled, the Port Mirroring setting survives a soft reboot of the IP Deskhone, but not a power off. If the IP Deskphone is powered off, Port Mirroring becomes disabled.

Toggling Port Mirroring on and off by using the key sequence ([MUTE]-[UP]-[DOWN]-[UP]-[DOWN]-[UP]-[7]) is no longer supported; if Port Mirroring is enabled through the provisioning file, it can only be turned on and off through the Port Mirroring option in the **Advanced Diag Tools** menu.

For more information, see Port Mirroring on page 357 and Feature configuration commands on page 73.

Improvements in *prtcfg* pdt command output

SIP 4.4 enables faster debugging as the configuration of a customer's phone can be easily converted into a config file for duplicating problems.

The output can be directly copied to another phone's .cfg file. Displayed names match the device configuration file parameter names. The output now matches the device configuration file format. Previously missing parameters are now listed and detailed server profile information is shown.

SIP Software Release 4.4 provides the following enhancements to the output of the `prtcfg` pdt command:

- All printed parameters and their values correspond with parameters and values that can be provisioned on the IP Deskphones.
- DHCP information has been added to the system configuration section of the command output.
- The parameter **device certificate version** has been added to the command output.
- Domain-related information has been grouped together and is now separated by "**# comments**" for ease of use.

- Detailed configured server profiles information has been added to the command output.
- The displayed values of ADMIN_PASSWORD and other passwords have been replaced by "***" in the command output

Miscellaneous changes for IP Deskphones

Default input mode in Address Book

The default input mode for a telephone number has been changed to `123` when adding a new entry to the Address Book of an IP Deskphone.

User ID on IP Deskphone display

The User ID is still displayed near the Primary DN key of the IP Deskphone display, but is no longer displayed in the Context field.

Releasing a call on hold

An IP Deskphone user can no longer release a call on hold by pressing the Goodbye key. The IP Deskphone user is now required to retrieve the call from hold and then release it by pressing the Goodbye key or hanging up the handset.

Improved user interface during multiple calls

SIP 4.4 brings a more predictable user interface operation to the IP Deskphone. Fixed key presses (for example, line, hold, release, mute, headset, hookswitch) are now applied to the active call. If there is no active call, the action is applied to the highlighted call.

Instant Message display

The Instant Message Details window on the IP Deskphone now uses the full display area.

CALL_ORIGIN_BUSY parameter

This parameter determines if the user is presented with an incoming call when entering the address of an outbound call.

In SIP 4.4, it is no longer necessary for the DOD_ENABLE parameter to be set to YES to enable the CALL_ORIGIN_BUSY parameter.

Avaya Aura®-specific features

This section contains information on SIP 4.4 features and functionality specific to 1100 Series IP Deskphones with SIP 4.4 Software in an Avaya Aura® environment.

Presence support for 1100 Series IP Deskphones

SIP 4.4 introduces support for the Presence feature for 1100 Series IP Deskphone users on Avaya Aura® with Avaya Presence Server (PS).

The Presence feature is configured in SIP 4.4 with the following new configuration parameters:

- RPID_PRESENCE_ENABLE <YES/NO>
- PRES_SERVER_IP <IP address of Presence Server>

If the RPID_PRESENCE_ENABLE parameter is set to YES, RPID-based subscription and notification messages, required for Avaya Presence Services, are sent.

PRES_SERVER_IP parameter defines the IP address of the Avaya Presence Server.

Important:

If RPID_PRESENCE_ENABLE is configured as YES:

- The IP Deskphone must be configured to use TLS for connection to the SIP proxy.
- USE_PUBLISH_FOR_PRESENCE must be set to YES.
- USE_DEFAULT_DEV_CERT must be set to YES to use the default device certificate for the TLS connection to Avaya Aura to work with the contact list stored on Avaya Aura Session Manager.
- ENABLE_SERVICE_PACKAGE must be set to PPM.
- In the phone's Communication Profile, check **Presence Profile** and select the appropriate Presence Server from the drop-down list.

Presence states

Presence dialog has been expanded to include the list of activities according to RFC4480.

The following activities are available when RPID_PRESENCE_ENABLE is set to YES:

Appointment	Permanent absence
Away	Playing
Breakfast	Presentation
Busy	Shopping
Dinner	Sleeping
Holiday	Spectator
In transit	Steering
Looking for work	Travel
Lunch	TV
Meal	Vacation
Meeting	Working
On the phone	Worship
Performance	Unknown

To set the desired presence state and activity, the IP Deskphone user must open the Presence dialog, select the presence state (Connected or Unavailable) and then select the desired activity. Any combination of presence state and activity can be selected.

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382
Presence status in Address Book on page 23

Presence status in Address Book

The status dialog of the Address Book displays the presence state of contacts designated as Friends. In SIP 4.4, the IP Deskphone Address Book displays the presence state of Friends if RPID_PRESENCE_ENABLE is set to YES.

Phone state

Phone state is determined automatically, based on notifications received from Avaya Presence Server. Phone state can be one of the following:

- On hook – when the phone handset is on hook; there are no active calls
- On a call – the user is on a call
- Do Not Disturb – when the user activated Do Not Disturb mode
- Unknown

Note:

Phone state does not depend on the presence state and activity selected by the end user.

Note:

- The 1100 Series IP Deskphones support more presence states than the Aura Presence Server (PS); activity detail appears on the 1100 Series and 1200 Series IP Deskphones but not on Avaya 96xx Series phones.
- Idle 1100 Series IP Deskphones appear as "offline" in the Avaya 96xx Series phones presence status; however, Busy, On the Phone and Away activities are displayed correctly.

Related links

Presence support for 1100 Series IP Deskphones on page 21

Personal Profile Manager support

SIP 4.4 introduces support of the Personal Profile Manage (PPM) for Avaya Aura Communication Manager/Session Manager.

The PPM) is a web service that runs as part of the Avaya Aura® Session Manager and the System Manager. PPM processes SOAP messages over HTTP/HTTPS with digest authentication.

PPM is responsible for maintaining and managing an end user's personal information in the system. This information includes (but is not limited to) contact list information, profile information, session history, access control lists, and other permissions management. In addition to communicating with other server components for managing the data within the infrastructure servers, the PPM also interfaces directly with end clients.

SIP 4.4 supports the following functionality with PPM:

- retrieving contact list from PPM

- adding and deleting contacts
- updating contact
- searching user
- retrieving E911 numbers
- PPM reboot mechanism

Configuration parameter

The ENABLE_SERVICE_PACKAGE configuration parameter is expanded to include the value PPM, which switches the mode to obtain PPM data.

Global search with PPM

When PPM is enabled, and a global search is initiated from the IP Deskphone, PPM allows the IP Deskphone to search the Session Manager database for administered users. This search is based on search criteria sent in the request. IP Deskphone users can search using the following criteria:

- User Name (login name of the user; for example, 508@abc.com)
- First Name
- Last Name
- Phone Number

All users who correspond to the submitted criteria are retrieved from the database and displayed as list. It is possible to call any contact in the list, save any contact from the list to the Adress Book, and view the contact details

Note:

A maximum of 250 contacts can be loaded from PPM using global search.

Embedded device certificates

TLS connection with Avaya Aura® Session Manager requires mutual authentication by default. Mutual authentication requires proper Certificate Authority (CA) and device certificates to be installed on every IP Deskphone.

SIP 4.4 includes a default device certificate in the firmware, allowing easy connection to Avaya Aura through Session Manager using TLS . The IP Deskphones already have an embedded CA certificate which is trusted by Avaya Aura®; the embedded device certificate eliminates the need for customers to generate and install device certificates manually.

If used, embedded device certificate information is displayed in the IP Deskphone and in the output of appropriate PDT commands.

The default embedded device certificates are trusted by the Avaya Aura® system. If Aura is configured so that default certificates are replaced by customer certificates, then appropriate CA and device certificates must be installed on the IP Deskphones.

Important:

The default embedded device certificates are trusted by the Avaya Aura® system. If Aura® is configured so that the default certificates are replaced by customer certificates, then the appropriate CA and device certificates must be installed on the IP Deskphones as well.

Configuration

To support the embedded device certificate, SIP 4.4 introduces the following parameter:

USE_DEFAULT_DEV_CERT [YES/NO]

— YES – Use the default device certificate if no customer device certificate is installed.

— NO – Do not use the default device certificate (default).

This parameter controls the use of the default device certificate for HTTPS/TLS connections. The default value is NO. It is configured in the device configuration file.

SRTP support with Avaya Aura®

SIP 4.4 introduces support for SRTP with Avaya Aura®.

Note:

To use SRTP, you first have to be using TLS. That is, you cannot have secure media without using secure signalling.

The following SRTP modes are supported:

- Secure Only
- Best Effort Capability Negotiation

Configuration

SIP 4.4 introduces the following parameter to support SRTP on Avaya Aura®:

AVAYA_AURA_MODE_ENABLE [YES | NO]

The command specifies if Avaya Aura®-specific features are active on the IP Deskphone or not. The default value is NO. It can be configured through the device configuration file and through server profiles.

— YES – Avaya Aura-specific features are active.

— NO – Avaya Aura-specific features are not active.

Important:

In the device configuration file, the parameter MKI must be set to NO.

Session Border Control support

Session Border Control (SBC) enables secure access for remote users.

SIP 4.4 supports the Avaya SBC for Enterprise 6.2 when the IP Deskphone is configured to use TLS.

Other changes

Migration information

The following migration information has been added to this document:

1. UNIStim IP Deskphone migration from CS 1000 to Avaya Aura®. See Migrating UNIStim IP Deskphones from CS 1000 to Avaya Aura using Aura Utility Server on page 407.
2. SIP IP Deskphone migration from MCS 5200 to Avaya Aura®. See Migrating IP Deskphones with SIP software from MCS 5200 to Avaya Aura® using Aura® Utility Server on page 415.
3. Migrating IP Deskphones with UNIStim firmware from CS 1000 to IP Office. See Migrating IP Deskphones with UNIStim firmware from CS 1000 to IP Office on page 423.

User provisioning

Information on IP Deskphone user provisioning using System Manager 6.3 FP2 has been added to this document. See User provisioning using System Manager 6.3 FP2 on page 429.

Adding the IP Deskphone to Avaya Aura

A Quickstart Guide — Add an 1100 Series IP Deskphone to Avaya Aura® has been added to this document. See Adding a new IP Deskphone to Avaya Aura® on page 434.

Configuring FACs and FNEs

Information on configuring FACs and FNEs on Avaya Aura® for the IP Deskphones has been added to this document. See Configuring FACs and FNEs for the IP Deskphones on page 437.

Creating speed dial lists

Information on creating a speed dial list on the IP Deskphone has been added to this document. See Creating a speed dial list on page 441.

Additional information

An appendix containing a listing of reference material and additional documentation has been added to this document. See Reference and additional documentation on page 444.

Revision history

December 2015	Standard 06.06. This document is up-issued for the following changes: • Update information about device certificate installation, including PKCS#12 and SCEP.

Table continues…

	• Update information about EAP-TLS.
July 2015	Standard 06.05. This document is up-issued for the following changes: • Remove information about support of Avaya one-X client software. • Add limits for a Speed Dial List. • Change supported bit rate for the G.722 codec from 48 Kbps to 64 Kbps.
March 2015	Standard 06.04. This document is up-issued for the following changes: • Add SURV_SIP_SVR_ENABLE and TCP_SIP_PING_FAILBACK to the list of server and network configuration commands. • Add BLIND_TRANSFER_EARLY_RELEASE, DST_START, DST_STOP, LINE_KEY_SCROLLING, and USE_CONTACT_IN_REFERTO to the list of feature configuration commands. • Add definitions for the LINE_KEY_SCROLLING, and USE_CONTACT_IN_REFERTO feature configuration commands.
January 2015	Standard 06.03. This document is up-issued to add the following items: • Change the definition and default setting of the MAX_RING_TIME option.
September 2014	Standard 06.02. This document is up-issued to add the following items: • Add new SURV_SIP_SVR_ENABLE, BLIND_TRANSFER_EARLY_RELEASE, TCP_SIP_PING_FAILBACK, DST_START, DST_STOP options. • Add updated information to the TIMEZONE_OFFSET and FAST_EARLY_MEDIA_ENABLE options. • Change the maximum image size for 1140E and 1165E models from 512 MB to 512 KB. • Update the description of the Speakerphone Exclusive to 911 Emergency feature.
November 2013	Standard 06.01. This document is up-issued to support SIP Software Release 4.4.
September 2013	Standard 05.02. This document is up-issued to reflect changes in technical content for the DEF_AUDIO_QUALITY parameter and a note has been added to Codecs preferences on the IP Deskphone on page 271.
June 2013	Standard 05.01. This document is up-issued to support SIP Software Release 4.3 Service Pack 2 (SP2).
April 2013	Standard 04.07. This document is up-issued to reflect changes in technical content in the section **"IP Deskphone bug logging/recovery commands"**.
November 2012	Standard 04.06. This document is up-issued to remove references to Broadsoft.
April 2012	Standard 04.05. This document is up-issued to reflect re-branding changes in the "Configure the DHCP Server" section and changes to the technical content in the "IP DeskPhone security configuration" and the "Server and network configuration commands" sections.

Table continues…

March 2012	Standard 04.04. This document is up-issued for changes to the “Multiuser” and “Multiple Appearance Directory Number” sections.
February 2012	Standard 04.03. This document is up-issued to include revisions to Busy Lamp Field on page 203 and for changes in technical content in the section Configure the DHCP server to support SIP IP Deskphone class identifier on page 132.
December 2011	Standard 04.02. This document is up-issued to support SIP 4.3 with changes in technical content for keep-alive parameter values.
December 2011	Standard 04.01. This document is up-issued to support SIP 4.3.
September 2011	Standard 03.05. This document is up-issued to reflect changes in technical content for the inclusion of the FAIL_BACK_TO_PRIMARY configuration parameter.
August 2011	Standard 03.04. This document is up-issued to reflect changes in technical content for Node lock licensing.
May 2011	Standard 03.03. This document is up-issued to reflect changes in global power supply information and information on supported languages.
May 2011	Standard 03.02. This document is up-issued to reflect changes in technical content for: • AUTOLOGIN_ID_KEY parameters • roaming profiles and network address book • reset codecs to default • modifying the SIP provisioning file
April 2011	Standard 03.01. This document is up-issued to support SIP Software Release 4.1.
January 2011	Standard 02.03. This document is published to support SIP Software Release 4.0.
January 2011	Standard 02.02. This document is up-issued to support SIP Software Release 4.0.
October 2010	Standard 02.01. This document is up-issued to support SIP Software Release 4.0.
October 2010	Standard 01.04. This document is up-issued to reflect changes in technical content for TLS.
October 2010	Standard 01.03. This document is up-issued to reflect changes in technical content for Licensing.
September 2010	Standard 01.02. This document is up-issued to add content for Multi-Level Precedence and Preemption.
August 2010	Standard 01.01. This is a new document for Avaya 1100 Series IP Deskphones and is issued to support SIP Software Release 3.2.

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to http://www.avaya.com/support or go to one of the pages listed in the following sections.

Navigation

- Getting technical documentation on page 29
- Getting product training on page 29
- Getting help from a distributor or reseller on page 29
- Getting technical support from the Avaya Web site on page 30

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to http://www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at http://www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at http://support.avaya.com.

Chapter 3: Introduction to this guide

Subject

SIP Software for Avaya 1100 Series IP Deskphones — Administration, NN43170-600 describes how to install, configure, and provision the Avaya 1120E IP Deskphone, Avaya 1140E IP Deskphone, and Avaya 1165E IP Deskphone for use on a SIP network. These IP Deskphones are collectively known as Avaya 1100 Series IP Deskphones. In this document, the Avaya 1100 Series IP Deskphones are referred to as IP Deskphones.

Part II

Part II of this document, Avaya Aura® support for 1100 Series IP Deskphones on page 382, provides information specific to the 1100 Series IP Deskphones with SIP Software on an Avaya Aura® system.

Part III

Part III of this document, IP Deskphone migration on page 404, provides information on how to migrate 1100 Series IP Deskphones in the following scenarios:

- UNIStim IP Deskphone migration from CS 1000 to Avaya Aura® on page 405
- SIP IP Deskphone migration from MCS 5200 to Avaya Aura® on page 413
- UNIStim IP Deskphone migration from CS 1000 to IP Office on page 421

Appendix information

The following appendices provide additional information:

- User provisioning using System Manager 6.3 FP2 on page 429
- Quickstart - Add an 1100 Series IP Deskphone to Avaya Aura on page 434
- Configuring FACs and FNEs for the IP Deskphones on Avaya Aura® on page 437
- Creating a speed dial list on page 441
- Reference and additional documentation on page 444

Intended audience

This administration guide is intended for system administrators of the Avaya 1120E IP Deskphone, Avaya 1140E IP Deskphone, and Avaya 1165E IP Deskphone with a basic understanding of SIP. This guide is not intended for end users of the Avaya IP Deskphones . Many of the tasks outlined in the guide influence the function of the IP Deskphone on the network and require an understanding of telephony and Internet Protocol (IP) networking.

Acronyms

This guide uses the following acronyms:

Table 1: Acronyms used

AAA	Authentication, Authorization, and Accounting
ALG	Application Layer Gateway
BER	Bit Error Rate
CA	Certificate Authority
CN	Common Name
CRL	Certificate Revocation List
CTL	Certificate Trust List
DCP	Device Certificate Profile
DET	Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DND	Do Not Disturb feature
DNS	Domain Name System
DOD	Department of Defense
DRegex	Digit Regular Expression
DSCP	Differentiated Services Code Point
DSN	Defense Switched Network
EAP	Extensible Authentication Protocol
ECR	Error Collection and Recovery
EJBCA	Enterprise Java Bean Certificate Authority
ERE	Extended Regular Expressions
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GARP	Gratuitous Address Resolution Protocol
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over SSL

Table continues…

IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
ISDN	Integrated Services Digital Network
IM	Instant Message
IP	Internet Protocol
IPv6	Internet Protocol version 6
ITU-T	Telecommunications Standardization sector of the International Telecommunications Union
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
MADN	Multiple Appearance Directory Number
MD5	Message Digest v5
MLLP	Multi-Level Precedence and Pre-emption
MS	Avaya Media Server
NAT	Network Address Translator
NetConfig	Configuration screens available after an IP Deskphone resets
NDU	Network Diagnostic Utility
OAM	Operation, Administration (and) Maintenance
PDT	Problem Determination Tool
PEAP	Protected Extensible Authentication Protocol
PEC	Product Engineering Code
PKCS#12	Public Key Cryptographic Standard #12
POE	Power Over Ethernet
POSIX	Portable Operating System Interface
PRACK	Provisional Acknowledgement
PSTN	Public Switched Telephone Network
PVQMon	Proactive Voice Quality Monitoring
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RTCP	Real-time Control Protocol
RTCP XR	RTP Control Protocol Extended Reports
RTP	Real-time Transfer Protocol
SAN	Subject Alternate Name
SCA	Single Call Arrangement Shared Call Appearance
SCEP	Simple Certificate Enrollment Protocol

Table continues…

SDP	Session Description Protocol
SDESC	Session Description Protocol
SFS	Security File System
SFTP	Secure File Transport Protocol
SSH	Secure Shell Handler
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SKS	Special Key Sequence
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SRTCP	Secure Real-time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol
STUN	Simple Traversal of UDP through NAT devices
TCP	Transport Control Protocol
TFTP	Trivial File Transport Protocol
TLS	Transport Level Security
TPS	Terminal Proxy Server
TTL	Time-to-live
UDP	User Datagram Protocol
UFTP	UNIStim File Transfer Protocol
UI	User Interface
UNIStim	Unified Network IP Stimulus Protocol
USB	Universal Serial Bus
VoIP	Voice over IP
VLAN ID	Virtual Local Area Network Identification
VLAN IP	Virtual Local Area Network Internet Protocol
VQMon	Voice Quality Monitoring

Related publications

Other publications related to the SIP Software for Avaya 1100 Series IP Deskphones administration are:

- *Avaya 1120E IP Deskphone with SIP Software User Guide, NN43112-101*
- *Avaya 1140E IP Deskphone with SIP Software User Guide, NN43113-101*
- *Avaya 1165E IP Deskphone with SIP Software User Guide, NN43170-100*
- *Avaya 1120E IP Deskphone with SIP Software on Avaya Aura User Guide, 16-604273*
- *Avaya 1140E IP Deskphone with SIP Software on Avaya Aura User Guide, 16-604274*

- *Avaya 1165E IP Deskphone with SIP Software on Avaya Aura User Guide, 16-604275*
- *Avaya 1100 Series Expansion Module (SIP Software) User Guide, NN43110-301*
- *Avaya 1120E IP Deskphone with SIP Software Quick Reference Guide*
- *Avaya 1140E IP Deskphone with SIP Software Quick Reference Guide*
- *Avaya 1165E IP Deskphone with SIP Software Quick Reference Guide*
- *Avaya 1120E IP Deskphone with SIP Software on Avaya Aura Quick Reference Guide*
- *Avaya 1140E IP Deskphone with SIP Software on Avaya Aura Quick Reference Guide*
- *Avaya 1165E IP Deskphone with SIP Software on Avaya Aura Quick Reference Guide*
- Avaya 1100 Series IP Deskphone product bulletins on http://www.avaya.com/support.

Chapter 4: Overview

Introduction

This chapter describes the hardware and software features of the Avaya 1120E IP Deskphone, Avaya 1140E IP Deskphone, and Avaya 1165E IP Deskphone with SIP Software Release 4.4. In this document, Avaya 1100 Series IP Deskphones will be referred to as IP Deskphones.

SIP overview

Session Initiation Protocol (SIP) is a signaling protocol used for establishing multimedia sessions in an Internet Protocol (IP) network.

SIP is a text-based protocol similar to Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). With the introduction of SIP to IP Deskphones, telephony integrates easily with other Internet services. SIP allows the convergence of voice and multimedia.

Avaya 1100 Series IP Deskphones with SIP Software

The Avaya 1100 Series IP Deskphones connect to an IP network using an Ethernet connection. All voice and signaling information is converted into IP packets and sent across the network.

IP Deskphones come with UNIStim software installed and must be converted to SIP software.

If you have an IP Deskphone with UNIStim software, you can convert the software to SIP software. To download the most recent version of SIP software, see Download the SIP Software on page 46.

This guide explains how to:

- configure the provisioning server and the DHCP server. Note: The provisioning server contains the software and the configuration files for the IP Deskphones.
- convert an IP Deskphone with UNIStim software to an IP Deskphone with SIP software
- provision the Device Settings parameters on the IP Deskphone with SIP software

Important:

Converting the software on an IP Deskphone from UNIStim software to SIP software overwrites the UNIStim software. The IP Deskphone cannot operate in both modes simultaneously. A switch from UNIStim to SIP software or SIP to UNIStim software requires a software reload.

The following figure shows the main components of the Avaya 1165E IP Deskphone with SIP software.

Figure 1: Avaya 1165E IP Deskphone with SIP Software

The following figure shows the main components of the Avaya 1140E IP Deskphone with SIP software.

Figure 2: Avaya 1140E IP Deskphone with SIP Software

The following figure shows the main components of the Avaya 1120E IP Deskphone with SIP software.

Figure 3: Avaya 1120E IP Deskphone with SIP Software

Related documentation

The Avaya 1100 Series IP Deskphones with SIP Software User Guides explains how to do the following:

- use the context-sensitive soft keys and Navigation key cluster
- enter text
- use the address book
- access and use the call inbox and call outbox
- configure and use instant messaging
- receive, identify, answer, redirect, decline, or ignore an incoming call
- operate hold, three-way calling, call transfer, and call park
- use other features such as speed dial, call forward, do not disturb, and setting up conference calls

- configure Bluetooth headset operation (Avaya 1140E IP Deskphone and Avaya 1165E IP Deskphone only)
- configure Screensaver slide show (Avaya 1165E IP Deskphone only)

For more information about using the IP Deskphones, see *Avaya 1120E IP Deskphone with SIP Software User Guide, NN43112-101*, *Avaya 1140E IP Deskphone with SIP Software User Guide , NN43113-101* and *Avaya 1165E IP Deskphone with SIP Software User Guide, NN43170-100*.

The IP Deskphones Getting Started Card included in the box with the IP Deskphones explains how to do the following:

- connect the AC power adapter
- control the volume when answering a call
- make a call using the handset
- make a call with the headset or using handsfree
- use hold and mute
- set the contrast
- set the language

Installation overview

To install the Avaya 1100 Series IP Deskphones with SIP Software, three basic steps are required.

1. Configure the provisioning server and, optionally, the DHCP server. The function of the provisioning server is to provide configuration options to every IP Deskphone throughout the network. The DHCP server can be configured to provide basic network-configuration data or a more comprehensive set of network-configuration data for the IP Deskphone with SIP Software.
2. Load SIP Software on the IP Deskphone.
3. Configure the initial network-configuration parameters on the IP Deskphone with SIP Software.

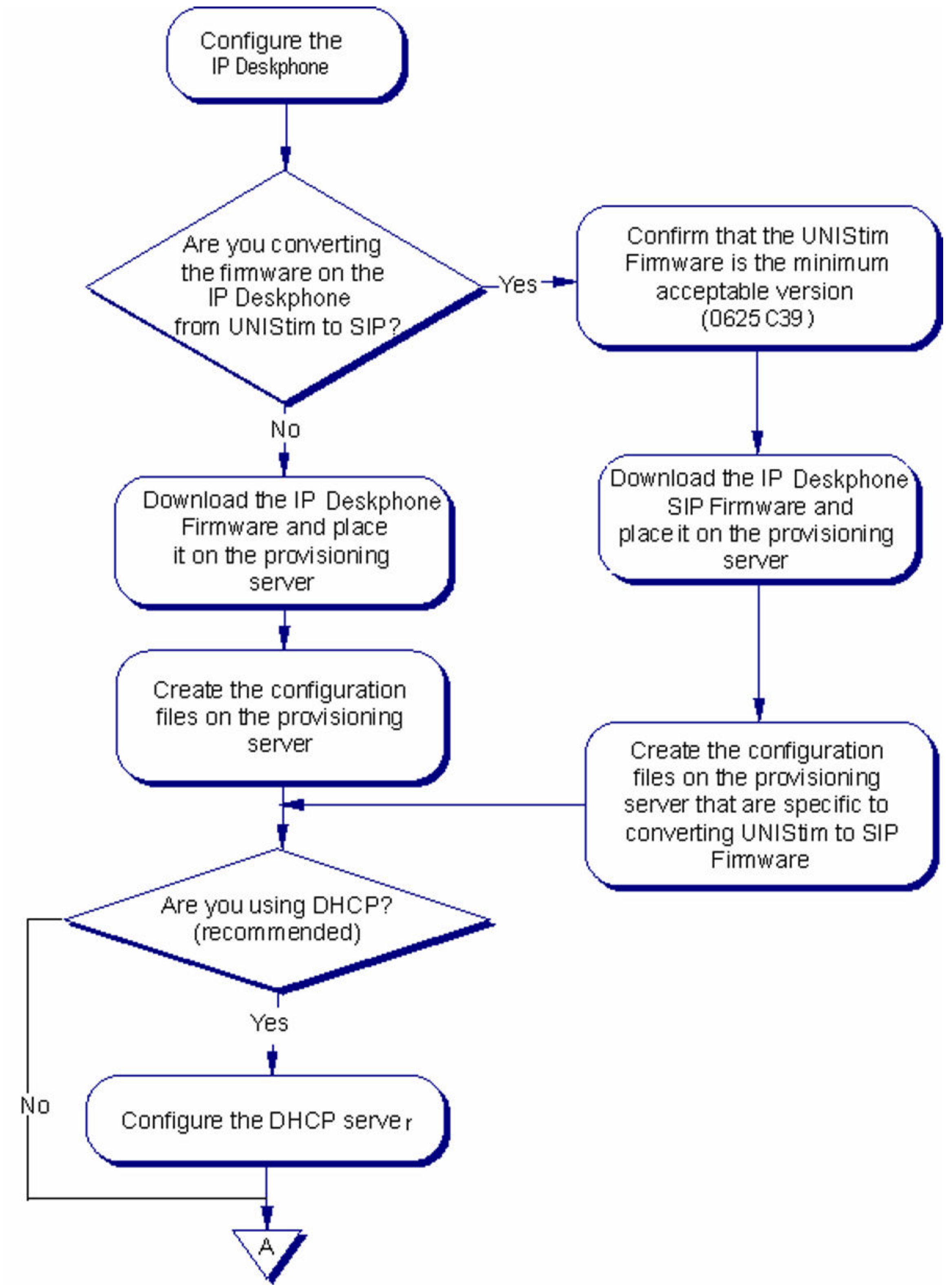


Figure 4: Installation of IP Deskphones with SIP Software, page 1 of 2

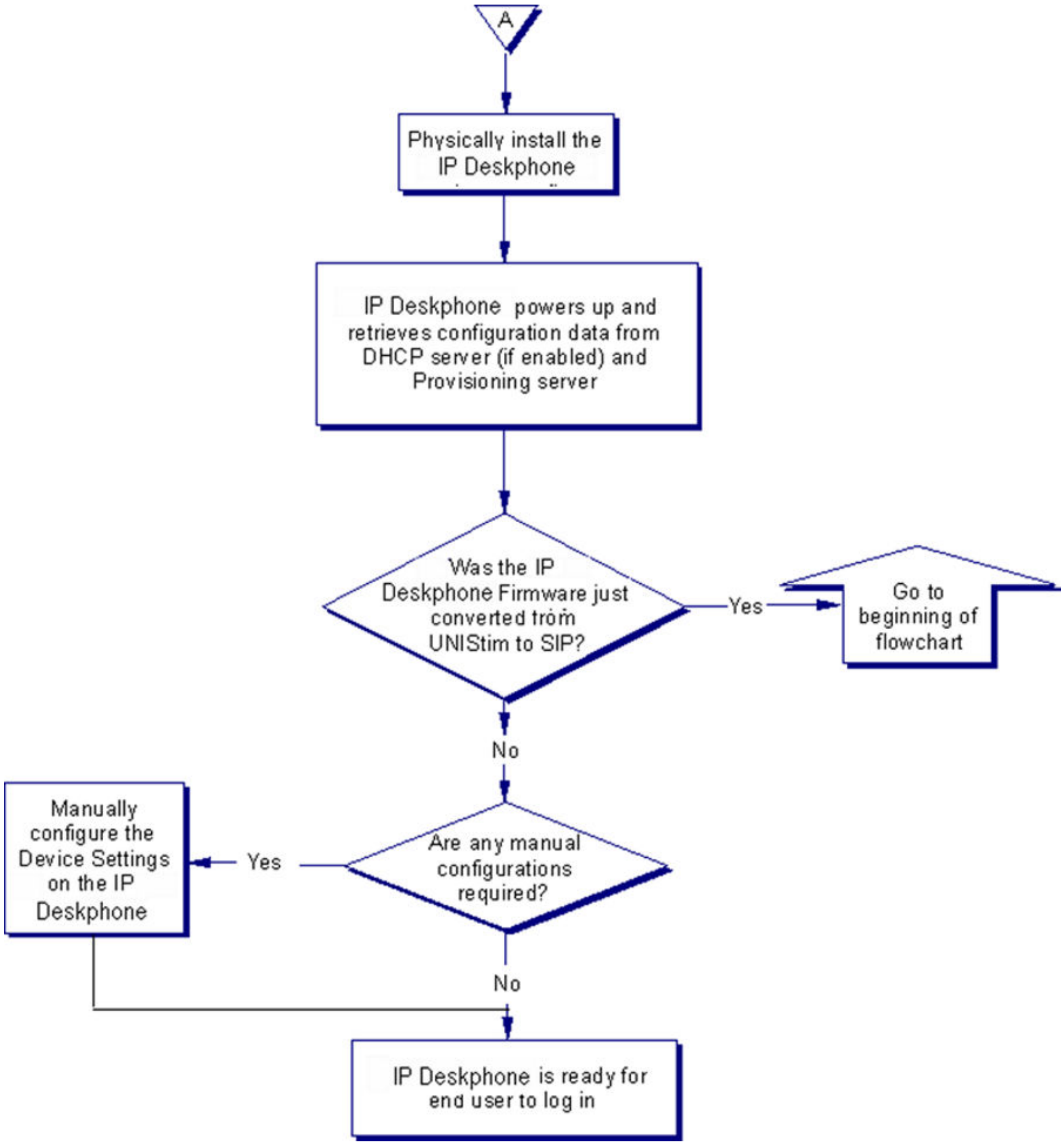


Figure 5: Installation of IP Deskphones with SIP Software, page 2 of 2

Chapter 5: Before installation

Introduction

This chapter features a checklist of tasks you must complete before you install SIP Software on the Avaya 1100 Series IP Deskphones.

Preinstallation

Complete the following checklist.

Preinstallation checklist

1. Read and become familiar with your IP Deskphone User Guide.
2. Ensure there is one IP Deskphone boxed package for each IP Deskphone being installed.
3. Ensure that the IP Deskphone box includes:
    - IP Deskphone, graphite with:
        - icon keys without PS (SIP) (RoHS), or
        - English keys without PS (SIP) (RoHS)
    - handset
    - handset cord
    - footstand kit
    - IP Deskphone number label and lens kit
    - 2.3 m (7 ft) CAT5 Ethernet cable

    The IP Deskphone can be powered either by Power Over Ethernet (POE) or through an AC adapter power supply. If required, order the AC adapter power supply separately.

    Warning:

    Do not use the AC adapter if you are connected to a Power over the Ethernet (PoE) connection. Only use the AC adapter global power supply when you do not have a PoE connection.

    If the IP Deskphone has a Graphical Expansion Module connected, the type of power supply to the IP Deskphone controls what is functional on the Expansion Module. The

Expansion Module backlight can only light when the AC adapter global power supply is present.

On the other hand, either the AC adapter global power supply or Power over Ethernet (PoE) to the IP Deskphone will power all of the Expansion Module's other functionality. To have the backlight on for the Expansion Module, the IP Deskphone should be powered by AC global power supply only.

Table 2: External power supply parts list (order separately)

CPC code	PEC code	Product description
	NTYS17xxE6	IP Deskphone Global Power Supply (2000 series, 1100 series, 1200 series) (RoHS)
N0089603	NTYS14AAE6	Standard IEC Cable - North America (RoHS)
A0781922	NTTK15AA	Standard IEC Cable – Australia / NZ (Note: RoHS not required)
N0114986	NTTK16ABE6	Standard IEC Cable – Europe
N0109787	NTTK17ABE6	Standard IEC Cable – Switzerland
N0109881	NTTK18ABE6	Standard IEC Cable – UK
N010978	NTTK22ABE6	Standard IEC Cable – Denmark
A0814961	A0814961	Standard IEC Cable - Argentina (Note: RoHS not required)
N0118951	NTTK26AAE6	Standard IEC Cable - Japan

Caution:

The IP Deskphone must be plugged into a 10/100-BaseT Ethernet jack. Severe damage occurs if this IP Deskphone is plugged into an ISDN connection.

4. Ensure that the location meets the network requirements:

   - a DNS server and a DHCP server with DHCP relay agents installed, configured, and running. Using DHCP and DNS servers with CS 2000 or Avaya Aura® Application Server 5300 networks is recommended but not mandatory.
   - An Ethernet connection to a network with an appropriate SIP proxy server.
   - One of the following file servers used as a Provisioning server:
     - TFTP server
     - FTP server
     - HTTP server
     - HTTPS server

   An IP Deskphone with SIP Software can operate with a TFTP, FTP, HTTP, or HTTPS file server.

Chapter 6: Creating the provisioning files

Important:

If you have UNIStim software on your IP Deskphone, the software must be converted from UNIStim to SIP before you proceed with the following instructions. See the chapter Upgrade and convert the IP Deskphone software on page 144 for instructions on how to convert the software on an IP Deskphone from UNIStim to SIP.

If the IP Deskphone is installed with SIP Software, further SIP Software upgrades can be done with a TFTP, an FTP, an HTTP, or an HTTPS server.

How provisioning works

Provisioning is performed without interaction with the Call Server. The Avaya IP Deskphone with SIP Software connects directly with the provisioning server in order to retrieve software files and configuration files. In this case, the provisioning server is not to be confused with the IP Client Manager on the Call Server. The methods of provisioning are:

- Automatic provisioning at power-up: After the IP Deskphone powers up or is reset, it checks the provisioning server for the latest files.
- Provisioning through user interaction: While logged in to the phone, the user can manually check for updates by pressing the **Services** key and selecting **Check for Updates**.

  Caution:

  You must not request a provisioning update while on an active call because the phone may reboot during processing of the received configuration data. While the phone checks for an update, it activates Do Not Disturb (DND). When the update is finished, DND is deactivated.
- Automatic provisioning at a preconfigured time: The IP Deskphone with SIP Software checks for updates every 24 hours, at a time specified by a parameter in the device configuration file.

The following describes the sequence of events when provisioning updates occur. The IP Deskphone with SIP Software:

1. connects to the provisioning server
2. retrieves the provisioning file (for example, 1165eSIP.cfg) from the provisioning server
3. reads and acts upon the content of the provisioning file and decides whether any other file is needed, based on a set of rules. If files need to be downloaded to the IP Deskphone, a new

file transfer session starts for each file to be downloaded. The provisioning file (for example, 1165eSIP.cfg) can contain commands that prompt for confirmation before a file is downloaded.

Download the SIP Software

To download the SIP Software from the Avaya web site, perform the following procedure.

Downloading SIP Software for the IP Deskphone

1. Go to http://www.avaya.com/support.

   The **Avaya Support** page appears.
2. Click **Downloads & Documents** in the menu at the top of the page.
3. Enter the IP Deskphone type in the **Enter Your Product Here** box.
4. From the **Choose Release** drop down list, select the desired release of SIP software.
5. In the **Select a content type** pane, click the **Downloads** radio button and click **Enter**.
6. From the search results, select the desired release of the SIP Software for the IP Deskphone.

   A new window opens.
7. Scroll down the page and click the desired version of software; for example, SIP1165e04.04.09.00.bin.

   The **File Download** window opens.
8. Click **Save**.

   The **Save As** window opens.
9. Select the location to save the file and click **Save**.
10. After the file has downloaded, place the file in the correct directory on the provisioning server.

Create the SIP provisioning files

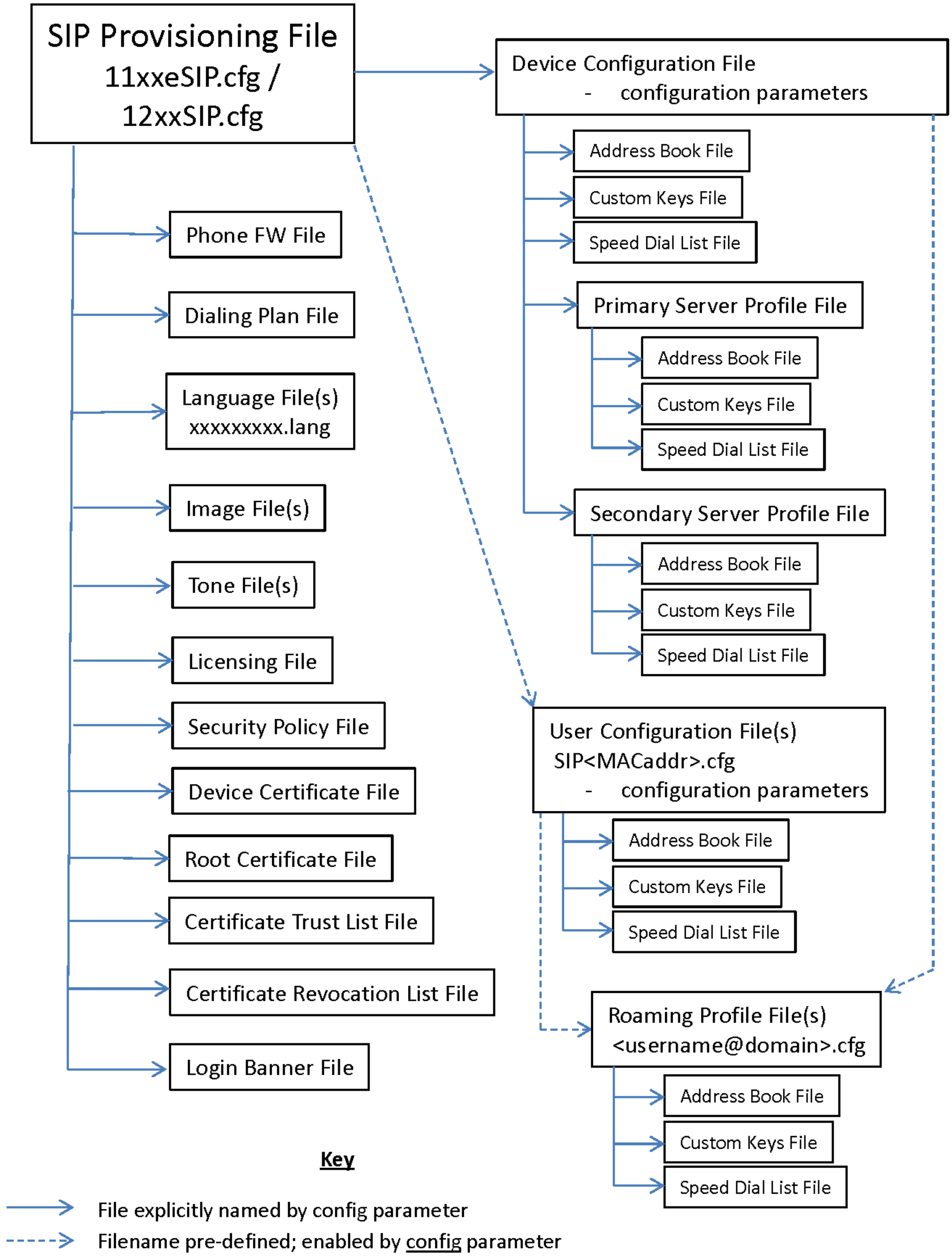
The provisioning file is saved on the provisioning server and downloaded from the provisioning server to the IP Deskphone every time the IP Deskphone checks for updates. The provisioning file is a clear text file that has the naming convention 1xxxeSIP.cfg. The provisioning file contains various sections.

The following is a graphical representation of the sections that can be contained in a provisioning file. It illustrates the files which can be explicitly named as well as those that have pre-defined names.

One thing to note is the address book, custom keys and speed dial list files can be associated with different components. The phone downloads the these configuration files on bootup or user registration (depending on the file) and then uses the parameters from them as required. An address book, custom keys and speed dial list can be associated with:

- The overall device configuration file – generally used for the phone model.
- The primary server profile – used when the phone connects to the primary server.
- The secondary server profile – used when the phone connects to the secondary server.
- Each User Configuration file – used for a specific phone.
- Each Roaming Profile file – used for a specific user login.

The configuration can be as complex or as simple as you need. For instance, all phone models in a system can point to the same address book, custom keys and speed dial list files. Or you can individualize things to specify individual files for a user, a particular phone, when a phone is connected to a particular server or even when a user is logged into a particular phone. A common application of this is to configure specific lists of features or autodials for different phones, different users, or when a phone is connected to different systems.


SIP Provisioning File
11xxeSIP.cfg /
12xxSIP.cfg
Device Configuration File
- configuration parameters
Address Book File
Custom Keys File
Speed Dial List File
Primary Server Profile File
Address Book File
Custom Keys File
Speed Dial List File
Secondary Server Profile File
Address Book File
Custom Keys File
Speed Dial List File
Phone FW File
Dialing Plan File
Language File(s)
xxxxxxxxx.lang
Image File(s)
Tone File(s)
Licensing File
Security Policy File
Device Certificate File
Root Certificate File
Certificate Trust List File
Certificate Revocation List File
Login Banner File
User Configuration File(s)
SIP<MACaddr>.cfg
- configuration parameters
Address Book File
Custom Keys File
Speed Dial List File
Roaming Profile File(s)
<username@domain>.cfg
Address Book File
Custom Keys File
Speed Dial List File
Key
File explicitly named by config parameter
Filename pre-defined; enabled by config parameter

The following is an example of an IP Deskphone provisioning file:

[DEVICE_CONFIG] DOWNLOAD_MODE AUTO VERSION 000001 FILENAME 1120DeviceConfig.dat	Device configuration section
[FW] DOWNLOAD_MODE AUTO VERSION SIP1120E04.04.09.00 PROTOCOL TFTP FILENAME SIP1120e04.04.09.00.bin	Firmware load section
[DIALING_PLAN] DOWNLOAD_MODE AUTO VERSION 000024	Dialing plan section
[LANGUAGE] DOWNLOAD_MODE AUTO DELETE_FILES YES VERSION 000024 FILENAME French.lng FILENAME Portugues.lng FILENAME Czech.lng FILENAME Russian.lng	Language files section
[IMAGES] DOWNLOAD_MODE FORCED VERSION 000003 FILENAME mountains.png FILENAME sunrise.png	Images section
[TONES] DOWNLOAD_MODE AUTO DELETE_FILES YES VERSION 000003 FILENAME ring.wav	Tone files section
[LICENSING] DOWNLOAD_MODE AUTO VERSION 000001 FILENAME ipctoken*.cfg	Licensing section
[SEC_POLICY] DOWNLOAD_MODE AUTO VERSION 000001 PROTOCOL TFTP FILENAME SecPolicy.txt	Security Policy section
[DEV_CERT] DOWNLOAD_MODE AUTO VERSION 000001 PROFILE 1 PURPOSE -1 PROTOCOL TFTP FILENAME devcert*.p12	Device certificate section
[USER_KEYS] DOWNLOAD_MODE AUTO VERSION 000001 PROTOCOL TFTP FILENAME myRootCa.pem	Root certificate section
[CTL] DOWNLOAD_MODE AUTO VERSION 000001 PROTOCOL TFTP FILENAME ctl.txt	Certificate Trust List section

Table continues…

`[CRL]`
`DOWNLOAD_MODE FORCED`
`VERSION 000002`
`FILENAME CRL.pem`
`PROMPT YES`
	Certificate Revocation List section

`[LOGGIN_BANNER]`
`DOWNLOAD_MODE AUTO`
`VERSION       000002`
`FILENAME      warning_banner.txt`
	Login banner section

`[USER_CONFIG]`
`DOWNLOAD_MODE FORCED`
`VERSION       000001`
	IP Deskphone-specific configuration files

The following table lists the supported sections in a provisioning file.

Table 3: Provisioning file supported sections

[DEVICE_CONFIG]	Device configuration file
[FW]	Firmware image
[DIALING_PLAN]	Dialing plan
[LANGUAGE]	Downloadable language files (more than one can be specified in each section)
[IMAGES]	Downloadable images
[TONES]	Downloadable tones (.wav files)
[LICENSING]	License files
[SEC_POLICY]	License policy files
[DEV_CERT]	Device certification files
[CTL]	Certificate Trust List file
[CRL]	Certificate Revocation List file
[USER_KEYS]	Root certificates
[LOGIN_BANNER]	Login banner files
[USER_CONFIG]	IP Deskphone-specific configuration files

Provisioning file sections

Provisioning is performed using the commands in the 11xxeSIP.cfg configuration file. The configuration file can have multiple sections.

Note:

The maximum length of a line item in the configuration file is 80 characters. If a line item with more than 80 characters is encountered when parsing the configuration file, the remaining portion of the file following that line item is ignored.

The '#' symbol is used to indicate a comment. Anything after a '#' symbol is a comment.

Each section in the configuration file defines rules for different file types. A section starts with a [SECTION NAME] to specify rules for each file type; for example: [FW].

A section is a mandatory field. Parsing of download rules for each file type starts with finding this key word. Currently, the following sections are supported by the IP Deskphone with SIP Software:

- [DEVICE_CONFIG]—this section is used to configure various parameters in the IP Deskphone.
- [FW] —image files originate from Avaya only and are authenticated during software download. If the FW authentication fails, the IP Deskphone displays an error message and continues operation with the existing FW image.
- [DIALING_PLAN] —this section is used for configuring dialing patterns and the format of originated URIs in the SIP message.
- [LANGUAGE] —simple text files containing all text prompts used by the IP Deskphone. Language files are used for the localization of the IP Deskphone without software upgrade. Language files are signed by Avaya and are authenticated by the software for security reasons.

  The following languages are supported. The language file name used in this section has the format <language>.lng, where <language> is the language name from the following list

  - Czech
  - Danish
  - Dutch
  - Finnish
  - French
  - German
  - Greek
  - Hungarian
  - Italian
  - Japanese
  - Latvian
  - Norwegian
  - Polish
  - Portuguese
  - Russian
  - Slovenian
  - Spanish
  - Swedish
  - Turkish
- [IMAGE]—this section is used for downloading images for backgrounds and screensavers.
- [TONES]— The IP Deskphone supports custom ringtone files. The tone files must be WAV files with the following specification: A-law or u-law (8.0 kHz, 8-bit, mono or 16.0 kHz, 16 bit mono).

The WAV files can be created and downloaded to the IP Deskphone. These files are not authenticated by the IP Deskphone.

- [LICENSING]—this section is used for downloading license files.
- [SEC_POLICY]—this section is use for downloading a file, which contains rules that define the security policy for the IP Deskphone. After the file downloads, the IP Deskphone verifies that the file is signed by a trusted entity before it accepts the values in the security policy file.
- [DEV_CERT]—this section is used for downloading a file, which contains a device certificate in PKCS12 format. Appending a * to the filename — for example, devcert*.ca — forces the IP Deskphone to look for a filename that contains its MAC address. For example; devcert001122334455.p12.
- [CTL]—this section is used to enable an IP Deskphone to download the Certificate Trust List, which is a list of trusted device certificates.
- [CRL]—this section is used to enable an IP Deskphone to download the Certificate Revocation List, which is a list of device certificates that have been revoked.
- [USER_KEYS]—this section is used to enable an IP Deskphone to download a customer root certificate.
- [LOGIN_BANNER]—this section is used to download a text file, the contents of which are displayed on the IP Deskphone immediately after logging on.
- [USER_CONFIG]—including this section header triggers the IP Deskphone to attempt to download a phone-specific user configuration file. If the IP Deskphone encounters a [USER_CONFIG] section while parsing the 1xxxeSIP.cfg configuration file, the IP Deskphone downloads the IP Deskphone-specific configuration file SIP<mac id>.cfg.

  IP Deskphone-specific configuration files support customizing the IP Deskphone on an IP Deskphone//user level. Parameters in the device configuration file can be overwritten with an IP Deskphone-specific configuration file.

  Important:

  If the 1xxxeSIP.cfg configuration file contains a [USER_CONFIG] section, Avaya recommends that DOWNLOAD_MODE be configured as FORCED. This is a global setting for all IP Deskphones used to determine if the MAC ID file should be read. Alternatively, if the user wants to use DOWNLOAD_MODE configured to AUTO, when a change is made to any MAC ID file the version number should be incremented so that all IP Deskphones read the file.

The following lists the mandatory key words in the provisioning file:

- VERSION [xxxxxx], where xxxxxx is a six- to ten-digit number representing the version of the file on the server. The version of the module is specified in this field. The command is used for version comparison in AUTO mode. VERSION is mandatory for all sections. In the FW section, the software version of the load located on the provisioning server must be entered in this field. For all other sections, VERSION is just a counter that can be incremented if it is necessary to download a new file version.

Note:

The version number of the firmware [FW] can be longer, up to 19 characters, and must follow this format:

SIP1120e04.04.09.00

SIP1140e04.04.09.00

SIP1165e04.04.09.00

Caution:

The version number is stored permanently on the IP Deskphone until a higher version number is downloaded. However, if the Forced option is in the 11xxeSIP.cfg file, then the file is forced to download and the version number in the IP Deskphone is overwritten with the version number in the 1xxxeSIP.cfg file.

- DOWNLOAD_MODE [AUTO | FORCED] defines whether the version is checked. This command is optional. If this command is not present, AUTO mode is used as the default.
  - AUTO—This mode compares the version of the module from the VERSION field and the version of the module version stored in the FLASH memory of the IP Deskphone. The file download is initiated only if the version specified is higher than the current version stored in the IP Deskphone. If the version is not applicable, as in the case of language files, the date of the file must be used for the decision.

    Caution:

    The version number stored in the FLASH is permanent until a higher number is downloaded from the Provisioning file or you select **Services > Check for Updates** on the IP Deskphone.

  - FORCED—This mode forces the software download process. FORCED can be used for software downgrade procedures.

Note:

In FORCED or AUTO DOWNLOAD_MODE, the version number is overwritten with each software download.

- FILENAME [filename]— specifies the file name to be downloaded for this section. For the language and tone section, the use of multiple filenames is allowed.

The following lists optional keywords in the provisioning file:

- PROMPT [YES | NO] is used to indicate if the IP Deskphone should prompt the user for an update before the operation is performed. This command is optional with the default configured as NO.
  - YES – enables the prompt
  - NO – disables the prompt

- PROTOCOL [TFTP | FTP | HTTP] [HTTPS] defines the protocol used to download the file. The IP Deskphone with SIP Software supports TFTP, FTP, HTTP, and HTTPS protocols for file download. This command is optional. If it is not present, the default protocol TFTP is used.

  Important:

  When using the TFTP protocol to transfer the software image, the average round trip time must be < 75 ms. The IP Deskphone times out and aborts the software download if the total download time is less than 10 minutes.

  If the average round trip time is less than 75 ms, then use the FTP, HTTP, or HTTPS protocol to transfer the software image.

  Important:

  When using HTTPS, the IP Deskphone must have a device certificate loaded on the IP Deskphone.

  If using FTP, HTTP, or HTTPS, then SRV_USER_NAME and SRV_USER_PASS are also key words. These commands specify the credentials used to log on to the file server for file download. If not present, then the protocol default credentials are used (no credentials for TFTP, HTTP, and HTTPS; and anonymous with no password for FTP).
- SERVER_IP [address] allows the IP Deskphone to connect to the specified IP address or server name for which the file can be downloaded. If the address is not specified, the SERVER_IP that is used is the same SERVER_IP that is used to download the provisioning file.
- DELETE_FILES [YES | NO], if present, erases the language and tone files stored in the IP Deskphone before new files are downloaded. Otherwise, new files with different names are added without erasing existing files. This command is optional. Note that there is a limit of 5 language files and 5 tone files that can be stored in the IP Deskphone. When the limits are exceeded, no new file can be accepted for download.
  - YES – erases the existing language and tone files
  - NO – does not erase existing language and tone files
- SRV_USER_NAME [username] – if the protocol is FTP, HTTP or HTTPS, this keyword specifies the user name to log on to the server.
- SRV_USER_PASS [password] – if the protocol is FTP, HTTP or HTTPS, this keyword specifies the password to log on to the server.
- PROMPT_AUTHNAME_ENABLE [YES | NO] — used to determine if the authentication ID screen is presented to the user during login This allows the authentication name to be different from the registration name (for example, the SIP user name). It allows the user to enter an authentication ID independent of the login ID. The authentication ID is used when the server challenges the IP Deskphone. This is required for the SCA feature to work on the Avaya Communication Server 1000 proxy. The default value is NO.
  - YES – after the user login name is entered, the authentication ID screen appears.
  - NO – after the user login name is entered, the password screen appears.

- AUTOLOGIN_AUTHID_KEYxx [* | userid@domain] is used for auto login when the AUTOLOGIN_ENABLE method is configured to USE_AUTOLOGIN_ID. If this parameter is blank and AUTOLOGIN_ENABLE is configured to USE_AUTOLOGIN_ID (or 2) in the device configuration file, then the IP Deskphone uses the value associated with AUTOLOGIN_PASSWD_KEY01.

The downloading of these files is initiated when an IP Deskphone is powered on, when an automatic check for updates is invoked, or when a user selects **Services > Check for Updates**. Any of these actions causes the IP Deskphone to contact the provisioning server and attempt to read the provisioning file. A soft reset (**Services > Reset Phone**) does not cause the IP Deskphone to retrieve the provisioning file.

Order of provisioning file sections

The SIP software processes the [DEVICE_CONFIG] and [USER_CONFIG] sections in the order that they appear in the 1xxxxSIP.cfg provisioning file. If a configuration parameter appears in both files, then the parameter value that is used depends on the order that the sections appear in the provisioning file.

For example:

1. If you have the order: [DEVICE_CONFIG], then [USER_CONFIG]:

   Result:

   The parameter value in the [USER_CONFIG] section overwrites the parameter value in the [DEVICE_CONFIG] section.

2. If you have the order: [USER_CONFIG], then [DEVICE_CONFIG]:

   Result:

   The parameter value in the [DEVICE_CONFIG] section overwrites the parameter value in the [USER_CONFIG] section.

Once the SIP phone downloads and processes configuration file parameters, it continues to use those parameter values until it either receives the parameter with a different value or the phone is reset to factory defaults.

A consequence of this is if a phone is configured to use an IP Deskphone-specific configuration file where user specific data has been configured and then is moved to a configuration without the IP Deskphone-specific file, the phone will continue to use the user specific data unless the device configuration file provides and thus overrides the configuration values already set on the phone.

An example is when the IP Deskphone-specific configuration file contains AUTOLOGIN_ENABLE USE_AUTOLOGIN_ID with auto-login credentials. If the provisioning setup is changed so the phone only receives the device configuration file, it will continue to attempt to login to the previously configured user login. To prevent this, include parameters in the device configuration file to force settings. In this example, including AUTOLOGIN_ENABLE YES or NO would avoid the potential problem.

In general, when things are not working as you would expect, look for configuration parameters that had been used in the phone's prior configuration files which are now not present. Any parameter that is not specified in a configuration file is set to the prior configured value or the factory default value (if never configured). The **`prtcfg`** tool is a good way to see what the phone is actually using for its configuration parameters. See The PDT commands on page 364 for more information on using the **`prtcfg`** command.

Setting the default language on the IP Deskphone

To configure the default language on a new IP Deskphone, or an IP Deskphone that has not been logged into by an end user, include the following in the [DEVICE_CONFIG] and [LANGUAGE] sections of the 11xxeSIP.cfg configuration file, as shown in the following example. The example shows changing the default language to French; for other languages, use the same parameters but substitute the desired language filename and name.

```
[DEVICE_CONFIG]
DOWNLOAD_MODE AUTO
VERSION 000002
FILENAME DeviceConfig.dat
```

```
[LANGUAGE]
DOWNLOAD_MODE AUTO
VERSION 0000000001
FILENAME French.lng
```

The DeviceConfig.cfg file should contain the following.

```
DEF_LANG [language]
```

On a new IP Deskphone, the language switches to the specified language after downloading and processing the configuration files. The login menu displays in the specified language. On a subsequent bootup, the login menu and all boot messages are in the specified language.

For a new user login, the IP Deskphone creates a new user profile. All menus remain in the specified language. When a new user is created, the default language used is obtained from the DeviceConfig setting and stored as a user preference, after which the user preference for language is always used.

If a user has already logged in and either defaulted or chosen English as the user language preference, changing the configuration files does not affect the user's language display.

Create the device configuration file

After the IP Deskphone downloads the provisioning file from the provisioning server, the IP Deskphone reads the [DEVICE_CONFIG] section and is directed to download the device configuration file from the provisioning server.

The device configuration file is a clear text file and the naming convention is defined by the administrator. See the FILENAME keyword in the [DEVICE_CONFIG] section of the provisioning file.

The following is an example of a device configuration file.

```
# Server and Network configuration commands
DNS_DOMAIN corp.your_company.com
SIP_DOMAIN1 your_company.com
SERVER_IP1_1 10.1.2.3
SERVER_IP1_2 10.1.2.4
SERVER_PORT1_1 5060
```

```
SERVER_PORT1_2 5060

# VOICE FEATURE configuration commands
VMAIL 5555
VMAIL_DELAY 300

# Administrative feature commands
BANNER Avaya Aura
AUTOLOGIN_ENABLE YES

# Voice Application commands
DEF_LANG English
DEF_AUDIO_QUALITY High
ENABLE_BT YES
ENABLE_3WAY_CALL NO
```

The following table provides a summary of the commands that can be used in the device configuration file. A description and the exact syntax of each command is given in Device configuration file command syntax on page 63.

Table 4: Device configuration commands summary

Configuration command type	Configuration commands	
Server and network configuration commands	SIP_DOMAIN1	SERVER_IP3_1
	SIP_DOMAIN2	SERVER_IP3_2
	SIP_DOMAIN3	SERVER_IP4_1
	SIP_DOMAIN4	SERVER_IP4_2
	SIP_DOMAIN5	SERVER_IP5_1
	SERVER_IP1_1	SERVER_IP5_2
	SERVER_IP1_2	SERVER_PORT1_1
	SERVER_IP2_1	SERVER_PORT1_2
	SERVER_IP2_2	SERVER_PORT2_2
	SERVER_PORT4_1	SERVER_PORT3_1
	SERVER_PORT4_2	SERVER_PORT3_2
	SERVER_PORT5_1	DNS_DOMAIN
	SERVER_PORT5_2	SERVER_TCP_PORT1_1
	SERVER_TCP_PORT1_2	SERVER_TCP_PORT2_1
	SERVER_TCP_PORT2_2	SERVER_TCP_PORT3_1
	SERVER_TCP_PORT3_2	SERVER_TCP_PORT4_1
	SERVER_TCP_PORT4_2	SERVER_TCP_PORT5_1
	SERVER_TCP_PORT5_2	SERVER_TLS_PORT1_1
	SERVER_TLS_PORT1_2	SERVER_TLS_PORT2_1

Table continues…

Configuration command type	Configuration commands	
	SERVER_TLS_PORT2_2	SERVER_TLS_PORT3_1
	SERVER_TLS_PORT3_2	SERVER_TLS_PORT4_1
	SERVER_TLS_PORT4_2	SERVER_TLS_PORT5_1
	SERVER_TLS_PORT5_2	
	SIP_PING	SSH
	REG_REFRESH_INTERVAL	SFTP
	SIP_UDP_PORT	SSHID
	SIP_TCP_PORT	SSHPWD
	SIP_TLS_PORT	SFTP_READ_PATTERNS
	REGISTER_RETRY_TIME	SRTP_WRITE_PATTERS
	IPV6_ENABLE	HASH_ALGORITHM
	PREFER_IPV6	EAP
	IPV6_STATELESS	EAPID1
	IPV6_ENABLE_GUI	EAPID2
	IPV6_REDIRECT_IGNORE	EAPPWD
	IPV6_MCAST_ECHO_REPLY	CA
	SRTP_ENABLED	CA_DOMAIN
	SRTP_MODE	HOST_NAME
	SRTP_CIPHER_1	DOD_ENABLE
	SRTP_CIPHER_2	MLPP_NETWORK_DOMAIN
	PCPORT_ENABLE	MLPP_ALIAS_NETWORK_DOMAINS
	DHCP_NUMBER_OF_RETRIES	MLPP_PRECEDENCE_DOMAIN
	DHCP_INITIAL_TIMEOUT	MLPP_PRECEDENCE_ENABLE
	HTTP_RETRY_NUMBER	MLPP_PRECEDENCE_DEFAULT
	FAIL_BACK_TO_PRIMARY	CACHED_IP_ENABLED
	REGISTER_RETRY_MAXTIME	LLDP_ENABLE
	KEEPALIVE_RETRIES	DHCP_UNTAG_ENABLED
	SURV_SIP_SVR_ENABLE	TCP_SIP_PING_FAILBACK
Feature configuration commands	VMAIL	MAX_PRESENCENOTE
	VMAIL_DELAY	USE_PUBLISH_FOR_PRESENCE
	IP_OFFICE_ENABLE	DEF_LANG
	IPOFFICE_MSG_CODE	IPOFFICE_REDIAL_CODE

Table continues…

Configuration command type	Configuration commands	
	IPOFFICE_CONF_CODE	LLDP_WAITING_TIME
	AUTOLOGIN_ENABLE	MAX_IM_ENTRIES
	AUTO_UPDATE	MAX_ADDR_BOOK_ENTRIES
	AUTO_UPDATE_TIME	MAX_DOWNLOAD_ADDR_BOOK_ENTRIES
	AUTO_UPDATE_TIME_ RANGE	ADDR_BOOK_MODE
	USER_FILE_ENABLE	PROXY_CHECKING
	USER_FILE_PATH	ENABLE_BT
	AUTOLOGIN_AUTHID_KEYxx	AUTH_METHOD
	PROMPT_AUTHNAME_ENABLE	BANNER
	TRANSFER_TYPE	FORCE_BANNER
	REDIRECT_TYPE	ENABLE_ANSWER_MODE
	ENABLE_PRACK	ANSWER_MODE_MAXALLOWEDADDR
	SELECT_LAST_INCOMING	ANSWER_MODE_MICMUTE
	TECH_SUPPORT_LABEL	DISPLAY_CALL_SENDER_IM_KEY
	TECH_SUPPORT_ADDRESS	SERVICE_PACKAGE_PROTOCOL
	MAX_LOGINS	DST_ENABLED
	MAX_INBOX_ENTRIES	TIMEZONE_OFFSET
	MAX_OUTBOX_ENTRIES	FORCE_TIME_ZONE
	MAX_REJECTREASONS	IM_MODE
	MAX_CALLSUBJECT	IM_NOTIFY
	FAST_EARLY_MEDIA_ENABLE	
	DEF_DISPLAY_IM	DISABLE_PRIVACY_UI
	CALL_WAITING	DISABLE_OCT_ENDDIAL
	DISTINCTIVE_RINGING	FORCE_OCT_ENDDIAL
	USE_RPORT	SNTP_ENABLE
	TOVM_SOFTKEY_ENABLE	SNTP_SERVER
	TOVM_VOICEMAIL_ALIAS	MADN_TIMER
	TOVM_VOICEMAIL_PARAM	MADN_DIALOG
	MAX_RING_TIME	DEFAULT_CFWD_NOTIFY
	ENABLE_UPDATE	FORCE_CFWD_NOTIFY
	E911_TERMINATE_ENABLE	DISPLAY_CALL_SNDR_IM_KEY

Table continues…

Configuration command type	Configuration commands	
	E911_USERNAME	RTP_MIN_PORT
	E911_PASSWORD	RTP_MAX_PORT
	KEEP_ALIVE_TYPE	SCA_HOLD_BEHAVIOR
	CONN_KEEP_ALIVE	SCA_APPEARANCES
	AUTOLOGIN_ID_KEYxx	SCA_BROADWORKS
	AUTOLOGIN_PASSWD_KEYxx	SCA_LINE_SEIZE_EXPIRES
	HOLD_TYPE	EXP_MODULE_ENABLE
	ENABLE_3WAY_CALL	PROMPT_ON_LOCATION_OTHER
	E911_HIDE_MESSAGE	E911_PROXY
	E911_TXLOC	MAX_BLFCALLS
	MENU_AUTO_BACKOUT	BLF_ENABLE
	AUTOCLEAR_NEWCALL_MSG	BLF_RESOURCE_LIST_URI
	LOGIN_BANNER_ENABLE	FM_SOUNDS_ENABLE
	SECURE_UI_ENABLE	FM_PROFILES_ENABLE
	SCRNSVR_ENABLE	FM_LANGS_ENABLE
	SCRNSVR_UPASS_ENABLE	FM_IMAGES_ENABLE
	SCRNSVR_UNPRTCTD_ENABLE	FM_CERTS_ENABLE
	SCRNSVR_TEXT	FM_CONFIG_ENABLE
	SCRNSVR_MODE	FM_LOGS_ENABLE
	SCRNSVR_DELAY	ENABLE_USB_PORT
	SCRNSVR_IMAGE	USB_MOUSE
	BG_IMAGE_ENABLE	USB_KEYBOARD
	BG_IMG_SELECT_ENABLE	USB_HEADSET
	USE_BG_IMAGE	USB_MEMORY_STICK
	SPEEDLIST_KEY_INDEX	HOTLINE_ENABLE
	SPEEDLIST_LABEL	ATA_REGION
	INTERCOM-PAGING	HOTLINE_URL
	SESSION_TIMER_DEFAULT_SE	SESSION_TIMER_ENABLE
		SESSION_TIMER_MIN_SE
	SET_REQ_REFRESHER	DWNLD_CFG_ACCEPT
	SET_RESP_REFRESHER	AUTO_PRV_SIGNING
	MAX_ALLOWEDADDRESSES	DWNLD_CFG_SIGNING

Table continues…

Configuration command type	Configuration commands	
	PORT_MIRROR_ENABLE	FTP_PASSWORD
	MEMCHECK_PERIOD	CALL_WAITING_TONE
	DOS_PACKET_RATE	MAX_APPEARANCE
	DOS_MAX_LIMIT	DISABLE_SPKRPHN
	DOS_LOCK_TIME	CALL_ORIGIN_BUSY
	LOGSIP_ENABLE	SLOW_START_2000K
	CUST_CERT_ACCEPT	USER_FILE_ENABLE
	CERT_ADMIN_UI_ENABLE	DEFAULT_ADDRESSBOOK_FILE
	SEC_POLICY_ACCEPT	DEFAULT_SPEEDDIALLIST_FILE
	SECURITY_LOG_UI_ENABLE	DEFAULT_CUSTOMKEYS_FILE
	KEY_SIZE	LOGINALPHA_ENABLE
	KEY_ALGORITHM	INTERCOM_PAGING
	TLS_CIPHER	ADHOC_ENABLED1
	SIGN_SIP_CONFIG_FILES	ADHOC_ENABLED2
	FP_PRESENTED	ADHOC_ENABLED3
	FP_ENTERED	ADHOC_ENABLED4
	SUBJ_ALT_NAME_CHECK_ENAB LE	ADHOC_ENABLED5
	CERT_EXPIRE	CONFERENCE_URI1
	SECURITY_POLICY_PARAM_CHANGE	CONFERENCE_URI2
	AUTO_PRV_ACCEPT	CONFERENCE_URI3
	AUDIO_PROFILE	CONFERENCE_URI4
	ENABLE_SERVICE_PACKAGE	CONFERENCE_URI5
	ALPHA_ORDER_LOC_LIST	SECURE _INCALL_DIGITS
	LOGOUT_WITHOUT_PASSWORD	PRIMARY_SERVER_PROFILE
	REMOTE_CHECK_FOR_UPDATE	SECONDARY_SERVER_PROFILE
	PREFER_CUSTOMIZED_RBT	RPID_PRESENCE_ENABLE
	USE_DEFAULT_DEV_CERT	PRES_SERVER_IP
	AVAYA_AURA_MODE_ENABLE	CALL_ORIGIN_BUSY
	BLIND_TRANSFER_EARLY_RELEASE	DST_START
	DST_STOP	LINE_KEY_SCROLLING
	USE_CONTACT_IN_REFERTO	

Table continues…

Configuration command type	Configuration commands	
QoS and ToS commands	DSCP_CONTROL	802.1P_MEDIA
	802.1P_CONTROL	DSCP_DATA
	DSCP_MEDIA	802.1P_DATA
Tone configuration commands	DIAL_TONE	FASTBUSY_TONE
	RINGING_TONE	CONGESTION_TONE
	BUSY_TONE	
NAT configuration commands	NAT_SIGNALLING	STUN_SERVER_IP2
	NAT_MEDIA	STUN_SERVER_PORT1
	NAT_TTL	STUN_SERVER_PORT2
	STUN_SERVER_IP1	
Voice Quality Monitoring (VQMon) configuration commands	VQMON_PUBLISH	JITTER_ENABLE
	VQMON_PUBLISH_IP	JITTER_WARN
	LISTENING_R_ENABLE	JITTER_EXCE
	LISTENING_R_WARN	DELAY_ENABLE
	LISTENING_R_EXCE	DELAY_WARN
	PACKET_LOSS_ENABLE	DELAY_EXCE
	PACKET_LOSS_WARN	SESSION_RPT_EN
	PACKET_LOSS_EXCE	SESSION_RPT_INT
System commands	ADMIN_PASSWORD	
	ADMIN_PASSWORD_EXPIRY	
	ENABLE_LOCAL_ADMIN_UI	
	HASHED_ADMIN_PASSWORD	
Audio Codecs	G729_ENABLE_ANNEXB	AUDIO_CODEC8
	G723_ENABLE_ANNEXA	AUDIO_CODEC9
	DEF_AUDIO_QUALITY	AUDIO_CODEC10
	AUDIO_CODEC1	AUDIO_CODEC11
	AUDIO_CODEC2	AUDIO_CODEC12
	AUDIO_CODEC3	AUDIO_CODEC13
	AUDIO_CODEC4	AUDIO_CODEC14
	AUDIO_CODEC5	AUDIO_CODEC15
	AUDIO_CODEC6	
	AUDIO_CODEC7	

Table continues…

Configuration command type	Configuration commands
Deskphone bugs logging/Recovery commands	RECOVERY_LEVEL LOG_LEVEL

Device configuration file command syntax

Important:

The device configuration file uses the following syntax:

- [ ] – mandatory field
- < > – optional field

For example:

```
AUDIO_CODEC [ ] [ ] < >
```

would be filled in as

```
AUDIO_CODEC1 G729 G.729 codec
```

Important:

The syntax of the commands in the device configuration file is case-sensitive. Verify that the commands follow the case defined in this document.

Important:

Parameters in the device configuration file with empty values are not allowed and cause write failure.

Important:

Some parameters are configured by the service package, which is downloaded to the IP Deskphone at log-in time. Service packages are provided by Communication Server 2000, AS 5200, and Avaya Aura® Application Server 5300 proxies only.

Server and network configuration commands

SIP_DOMAIN[x] [domain_name]

This parameter preconfigures the proxy domain name for all servers. The same configuration can be done through the domain configuration menu on the IP Deskphone.

- x – the number of the SIP domain number from 1 to 5.
- domain_name – the proxy domain name for all servers.

Note:

SIP_DOMAIN[x] is provisioned after user logout.

SERVER_IP[x]_[y]_[ip_address]	This parameter configures the primary and secondary IP address for each domain; two proxies for each domain. • x – the domain number from 1 to 5. • y – indicates whether it is the primary or secondary IP address. y=1 indicates the primary address and y=2 indicates the secondary address. • ip_address – the IP address of the SIP proxy server.
SERVER_PORT[x]_[y] [port_number]	This parameter configures the signaling ports for each proxy. • x – the domain number. • y – indicates whether it is the primary or secondary IP address. y=1 indicates the primary IP address and y=2 indicates the secondary IP address. • port_number – the SIP proxy signaling port (default is 5060).
SERVER_TCP_PORT[x]_[y] [port_number]	This parameter configures the signaling TCP ports for each proxy. • x — the domain number. • y — indicates whether it is the primary or secondary IP address. y=1 indicates the primary IP address and y=2 indicates the secondary IP address. • port_number – the SIP proxy signaling TCP port (default is 5060).
SERVER_TLS_PORT[x]_[y] [port_number]	This parameter configures the signaling TLS ports for each proxy. • x — the domain number. • y — indicates whether it is the primary or secondary IP address. y=1 indicates the primary IP address and y=2 indicates the secondary IP address.

	• port_number – the SIP proxy signaling TLS port (default is 5061).
DNS_DOMAIN [domain]	This parameter is the DNS domain of the IP Deskphone.
SIP_PING [YES | NO]	This parameter is the SIP_PING configuration value is used to maintain server heartbeat detection and to keep a firewall pinhole open in the case of UDP signaling. For TCP signaling. the OS keep alive is used for failover mode. When used for server heartbeat detection, the IP Deskphone periodically pings the SIP Proxy and awaits a response. When three attempts to ping the SIP Proxy fail, the IP Deskphone begins a failover process and attempts to connect to the next configured SIP Proxy IP in the same domain. When a NAT TRAVERSAL method is selected, the SIP_PING configuration value also helps keep a firewall pinhole open. **Important:** Decide carefully whether SIP_PING usage is appropriate for your environment. Even when SIP_PING is not used for NAT TRAVERSAL, it is highly likely that you must keep SIP_PING enabled for server heartbeat detection. If the IP Deskphone is behind a firewall, it is very likely that you must keep SIP_PING enabled, unless an alternate method of keeping the firewall pinhole open is used. The default value is YES if not specified in the device configuration file. If SIP_PING is changed in the Device configuration file, the IP Deskphone must be rebooted for the change to take effect. • YES – enables pinging • NO – disables pinging
TCP_SIP_PING_FAILBACK [YES | NO]	This parameter is used to maintain server behavior. If TCP/TLS connection to S1 is established, the phone should send a SIP PING request to S1 to determine if S1 is able to serve SIP requests. • YES – enables pinging. If S1 responds to the PING with 503 response code (or other code indicating server's inability of serving SIP requests), the phone PINGs again after a timeout, This parameter should be enabled for Avaya Aura.

	• NO (default) – disables pinging, so a phone performs the failback even if server is unable to serve SIP requests.
REG_REFRESH_INTERVAL [seconds]	This parameter allows the administrator to change the default re-registration time of the IP Deskphone. The default is 86400 seconds (or 24 hours). The minimum value is 300 and the maximum value is 86400. Note that the proxy can override this value and force the IP Deskphone to have a different refresh interval.
IPV6_ENABLE [YES] [NO]	This parameter must be applied at boot time prior to the network being enabled. The default value is NO. When this parameter is enabled, IPv4/IPv6 are supported on the IP Deskphone. When this parameter is not enabled only IPv4 is supported on the IP Deskphone. • YES – enables IPv6 functionality in a dual mode • NO – disables IPv6 functionality (default) When the protocol is changed, the IP Deskphone automatically restarts and updates the Device Settings on the IP Deskphone.
PREFER_IPV6 [YES] | NO]	This parameter allows the administrator to select the source address from the set of IPv4/IPv6 addresses. In a dual mode, by default all IP Deskphones prefer IPv4 addresses. The default value is NO. When PREFER_IPV6 is configured to YE,S the IP Deskphone selects the IPv6 address when there is a choice between IPv4 and IPv6 addresses. • YES –IPv6 address is selected. • NO –IPv4 address is selected.
IPV6_STATELESS [YES | NO]	This parameter configures stateless autoconfiguration. If IPV6_STATELESS parameter is configured to [YES], then autoconfiguration is enabled. The default value is YES. If this parameter is configured to [NO], then addresses must be configured through manual or static configuration. • YES – enables IPv6 stateless autoconfiguration (default). • NO – disables IPv6 stateless autoconfiguration.
IPV6_REDIRECT_IGNORE [YES | NO]	This parameter configures the system to ignore redirect messages sent by routers. The default value is NO. • YES – the system ignores all redirect messages. • NO – the system processes all redirect messages. This is the default.

IPV6_MCAST_ECHO_REPLY [Yes | /No]	This parameter enables or disables the sending of an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address. The default value is Yes. • Yes — the IP Deskphone responds to the Echo Request message with an Echo Reply message. This is the default. • No — the IP Deskphone ignores the Echo Request message.
REGISTER_RETRY_TIME [seconds]	This parameter configures in seconds how long the IP Deskphone waits before it attempts to reregister with the proxy server. The default value is 30 (seconds). • Minimum – 30 (seconds) • Maximum – 1800 (seconds)
REGISTER_RETRY_MAXTIME [seconds]	This parameter configures in seconds the maximum value that the IP Deskphone waits before it attempts to reregister with the proxy server. The default value is 1800 (seconds). • Minimum – 600 (seconds) • Maximum – 1800 (seconds)
SRTP_ENABLED [YES | NO]	This parameter configures SFTP configuration values. The default value is NO. • YES – enables SRTP. • NO – disables SRTP (default).
SRTP_MODE [BE-2MLines | BE-Cap Neg | SecureOnly]	This parameter configures SFTP configuration values. The default value is BE-2MLines. • BE-2MLines (default) • BE-Cap Neg • SecureOnly
SRTP_CIPHER_1 [AES_CM_128_HMAC_SHA1_80 | AES_CM_128_HMAC_SHA1_32]	This parameter configures the preferred order for SRTP cipher offers. The default value is AES_CM_128_HMAC_SHA1_80. • AES_CM_128_HMAC_SHA1_80 (default value) • AES_CM_128_HMAC_SHA1_32 • None

SRTP_CIPHER_2 [AES_CM_128_HMAC_SHA1_80 | AES_CM_128_HMAC_SHA1_32]	This parameter configures the preferred order for SRTP cipher offers. The default value is AES_CM_128_HMAC_SHA1_32. • AES_CM_128_HMAC_SHA1_32 (default value) • AES_CM_128_HMAC_SHA1_80 • None
SSH [YES | NO]	This parameter configures the SSH server on the IP Deskphone. The default value is NO. • YES – configure the SSH server • NO – do not configure the SSH server (default)
SFTP [YES | NO]	This parameter configures the SFTP server on the IP Deskphone. The default value is NO. • YES – configure the SFTP server • NO – do not configure the SFTP server (default)
SSHID [x]	This parameter configures SSH and SFTP user IDs. The maximum limit is 49 characters.
SSHPWD [x]	This parameter configures SSH and SFTP passwords. The maximum limit is 49 characters.
SFTP_READ_PATTERNS [x]	This parameter enables file extensions to read from the IP Deskphone. The default values are .cfg and .dat. The read pattern for this entry should be strictly followed. A valid example is as follows: SFTP_READ_PATTERNS .cfg,.re1,.re2,.re3,.dat **Important:** Ensure there are no spaces between the extensions. When this parameter is changed, the system resets.
SFTP_WRITE_PATTERNS [x]	This parameter enables file extensions to write from the IP Deskphone. The default values are .cfg and .dat. The write pattern for this entry should be strictly followed. A valid example is as follows: SFTP_WRITE_PATTERNS ..cfg,.txt,.wr1,.wr2 **Important:** Ensure there are no spaces between the extensions. When this parameter is changed, the system resets.

HASH_ALGORITHM [SHA1 | MD5]	This parameter provides the hash algorithm. The default value is SHA1. • SHA1 – algorithm is Secure HASH Algorithm 1 • MD5 – algorithm is Message-Digest algorithm 5
MKI_ENABLE [YES | NO]	This parameter indicates whether to use the Master Key Identifier (MKI) or not. The default value is NO. • YES – MKI is configured • NO – MKI is not configured (use NO for Avaya Aura® systems)
EAP [MD5 | TLS | PEAP | DISABLE]	This parameter allows the administrator to ensure that individual devices are authorized to access the enterprise LAN environment. The default value is DISABLE. • MD5 – MD5 encryption • TLS – TLS encryption • PEAP – PEAP encryption • DISABLE – erases existing IDs and Passwords
EAPID1 [x]	The administrator is prompted to enter the EAP ID EAPID1 when EAP-MD5, EAP-TLS, and EAP-PEAP/MD5 are selected. • minimum value – 4 characters • maximum value – 20 characters
EAPID2 [x]	The administrator is prompted to enter the EAP ID EAPID2 when EAP-PEAP is selected. If the administrator only enters the ID 1 value, the ID 2 has the same value as ID 1. • minimum value – 4 characters • maximum value –20 characters
EAPPWD [x]	The administrator is prompted to enter a password when EAP-PEAP and EAP-MD5 are selected. • minimum value – 4 characters • maximum value –12 characters
CA [IP address]	This parameter is the IP address of the Certificates Server.
CA_DOMAIN [phone name]	This parameter is the IP Deskphone phone name. • minimum value – 4 characters

	• maximum value –12 characters
HOST_NAME [hostname]	This parameter is the IP Deskphone host name. • minimum value – 4 characters • maximum value –12 characters
SIP_UDP_PORT [1024 to 65535 | 0]	This parameter configures the listening port for incoming UDP requests. The default value is 5060. • minimum value – 1024 • maximum value – 65535 • Disabled – 0
SIP_TCP_PORT [1024 to 65535 | 0]	This parameter configures the listening port for incoming TCP requests. The default value is 5060. • minimum value – 1024 • maximum value – 65535 • Disabled – 0
SIP_TLS_PORT [1024 to 65535 | 0]	This parameter configures the listening port for incoming TCP requests. The default value is 0. • minimum value – 1024 • maximum value – 65535 • Disabled – 0
CACHED_IP_ENABLED [YES | NO]	This parameter configures the cached IP address feature. The parameter defines whether the IP Deskphone uses the previous IP address information if the IP Deskphone is not able to reach the DHCP server, or if the IP Deskphone should interrupt regular work and wait for a DHCP response. The default is NO. • YES — the last IP address information is used if the DHCP server is not reached. • NO — Must receive a response from the DHCP server to assign the IP Deskphone an IP address (default). If DHCP=YES on the IP Deskphone, then the cached IP parameter can also be modified through the IP Deskphone's UI in the **Network > Diagnostics** menu.

PCPORT_ENABLE [YES | NO]	This parameter enables/disables the PC port. The default is YES. • YES — PC port is active (default). • NO — PC port is disabled.
LLDP_ENABLE [YES | NO]	This parameter enables/disables LLDP on the IP Deskphone. The default is NO. • YES – 802.1ab (LLDP) is enabled. • NO – 802.1ab (LLDP) is disabled (default).
DHCP_NUMBER_OF_RETRIES [x]	This parameter configures the number of times the IP Deskphone attempts to contact the DHCP server. The default value is 4. • minimum value is 1 • maximum value is 10 If the value defined in the System Configuration file is incorrect, the default value is used.
DHCP_INITIAL_TIMEOUT [x]	This parameter configures the initial time interval between attempts by the IP Deskphone to contact the DHCP server. The default value is 4 seconds. If the DHCP server does not respond, the IP Deskphone sends several requests one after another in different timeout intervals, based on the formula `timeout[i]=2*timeout[i-1] +- 1 second` where “i” is the number of retries and timeout[0]= DHCP_INITIAL_TIMEOUT. The maximum timeout between Discovery requests cannot be greater than 64 seconds. If the value of the next timeout becomes greater than 64 seconds, the DHCP client stops increasing the timeout interval and keeps the timeout value of 64 seconds. • minimum value is 4 seconds • maximum value is 10 seconds If the value defined in the System Configuration file is incorrect, the default value is used.
DHCP_UNTAG_ENABLED [YES | NO]	When this parameter is enabled, the IP Deskphone attempts to obtain an IP address in a VLAN (DHCP discovery frames are tagged), and the DHCP server is unreachable, then after the pre-defined number of Discovery attempts the IP Deskphone begins sending Discovery frames in non-VLAN mode. If the IP Deskphone still does not receive an Offer

	then, after a pre-defined number of Discovery attempts, the IP Deskphone reverts to VLAN tag mode again. The default is NO.
HTTP_RETRY_NUMBER [x]	This parameter configures the number of times the IP Deskphone attempts to contact the server when an HTTP 503 (server is unavailable) response is received. The IP Deskphone stops trying to connect to the server after HTTP_RETRY_NUMBER unsuccessful attempts have been made, or if any other response except HTTP 503 is received from the server. x = positive integer. The default value is 5. If HTTP_RETRY_NUMBER is not specified in the Device Configuration file, the default number of attempts is applied. If HTTP_RETRY_NUMBER is set to 0 in the Device Configuration file, the IP Deskphone performs HTTP retries continuously until it receives a response other than HTTP 503. If the HTTP_RETRY_NUMBER is configured as a negative value, the default number of attempts is applied.
FAIL_BACK_TO_PRIMARY [YES | NO]	This parameter allows you to enable/disable the Fail Back to Primary feature. • YES – enables the fail back • NO – disables the fail back (default) **Note:** Set the KEEPALIVE_RETRIES parameter to 1 to more quickly determine if the primary proxy server is unavailable and to re-register to the secondary proxy server.
SURV_SIP_SVR_ENABLE [YES | NO]	This enabled parameter lets a user know that they are in fail-over mode. • YES – enables the Avaya Survivable SIP Server. In fail-over mode, "Server Fail Over Mode" is displayed on the phone; the primary line key is flashing. • NO (default) – disables the Avaya Survivable SIP Server. In fail-over mode, "Server Fail Over Mode" is not displayed on the phone.
REGISTER_RETRY_MAXTIME [seconds]	This parameter configures in seconds the maximum length of time that the IP Deskphone waits before it attempts to re-register with the proxy server.

The default value is 1800 (seconds).

- minimum value – 600 (seconds)
- maximum value – 1800 (seconds)

KEEPALIVE_RETRIES [x]

This parameter specifies the number of times that the IP Deskphone attempts to connect to the proxy server. When the IP Deskphone determines that the proxy server does not respond (keep-alive mechanism fails), it tries to re-establish the connection the specified number of times.
Each reconnection attempt consists of several messages:

- TCP SYN messages if the connection is TCP or TLS
- SIP PING messages if the connection is UDP

The IP Deskphone logs out or registers to the secondary server if the primary proxy server does not respond during the specified number of reconnection attempts.
The default value is 3 .

- minimum value – 1
- maximum value – 10

Feature configuration commands

TOVM_SOFTKEY_ENABLE [YES | NO]

This feature enables the Transfer to Voice Mail feature and displays a soft key on the IP Deskphone. When a user has an incoming call, they can transfer the call directly to their voice mail. This is supported on the AS5200 and Avaya Aura® Application Server 5300 servers.

- YES – enables the toVM soft key on the IP Deskphone.
- NO – disables the toVM soft key on the IP Deskphone.

TOVM_VOICEMAIL_ALIAS [string]

This parameter customizes the user ID of the SIP URI of the voice mail system.

The default is transfertovm.

TOVM_VOICEMAIL_PARAM [string]

This parameter customizes the parameter name of the SIP URI of the voice mail system.

	The default is mbid.
SCA_APPEARANCES [x]	This parameter configures the maximum number of appearances used for outgoing calls by the Shared Call Appearance (SCA) group. The valid range for this parameter is 2 to 24. The default value is 12.
SCA_HOLD_BEHAVIOR [PRIVATE | PUBLIC]	This parameter configures the default behavior of the hold button when user-determined behavior does not exist. When a user creates a new profile, the default behavior is taken from this setting. After the creation of a new profile, this configuration setting is not used. The default option is PUBLIC.
SCA_LINE_SEIZE_EXPIRES [timeout]	This parameter allows the administrator to specify expiration time in seconds for line-seize subscriptions (Single Call Appearance). Allowed values are from 10 to 30 seconds. The default value is 15 seconds. — timeout - expiration time for line-seize subscriptions in seconds.
RTP_MIN_PORT [x]	The minimum RTP port value is an integer between 2048 and 65535, exclusive of the restricted SIP ports between 5059 and 5080. The default value is 16384.
RTP_MAX_PORT [x]	The maximum RTP port value is an integer between 2048 and 65535, exclusive of the restricted SIP ports between 5059 and 5080. The default value is 32764. **Note:** The RTP port configuration parameters must satisfy the constraints that (RTP_MAX_PORT - RTP_MIN_PORT) is greater than or equal to 10 and less than 1000. **Note:** If there is a provisioning error, RTP_MIN_PORT is reset to the default value of 16384 and RTP_MAX_PORT is reset to the default value of 32764. An error message is logged. The SystemConfig file

<table>
<tr><td></td><td>stores 16384 and 32764, rather than the erroneous configuration values, to indicate that the configuration attempt has been rejected.</td></tr>
<tr><td>CALL_WAITING [SPEAKER | STREAM]</td><td>• SPEAKER – the Call Waiting tone is played on the IP Deskphone speaker. This is the default option.
• STREAM – the Call Waiting tone is injected into the stream played on the transducer in use for the active call.</td></tr>
<tr><td>DISTINCTIVE_RINGING [YES | NO]</td><td>This feature works with the CS 2000 proxy.
• YES– turns on the distinctive ringing feature. This is the default option.
• NO – turns off the distinctive ringing feature.</td></tr>
<tr><td>USE_RPORT [YES | NO]</td><td>• YES – allows the IP Deskphone to work from behind and/or in front of a symmetrical NAT with servers and/or clients that support RFC3581.
• NO – disables implementation of support for RFC3581. This is the default option.</td></tr>
<tr><td>EXP_MODULE_ENABLE [YES | NO]</td><td>• YES – the IP Deskphone detects and enables an expansion module.
• NO – the IP Deskphone does not detect an expansion module. This is the default option.</td></tr>
<tr><td>MAX_RING_TIME [x]</td><td>This parameter is an integer between 30 and 600 that configures the number of seconds for incoming calls to ring before ignoring them. 0 is a special value which disables this feature. The default value is 0.</td></tr>
<tr><td>ENABLE_UPDATE [YES | NO]</td><td>• YES – enables UPDATE message support and adds “UPDATE” to the ALLOW header. This is the default option.
• NO – disables UPDATE message support.
Note:
ENABLE_UPDATE is provisioned after user logoff.</td></tr>
</table>

PROMPT_ON_LOCATION_OTHER [YES | NO]	• YES – prompt the user to select new location if location “other” was previously selected. • NO – do not prompt the user to select new location if location “other” was previously selected. This is the default option.
VMAIL [vmail_number]	This parameter is the voice mail address, which can be the URI or the DN of the voice mail server. This command takes a string as a parameter. This is the default link for a new user profile only. Individual users can customize the link through **Prefs > User Options > Voice Mail Settings**. This command has no effect on the user profiles after it is created. vmail_number is the number or URI of the voice mail server.
VMAIL_DELAY[x]	This parameter is a delay, configured in milliseconds, between when the voice mail server answers the call and the start of dialing the voice mail user ID. The default value is 1000ms. • x – the delay in milliseconds
LLDP_WAITING_TIME [timeout_sec]	This parameter allows the administrator to configure the timeout in seconds that the client should wait for the LLDP response. The allowed values of the parameter are from 30 to 300 seconds. The default value is 30 seconds. — timeout_sec – timeout value in seconds
IP_OFFICE_ENABLE [YES | NO]	This parameter is a command that specifies if IP Office-specific features are active on the IP Deskphone or not. The default value is NO. • YES – IP Office-specific features are active. • NO – IP Office-specific features are not active.
IPOFFICE_CONF_CODE [opt_string]	This parameter allows the administrator to configure the **Conf** soft key. If the parameter is configured, the IP Deskphone user is able to call the IP Office option **"Conference"**. — opt_string = code of the **Conference** option Example:

	`IPOFFICE_CONF_CODE *3` **Note:** The option is available if IP_OFFICE_ENABLE is YES. The code of the option is specified in the IP Office Administration Guide
IPOFFICE_MSG_CODE [opt_string]	This parameter allows the administrator to configure the **Msgs** soft key. If the parameter is configured, the IP Deskphone user is able to call the IP Office option **"Send Message"**. — opt_string - code of the **Send Message** option Example: `IPOFFICE_MSG_CODE *5` **Note:** The option is available if IP_OFFICE_ENABLE is YES. The code of the option is specified in the IP Office Administration Guide
IPOFFICE_REDIAL_CODE [opt_string]	This parameter allows the administrator to configure the **Redial** soft key. If the parameter is configured, the IP Deskphone user is able to call the IP Office option **"Redial"**. — opt_string - code of the **Redial** option Example: `IPOFFICE_REDIAL_CODE *6` **Note:** The option is available if IP_OFFICE_ENABLE is YES. The code of the option is specified in the IP Office Administration Guide
AUTOLOGIN_ENABLE [YES | NO | USE_AUTOLOGIN_ID] or [1 | 0 | 2]	This parameter controls whether or not the IP Deskphone attempts to automatically log on to the proxy server. • YES (or 1) – turns on the auto login feature. • NO (or 0) – turns off the auto login feature.

	• USE_AUTOLOGIN_ID (or 2) – enables the auto login id feature using the userid specified in AUTOLOGIN_ID_KEY01 and the password specified in AUTOLOGIN_PASSWD_KEY01 to register and authenticate. Both userid and password must be specified. The AUTOLOGIN_ID_KEY01 and AUTOLOGIN_PASSWD_KEY01 parameters are defined in the IP Deskphone-specific configuration file. **Note:** When USE_AUTOLOGIN_ID is used, the user is prevented from logging off the IP Deskphone. **Note:** If AUTOLOGIN_ENABLE is configured as USE_AUTOLOGIN_ID (2) in the IP Deskphone-specific configuration file, it is recommended that AUTOLOGIN_ENABLE be configured as YES (1) or NO (0) in the device configuration file. This makes it easier to reconfigure an IP Deskphone that used the IP Deskphone-specific configuration file to use only the device configuration file. Otherwise a phone may try to login with the old IP Deskphone-specific configuration file auto-login parameters.
AUTO_UPDATE [YES | NO]	This parameter is a command to enable or disable the automatic updating of the IP Deskphone with SIP Software configuration files from the provisioning server. Enabling this command causes the IP Deskphone with SIP Software to check for updates once every day. The default is NO. • YES – turns on the AUTO_UPDATE feature. • NO – turns off the AUTO_UPDATE feature. **Note:** If the IP Deskphone encounters any Major or Critical error in memory during the Auto

	update process, the IP Deskphone reboots based on the recovery level configured.
AUTO_UPDATE_TIME [x]	This parameter is the actual time in seconds, starting from midnight, before an automatic update occurs. Each IP Deskphone adds random numbers to the time specified by this command so every IP Deskphone does not try to access the provisioning server at the same time. By default the automatic update feature is disabled (see AUTO_UPDATE_TIME_RANGE). • x – the time after midnight that the automatic update occurs.
AUTO_UPDATE_TIME_RANGE [x]	This parameter is the range in hours, from the AUTO_UPDATE_TIME where an IP Deskphone checks for updates from the server. The default range is 1 hour. • x – the range in hours when the IP Deskphone checks for updates from the server. The range can be from 1 to 6 hours.
TRANSFER_TYPE [MCS |RFC3261]	This parameter is used to configure the IP Deskphone to activate Avaya conference server-assisted attended transfers, instead of the industry-standard method of attended transfers. The default setting is RFC3261. • MCS – the typical attended transfer used by Avaya proxies. MCS uses a conference server to do the attended transfer. • RFC3261 – the standard method of a transfer. This method does not involve a conference server.
BLIND_TRANSFER_EARLY_RELEASE [YES | NO]	This parameter determines whether phone allows releasing while it is in transfer state. • YES – enables the ability to switch to the idle state after the "release" keypress during the transfer state until the transfer is finished or has failed. • NO (default) – disables the ability to exit the transferring state until the transfer is finished or has failed.

REDIRECT_TYPE [MCS | RFC3261]	This parameter is a command used to select different protocols for IP Deskphone redirection. The default setting is MCS. • MCS – when the IP Deskphone receives either 301 (moved permanently) or 302 (moved temporarily) during registration, it is assumed the IP Deskphone is moved to a new system (proxy+registrar) and all subsequent messages are sent to the new address. • RFC3261 – the IP Deskphone assumes that, if during registration, a 301 (moved permanently) is received, the message contains a new registrar address. The IP Deskphone tries to register to the registrar using the existing proxy.
ENABLE_PRACK [YES | NO]	PRACK is utilized to make some SIP messages reliable and requires that an ACK be sent with many SIP messages. ENABLE_PRACK is often utilized to verify that early media is being received. See RFC3262 for details. **Note:** ENABLE_PRACK must be configured as NO when connected to the MCS 5100 Release 3.5 system. **Note:** ENABLE_PRACK is provisioned after user logoff. • YES – enables PRACK. • NO – disables PRACK and is the default value.
PROXY_CHECKING [YES | NO]	This parameter enables and disables extra security checking when incoming requests are sent to the IP Deskphone. The IP Deskphone with SIP Software always sends requests through an outgoing proxy. However, it is possible, through this configuration, to be able

	to accept an incoming request directly or through an incoming proxy. • YES – the request must come directly from the proxy server. YES is the default to enable proxy checking. • NO – the request can be sent directly to the IP Deskphone. (NO is only suitable in a few situations).
ENABLE_BT [YES | NO]	This parameter is a flag to enable and disable Bluetooth support in the IP Deskphone. • YES – enables Bluetooth. • NO – disables Bluetooth. The default is NO. **Note:** This applies to the Avaya 1100 Series IP Deskphones only.
AUDIO_CODEC[n] [codec id] <description>	This parameter is a command that specifies the codecs that are available for the user to select. You can configure up to 15 codecs. • n – the codec number. The value is 1 to 15. • codec ID – the codec identifiers are as follows: - PCMA - PCMU - G729 - G722 - G723 • text description – a text description of the codec. For more information about audio codec configuration, see Audio codecs on page 268
DEF_AUDIO_QUALITY [Low | Medium | High]	This parameter is used to configure the default audio quality by setting the preferred audio codec order. If this parameter is not present in the device configuration file, the IP Deskphone uses **High** quality as the default value. The possible parameters for this command are High, Medium, and Low. If any other parameter is entered or if these commands are misspelled,

	the IP Deskphone uses **High** as the default setting. This parameter is used only if the audio codecs are not configured in the device configuration file. The following codecs are used for each selection: • High – G711 (PCMU), G711 (PCMA), G729 • Medium – G711 (PCMA), G711 (PCMU), G729 • Low – G729, G711 (PCMA), G711 (PCMU)
AUTH_METHOD [AUTH | AUTH_INT]	This parameter is used to configure the SIP authentication method. The default is AUTH. • AUTH – only authenticates (username/ password) (default). • AUTH_INT – authentication plus integrity checking (an MD5 hash of the entity is also computed and checked).
BANNER [banner_text]	This parameter preconfigures the banner on the IP Deskphone. The banner is displayed on the IP Deskphone when the phone is idle. Use a text string to configure the banner. For example, BANNER ABC Company configures the banner to ABC Company. The text string can have a maximum of 24 characters. • banner_text – an ASCII string displayed on the screen of the IP Deskphone with SIP Software.
FORCE_BANNER [YES | NO]	This parameter is configured by the system administrator through the configuration file. If FORCE_BANNER is configured as YES, the banner from the configuration file is reloaded each time the IP Deskphone powers up, even if the user changes the banner manually. The default value is NO. • YES – causes the banner configured by the administrator to override any banner configured by the user. • NO – allows the user to configure the banner (default).

DST_ENABLED [YES | NO]	This parameter enables and disables the Daylight Saving Time (DST) mechanism. The time received from the server is GMT and is converted to the proper timezone by the IP Deskphone. If the DST feature is enabled, the IP Deskphone automatically calculates the DST time at the appropriate date and converts the time to and from DST. The calculations used are based on the new rules applicable to DST in 2007. The IP Deskphone is programmed to use the North American DST scheme. If the DST_ENABLE parameter is set to YES, but the DST_START and DST_STOP parameters are not provided, the North American DST start/stop dates are applied: 2nd Sunday of March 02:00 Local and 1st Sunday of November 01:00 Local. • YES (default) – enables DST. • NO – disables DST.
DST_START/DST_STOP [dst_settings_str]	The DST_START and DST_STOP options use the parameters shown in the following table. Parameters should be configured when DST_ENABLED is set to YES. • DST_START - parameter configures the date/time after which the DST offset is applied. • DST_STOP - parameter configures the date/time after which the DST offset is not applied. **Note:** Standard Time should be provided as a part of DST_STOP value in case if Local time option is chosen. Examples: 2SunJul2L means 2nd Sunday of July 2:00 Local time. LSatNov23U means Last Saturday of November 23:00 UTC time

Table 5: DST start and stop parameters

Char #	Value
1	Ordinal week number in month [1-4/L]; L = last week
2–4	3–letter shortcut for the weekday name (Sun, Mon, Tue, Wed, Thu, Fri, Sat)
5–7	3–letter shortcut for month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec)
8/8–9	1– or 2–digit hour (0–9 or 00–23)
9/10	Local/UTC time marker (L or U)

TIMEZONE_OFFSET [x]

This parameter is used to configure the current time zone offset from GMT in seconds. TIMEZONE_OFFSET takes a number as a parameter. For example, TIMEZONE_OFFSET -25200 configures the time zone offset to MST, which is GMT-7 (-7*3600 = -25200 seconds).

Table 6: Time zone offset

Location	Time zone offset (seconds)
(GMT-11:00) Samoa	-39600
(GMT-10:00) Hawaii	-36000
(GMT-09:00) Alaska Standard Time	-32400
(GMT-08:00) Pacific Standard Time	-28800
(GMT-07:00) Mountain Standard Time	-25200
(GMT-06:00) Central Standard Time	-21600
(GMT-05:00) Eastern Standard Time	-18000

Table continues…

Location	Time zone offset (seconds)
(GMT-04:00) Atlantic Standard Time	-14400
(GMT-03:30) Newfoundland	-12600
(GMT-03:00) Buenos Aires	-10800
(GMT-02:30) Newfoundland DST	-9000
(GMT-01:00) Azores	-3600
(GMT+00:00) Greenwich, Dublin, Lisbon, London	0
(GMT+01:00) Central European Time	3600
(GMT+02:00) Athens	7200
(GMT+03:00) Moscow	10800
(GMT+03:30) Tehran	12600
(GMT+04:00) Abu Dhabi	14400
(GMT+04:30) Khabul	16200
(GMT+05:00) Islamabad	18000
(GMT+05:30) Indian Standard Time	19800
(GMT+06:00) Sri Lanka	21600
(GMT+06:30) Myanmar	23400
(GMT+07:00) Bangkok	25200
(GMT+08:00) China Standard Time	28800
(GMT+09:00) Japan Standard Time	32400
(GMT+09:30) Australian Central Standard Time	34200
(GMT+10:00) Australian Eastern Standard Time	36000
(GMT+11:00) Micronesia	39600
(GMT+12:00) Fiji	43200
(GMT+13:00) New Zealand	46800

FORCE_TIME_ZONE [YES | NO]	This parameter allows you to force the timezone offset on each user's IP Deskphone. The default is NO. • YES – forces the IP Deskphone to use the TIMEZONE_OFFSET specified in the device configuration file. • NO – uses the value stored in the user preferences.
IM_MODE [ENCRYPTED | TEXT | SIMPLE | DISABLED]	This parameter configures the mode of Instant Messaging (IM). The default setting is ENCRYPTED. • ENCRYPTED – Instant Messages are sent encrypted • TEXT – Instant Messages are sent as text. • SIMPLE – Instant Messages are sent using SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE) protocol. • DISABLED – Instant Messaging is turned off and no Instant Messages can be sent or received. **Note:** According to the Federal Requirements: If the parameter FIPS_MODE=NO and IM_MODE=TEXT, the IM_MODE is changed to ENCRYPTED by force. If the parameter FIPS_MODE=YES, the IM_MODE is changed to TEXT by force
IM_NOTIFY [YES | NO]	This parameter is used to turn on or off the Blue LED indicator upon receipt of an Instant Message. The default value is YES. • YES – the Blue LED functions when an Instant Message is received (default). • NO – the Blue LED does not function when an Instant Message is received. **Note:** If IM_NOTIFY is disabled, the Blue LED continues to operate for other features.

DEF_DISPLAY_IM [YES | NO]	This parameter enables or disables the display of Instant Messages (IM). The default setting is NO. • YES – enables display of IMs. • NO – disables display of IMs.
SELECT_LAST_INCOMING [YES |NO]	This parameter determines which call is selected when there are multiple calls ringing (or active). The default value is NO. • YES — the selected call in the call list jumps to the most recent ringing call after it is added to the list. • NO — leaves the last selected call static as new calls come in or are dropped.
SERVICE_PACKAGE_PROTOCOL [proto_string]	This parameter specifies which protocol is to be used for obtaining the service package. The supported values are HTTP or HTTPS. The default value is HTTP.
MAX_LOGINS [x]	This parameter determines the maximum number of user accounts that can be logged in at the same time. Numbers higher than the number of line keys on the IP Deskphone are equivalent to no limit other than the line keys. A value of 1 allows a single user at a time. A value of 0 is treated the same as a value of 1 because you cannot restrict the IP Deskphone to 0 logins. The number of concurrent logins can never exceed 24, regardless of the value configured on MAX_LOGINS. The default is 24. • x — the maximum number of user accounts that can be logged in at the same time.
MAX_INBOX_ENTRIES [x]	This parameter restricts the maximum number of inbox entries and takes a number as a parameter. For example, MAX_INBOX_ENTRIES 100 limits the number of entries in the inbox to 100. The default limit is 100. • x — the maximum number of inbox entries.

MAX_OUTBOX_ENTRIES [x]	This parameter restricts the maximum number of outbox entries and takes a number as a parameter. For example, MAX_OUTBOX_ENTRIES 100 limits the number of entries in the outbox to 100. The default limit is 100. • x — the maximum number of outbox entries.
MAX_REJECTREASONS [x]	This parameter restricts the maximum number of Call Decline Reasons (**Prefs > Feature Options > Call Decline Reasons**) and takes a number as a parameter. The default limit is 20. • x — the maximum number of reject reasons.
MAX_CALLSUBJECT [x]	This parameter restricts the maximum number of call subjects (**Prefs > Feature Options > Call Subject**) and takes a number as a parameter. The default limit is 20. • x — the maximum number of call subject reasons.
MAX_PRESENCENOTE [x]	This parameter restricts the maximum number of presence notes and takes a number as a parameter. The default limit is 20. • x — the maximum number of presence notes that an IP Deskphone can receive.
USE_PUBLISH_FOR_PRESENCE [YES|NO]	This parameter specifies whether to send the PUBLISH request when changing the Presence state. • YES - send the PUBLISH request • NO - do not send the request
DEF_LANG [language]	This parameter configures the default language file. Note that the corresponding language file must be downloaded and stored in the IP Deskphone through the [LANGUAGE] section in Provisioning. If the language file is not stored in the IP Deskphone, the default language English is used. • language — the name of the language file is used by default (without the filename extension).

MAX_IM_ENTRIES [x]	This parameter configures the maximum number of Instant Message (IM) entries and takes a number as a parameter. Once the maximum number is reached, the oldest IM is deleted without any user notification. The default limit is 999. • x – the maximum number of instant messages.
MAX_ADDR_BOOK_ENTRIES [x]	This parameter configures the maximum number of entries in the Address Book. • x – the maximum number of Address Book entries. • The values are from 0 to 1000. The default value is 1000 entries.
MAX_DOWNLOAD_ADDR_BOOK_ENTRIES [x]	This parameter specifies the maximum number of Address Book entries which can be downloaded from the network in LOCAL Address Book mode. • x – the maximum number of Address Book entries. • The values are from 0 to 1000. The default value is 1000 entries.
ADDR_BOOK_MODE [NETWORK | LOCAL | BOTH]	This parameter selects the Address Book that is used to search for other users. The default setting is NETWORK. • NETWORK – downloads the user's Address Book from the network. New Address Book entries are uploaded to the network. • LOCAL – creates a user Address Book and stores it locally on the IP Deskphone. • BOTH – attempts to download a network Address Book and keep a copy on the IP Deskphone. If a network Address Book is available, the IP Deskphone functions as if NETWORK mode has been selected.
HOLD_TYPE [RFC2543 | RFC3261]	This parameter selects the protocol to hold a call. The default setting is RFC3261. • RFC2543 – standard protocol of the Internet Engineering Task Force (IETF).

	• RFC3261 – standard protocol of the IETF.
ENABLE_3WAY_CALL [YES | NO]	This parameter enables or disables local telephone-based three-way calling for three-party conferences. • YES – enables local (telephone-based) three-way calling for three-party conferences. YES is the default. • NO – disables local (telephone-based) three-way calling.
DISABLE_PRIVACY_UI [YES | NO]	This parameter disables the privacy setting in UI menus. Disabling the privacy setting in UI menus disables the user's ability to configure privacy options (incoming and outgoing Caller ID). • YES – disables the privacy setting in the UI menus. • NO – enables the privacy setting in the UI menus. NO is the default.
DISABLE_OCT_ENDDIAL [YES | NO]	This parameter configures the pound (#) key. The default setting is YES. • YES – the pound (#) key initiates dialing when pressed after a telephone number is entered. • NO – the pound (#) key functions as any other digit or character on the dial pad typically used in networks that use vertical service codes or access codes.
FORCE_OCT_ENDDIAL [YES | NO]	This parameter overrides attempts to change the function of the pound (#) key on the Graphical User Interface (GUI). The default setting is NO. • YES – overrides attempts to change the function of the pound (#) key on the GUI. • NO – does not override a change of the function of the pound (#) key on the GUI.
SNTP_ENABLE [YES | NO]	This parameter allows the IP Deskphone to obtain the time and date from an NTP server. The default is NO. The IP Deskphone updates the time once every 24 hours from the NTP server. If the

	IP Deskphone cannot contact the server, the IP Deskphone tries every 15 minutes up to a maximum of 6 attempts, and then hourly attempts are made. If SNTP_ENABLE is configured as NO, the IP Deskphone tries to retrieve the time and date from the SIP proxy server. However, not all SIP proxy servers support this method of retrieving the time and date. • YES – enables NTP. • NO – disables NTP.
SNTP_SERVER [ip_address]	This parameter is the IP address or FQDN of the NTP server that provides the time and date to the IP Deskphone. If this is not specified, the IP Deskphone does not generate any NTP requests. • ip_address – the IP address of the NTP server in either Fully Qualified Domain Name (FQDN) or non-FQDN format.
MADN_TIMER [x]	This parameter configures the MADN polling timer interval (the interval at which the IP Deskphone attempts to determine the MADN group of the logged-in user). The minimum value for the polling interval is 900 seconds (15 minutes). The default value is 1800. This applies to the CS 2000 and Broadworks proxies. • x – the time delay (in seconds) between queries to find the MADN group DN of a user. The minimum value 900.
MADN_DIALOG [YES |NO]	This parameter configures the SIP URI or the GROUP DN for the subscription to the dialog event. The default value is NO. • YES – subscribes to the dialog event using the SIP URI of the user. • NO – subscribes to the dialog event using the group of the user.
DEFAULT_CFWD_NOTIFY [YES | NO]	This parameter configures the "ring splash" which occurs when either local call forwarding or network-based call forwarding have been enabled. If this configuration value is enabled,

	the IP Deskphone plays an abbreviated ring tone to remind the user that a call has been forwarded. This configuration value only effects users when their user profile is first created, unless the FORCE_CFWD_NOTIFY flag is also used. The default setting is NO. • YES – a brief ring splash plays when a call is forwarded. • NO – the ring splash does not play.
FORCE_CFWD_NOTIFY [YES | NO]	This parameter allows the administrator to force the behavior of the DEFAULT_CFWD_NOTIFY value on all users who login to the IP Deskphone. The default setting is NO. • YES – the DEFAULT_CFWD_NOTIFY configuration value is forced into effect for the user. • NO – the configuration value is not forced into effect for the user.
DISPLAY_CALL_SNDR_IM_KEY [YES|NO]	This parameter allows the administrator to display or hide the **Call** soft key when viewing Instant Messages (IMs). The default setting is YES. • YES – the Call soft key is displayed • NO – the Call soft key is not displayed
ALPHA_ORDER_LOC_LIST [YES | NO]	This parameter allows the administrator to specify whether the Location list should be sorted or not. The default value is YES. • YES - the list should be sorted • NO - the list is displayed as is
ENABLE_SERVICE_PACKAGE [YES | NO | PPM]	This parameter toggles the subscription to the Call Server service package. When the IP Deskphone connects to a Call Server that does not recognize the service package, the subscription for the service package fails. If this happens, ad hoc conferencing is not available, even if the Call Server supports ad hoc conferencing. You can configure values for ad hoc conferencing when the service package is not retrieved. The IP Deskphone retrieves the

	service package based on a configurable Boolean value. The default value is YES. • YES – the IP Deskphone requests and downloads the service package (supported with Avaya Aura® Application Server 5300/ CS 2000) (default). • NO – the IP Deskphone does not request and download the service package. • PPM – the IP Deskphone requests Personal Profile manager (PPM) data (supported with Avaya Aura®)
CONFERENCE_URI [x] <URI>	This parameter contains the conference Uniform Resource Identifier (URI); for example CONFERENCE_URI conference@bvw.com. This is the address of the conference server when the user attempts to make a conference call. The default is conference@avaya.com. If a service package is used, then this is provided by the service package. • x – the SIP domain number from 1 to 5 • URI – the address of the conference server
ADHOC_ENABLED [x] [YES | NO]	This parameter configures support for ad hoc conferencing for the Call Server. The default value is NO. If a service package is used then this is provided by the service package. • x – the SIP domain number from 1 to 5 • YES – the Call Server supports ad hoc conferencing. • NO – the Call Serverr does not support ad hoc conferencing.
MAX_ADHOC_PORTS[x] [max_ports_number]	This parameter configures the maximum number of ad hoc conference participants that can join the conference on the IP Deskphone. • x – the SIP domain number from 1 to 5 • max_ports_number - number of participants from 0 to 4. The default value is 0.

INTERCOM_PAGING [YES | NO]	This parameter allows the IP Deskphone to belong to a paging group. When a page group call is received, a one-way speech path is created to the IP Deskphone, and the IP Deskphone automatically goes to a handsfree intercom state. This is used with the SCS proxy. The default value is NO. • YES – intercom/paging functionality is enabled. • NO – intercom/paging functionality is disabled (default).
LOGOUT_WITHOUT_PASSWORD [YES | NO]	This parameter allows the user to log off without entering their password if the administrator enables LOGOUT_WITHOUT_PASSWORD feature. If USE_AUTOLOGIN_ID is used then the user is not able to log out of the IP Deskphone. The default value is NO. • YES – enables the user to logout without a password. • NO – does not allow the user to logout without a password (default).
REMOTE_CHECK_FOR_UPDATE [YES | NO]	This parameter provides the functionality to remotely force the IP Deskphone to check for new firmware and configuration files. The proxy sends a NOTIFY with Event header set to “check-sync”. There is no subscription alive for this NOTIFY; it is treated as an out of dialog NOTIFY. The IP Deskphone sends a 200 OK for the NOTIFY to the proxy for the acceptance of the event. • YES – enables the Remote Check for Updates feature. • NO – the IP Deskphone does not act on the NOTIFY message from the proxy.
SECURE _INCALL_DIGITS [YES | NO]	This parameter shows the typed digits as asterisks when the user makes a call into the voice mail. When this feature is enabled, the most recently-pressed key is displayed but is overwritten by an asterisk (*) when the next key is pressed. The user has the option to Hide or Unhide the digits typed. The default value is NO. • YES – provides the secure digits while in call functionality. • NO – disables the secure digits while in call functionality (default).

E911_TERMINATE_ENABLE [YES | NO]	This parameter specifies whether a 911 call can be terminated by the calling party or not. The default value is NO. • YES – the caller can terminate the emergency call. • NO – the caller cannot terminate the emergency call once the call has been established.
E911_USERNAME [username]	This parameter is an emergency username used for making an emergency call that does not require login. The proxy must be configured with the same emergency username, otherwise, the emergency call fails.
E911_PROXY [proxy_name]	This parameter is a default emergency proxy. This variable must contain the value that matches the value defined by one of the following variables specified in the same config file: • SIP_DOMAIN1 • SIP_DOMAIN2 • SIP_DOMAIN3 • SIP_DOMAIN4 • SIP_DOMAIN5 If E911_PROXY does not match the value defined by these five variables, or the variable E911_PROXY is not defined, the value of SIP_DOMAIN1 is used as the emergency proxy.
E911_PASSWORD [password]	This parameter is the password for the emergency username that is used for making an emergency call that does not require login. The proxy must be configured with the same password; otherwise the emergency call fails.
E911_TXLOC [Register | Invite]	This parameter is the variable that describes location information that must be sent with the REGISTER SIP message, or with the INVITE SIP message. • REGISTER – the location is sent in both the INVITE and the REGISTER message. • INVITE – the location is sent with the INVITE only.

E911_HIDE_MESSAGE [Y | N]	This parameter configures whether or not the message “Emergency Calls Only” is displayed when no user is logged in and the IP Deskphone is taken off-hook. The default is NO, which means that the Emergency Calls Only message is not hidden; it is displayed on the IP Deskphone when no user is logged in and the IP Deskphone is taken off-hook.
KEEP_ALIVE_TYPE [type_string]	This parameter indicates if OS keep-alive on the connection is enabled. The supported values are **OS** or **CRLF** (or any string). The default value is **OS**. — type_string - the keep-alive mode value
CONN_KEEP_ALIVE [conn_keep]	This parameter configures the time in seconds to use for the keep-alive. The values are from 5 to 1800 seconds. The default value is 120 seconds. — conn_keep - keep-alive time in seconds
MENU_AUTO_BACKOUT [x]	This parameter is a menu auto back-out time preference configuration used to configure the auto back-out time on newly created profiles (not for profiles that already exist). The values, in seconds, are 0, 15, 30, 60, 120, 300, 600. The default value is 30. • x – 0, 15, 30, 60, 120, 300, and 600 For example, MENU_AUTO_BACKOUT 15. **Note:** There are some application screens that do not time out. Some menus, such as the administration menus, require the user to press the Back or Quit key to exit the screen.
AUTOCLEAR_NEWCALL_MSG [YES | NO]	This parameter configures the missed calls notification mode. YES means that the notification is cleared as soon as the inbox is entered without needing to visit all missed entries. The default value is NO. • YES – configures missed calls notification mode. • NO – does not configures missed calls notification mode (default) This configuration value only affects users when a user profile is first created. It does not affect a user profile

	which already exists. A user can modify the feature parameter by using the **Preferences** menu on the IP Deskphone and then selecting the **Feature Options > Missed Call Notification** menu item.
LOGIN_BANNER_ENABLE [YES | NO]	This parameter enables or disables the customizable login banner. If configured as enable, the flag causes the login of the primary user to display the provisioned banner text as part of the login process. The banner text file is a separate file downloaded by provisioning. The banner text file is specified much like the current dialing plan is specified (file name listed in 1xxxeSIP.cfg, under section [LOGIN_BANNER], and is downloaded when enabled or disabled. To be accepted, the file must contain at least one byte and must be no bigger than 2048 bytes. The encoding of the file must be UTF-8, or compatible with UTF-8, to ensure that all the characters are displayed properly. The default value is NO. • YES – enables the customizable banner login banner. • NO – disables the customizable banner login banner (default).
SECURE_UI_ENABLE [YES| NO]	This parameter disables access to the Phone Information details screen, and the context-sensitive soft key that invokes it. The values are YES and NO. The default value is NO. • YES – disables access to the Phone Information details screen and the context-sensitive soft key that invokes it. • NO – enables access to the Phone Information details screen and the context-sensitive soft key that invokes it.
SCRNSVR_ENABLE [YES| NO]	This parameter enables or disables the screensaver feature. If configured to N, the screensaver UI is not available to users, and the screensaver is disabled on the IP Deskphone . The default value is YES. • YES – enables the screensaver feature (default). • NO – disables the screensaver feature
SCRNSVR_UPASS_ENABLE [YES| NO]	This parameter enables or disables the ability to configure and use a less secure user-defined password for the IP Deskphone screensaver in password

	protected mode. If configured as Y, the screensaver password screen, **Prefs > Display > Screensaver > Mode > \Enable** (with password), has a configured context-sensitive soft key that allows the user to define a password for the screensaver. The default value is NO. • YES – enables the ability to configure and use a less secure user-defined password for the IP Deskphone screensaver in password protected mode. • NO – disables the ability to configure and use a less secure user-defined password for the IP Deskphone screensaver in password protected mode (default).
SCRNSVR_UNPRTCTD_ENABLE [YES| NO]	This parameter enables or disables the User Interface (UI) for configuring and using the screensaver without a password. The default value is NO. • YES – enables the UI for configuring and using the screensaver without a password. • NO – disables the UI for configuring and using the screensaver without a password (default).
SCRNSVR_TEXT [text]	This parameter configures the text displayed on the screensaver of newly created profiles when the screensaver/lock is active. Changes to this value through the **Prefs** context-sensitive soft key overwrites the value provided through provisioning. The text string can have a maximum of 24 characters. The default value is "Screensaver active".
SCRNSVR_MODE [DISABLE | PASS | NO_PASS]	This parameter configures the display screensaver mode of newly created profiles. There is no option to pre-select a password protected mode with a user-defined password. Changes to this value through the Prefs context-sensitive soft key overwrites the value provided through provisioning. The values are DISABLE, NO_PASS, and PASS. The default value is DISABLE. **Note:** The selected setting must have the corresponding feature mode enabled. For example, if this flag is configured to NO_PASS, then SCRNSVR_UNPRTCTD_ENABLE must be configured to Y for the NO_PASS mode to be configured on the new profiles.

SCRNSVR_DELAY [[minutes]	This parameter determines how long an IP Deskphone remains at the idle screen before the screensaver is evoked. This parameterconfigures the delay, in minutes, for the display screensaver of newly created profiles. Changes to this value through the Prefs context-sensitive soft key overwrites the value provided through provisioning. The values, in minutes, are 5, 10, 30, and 60. The default value is 10.
SCRNSVR_IMAGE [image]	This parameter configures the background image file for the display screensaver of newly created profiles. The image must exist in the images folder or no background image is used for the screensaver.
BG_IMAGE_ENABLE [YES| NO]	This parameter configures the background image file for the display in newly created profiles, and can completely disable the background image feature and disable the corresponding user interface. If the specified file does not exist in the images folder of the IP Deskphone, no background image is used for the display. The default value is YES. • YES – configures the background image file for the display in newly created profile (default). • NO – does not configure the background image file for the display in newly created profile.
BG_IMG_SELECT_ENABLE [YES| NO]	This parameter changes the selected background image for the display. If the flag is configured to N, the UI to change the background image is hidden from the user, locking the currently configured image as the background image on the IP Deskphone. The default value is YES. • YES – changes the selected background image for the display (default). • NO – does not change the selected background image for the display.
USE_BG_IMAGE [YES| NO]	This parameter configures the background image for the display of newly created profiles by specifying a file name available on the FFS. BG_IMAGE_ENABLE must be configured as YES in order to select a background image. • YES – configures the background image for the display of newly created profiles.

	• NO – does not configure the background image for the display of newly created profiles. **Note:** Image files for the IP Deskphone must include the PNG format.
SPEEDLIST_KEY_INDEX [x]	This parameter specifies the programmable key used for displaying the Speed Dial List. If the specified index does not exist on the IP Deskphone, or is invalid, the speed dial list is not displayed on the IP Deskphone. The IP Deskphone retrieves the device configuration through provisioning. If the SPEEDLIST_KEY_INDEX flag is configured to a valid programmable key that can be used for the feature, for example, >1 and less than or equal to available number of programmable keys, the IP Deskphone verifies if it has previously loaded a "Speed Dial List" file (a file containing the contents of the speed dial list). This file is similar to the dialing plan file. It needs to be properly configured and uploaded to the IP Deskphone through provisioning. The IP Deskphone parses the file, and configures the feature key specified by SPEEDLIST_KEY_INDEX to hold the Speed Dial List. If the key defined for use by the Speed Dial List is already in use, the key is overwritten and the key is assigned speed dial list functionality. The Speed Dial List feature key then uses the label that is provisioned in SPEEDLIST_LABEL which cannot be modified by the end user. • x – label
SPEEDLIST_LABEL [label]	This parameter is a feature key label used by the speed dial list feature key. The default value is SDL.
MAX_APPEARANCE [x]	This parameter defines the maximum number of possible active calls on the IP Deskphone. The values are 1 to 12. . The default value is 10. x – the maximum number of possible active calls
MAX_BLFCALLS [x]	This parameter defines the maximum number of available Busy Lamp Field (BLF) calls on the IP Deskphone. The values are 1 to 10. The default value is 10. x – the maximum number of available Busy Lamp Field (BLF) calls

	The MAX_BLFCALLS parameter value cannot be greater than the MAX_APPEARANCE parameter value. If the value of the MAX_BLFCALLS parameter is greater than the value of the MAX_APPEARANCE parameter, the value of the MAX_BLFCALLS parameter is reduced by force and takes the value of the MAX_APPEARANCE parameter (MAX_BLFCALLS = MAX_APPEARANCE).
BLF_ENABLE [YES | NO | SCS | SIPX]	This parameter enables or disables the Busy Lamp Field (BLF) feature support. If configured as Y, the flag BLF_RESOURCE_LIST_URI is not ignored and the BLF feature is used. The values are Y, N, SCS, and SIPX. The default is N. When BLF_ENABLE has the SCS or SIPX value, the BLF_RESOURCE_LIST_URI parameter is ignored and the IP Deskphone autogenerates an URI of the following format: `~~rl~C~<username>@<domain>`
BLF_RESOURCE_LIST_URI [blf uri]	This parameter configures the Busy Lamp Field (BLF) resource list URI for the BLF feature. You must use the URI provided by the proxy when properly configuring the user for BLF. The `[blfuri]` is the server provided URI to subscribe for BLF notifications, for example, `blf-resource-list@as.avaya.com`
FM_PROFILES_ENABLE [YES | NO]	This parameter allows the user to perform actions on User Profiles using the file manager. The default value is YES. • YES – allows the user to perform actions on User Profiles using the file manager (default). - . • NO – does not allow the user to delete or copy User Profiles on the IP Deskphone or USB drive using the file manager
FM_LANGS_ENABLE	This parameter allows the user to perform actions on Languages files using the file manager. The default value is YES. • YES – allows the user to perform actions on Language files using the file manager (default). - . • NO – does not allow the user to delete or copy Language files on the IP Deskphone or USB drive using the file manager

FM_SOUNDS_ENABLE [YES | NO]	This parameter allows the user to act on WAV files using the file manager. If the value is configured as NO, the IP Deskphone cannot perform any actions on WAV files, such as deleting or copying a WAV file, through the file manager. If the user selects a WAV file on the IP Deskphone or on a USB drive and presses the Delete or Send context-sensitive soft key, an error message appears. If the value is configured as YES, the user can delete or copy WAV files with the file manager interface (this applies to WAV files on the IP Deskphone and a USB drive). The default value is YES. • YES – allows the user to delete or copy WAV files on the IP Deskphone or USB drive through the file manager (default). • NO – does not allow the user to delete of copy WAV files on the IP Deskphone or USB drive through the file manager.
FM_IMAGES_ENABLE [YES | NO]	This parameter allows the user to act on JPG and PNG files using the file manager. The default value is YES. • YES – can act on JPG and PNG files using the file manager (default). • NO – does not allow the user to delete of copy JPG and PNG files on the IP Deskphone or USB drive through the file manager.
FM_CERTS_ENABLE [YES | NO]	This parameter allows the user to act on CER and PEM files using the file manager. The default value is NO. • YES – can act on JPG and PNG files using the file manager. • NO – does not allow the user to delete of copy JPG and PNG files on the IP Deskphone or USB drive through the file manager (default).
FM_CONFIG_ENABLE [YES | NO]	This parameter allows the user to act on CFG files using the file manager. The default value is NO. • YES – can act on CFG files using the file manager. • NO – does not allow the user to delete of copy CFG files on the IP Deskphone or USB drive through the file manager (default).

FM_LOGS_ENABLE [YES | NO]

This parameter allows the user to act on CFG files using the file manager. The default value is YES.

- YES – can act on CFG files using the file manager (default).
- NO – does not allow the user to delete of copy CFG files on the IP Deskphone or USB drive through the file manager (default).

ENABLE_USB_PORT [YES | NO]

This parameter enables or disables the USB port. If configured as NO, all USB devices are disabled and all other USB commands are ignored. The default value is NO.

- YES – enables the USB port
- NO – disables the USB port (default).

Note:

If the default value is acceptable, the ENABLE_USB_PORT configuration command is not required to be in the device configuration file. If change is required, the ENABLE_USB_PORT configuration command must be placed in the device configuration file with the new value.

USB_MOUSE [YES | NO[

This parameter enables or disables the USB mouse. The dafault is NO.

- YES – enables the USB mouse
- NO – disables the USB mouse (default).

Note:

If the default value is acceptable, the USB_MOUSE configuration command is not required to be in the device configuration file. If change is required, the USB_MOUSE configuration command must be placed in the device configuration file with the new value.

USB_KEYBOARD [YES | NO[

This parameter enables or disables the USB keyboard. The default value is NO.

- YES – enables the USB keyboard
- NO – disables the USB keyboard (default).

	Note: If the default value is acceptable, the USB_KEYBOARD configuration command is not required to be in the device configuration file. If change is required, the USB_KEYBOARD configuration command must be placed in the device configuration file with the new value.
USB_HEADSET [YES | NO[	This parameter enables or disables the USB headset. The default value is NO. • YES – enables the USB headset • NO – disables the USB headset (default). **Note:** If the default value is acceptable, the USB_HEADSET configuration command is not required to be in the device configuration file. If change is required, the USB_HEADSET configuration command must be placed in the device configuration file with the new value. Avaya recommends that you use the following headset types: • GNNetcom GN9350e • Plantronics CS-50
USB_MEMORY_STICK [YES | NO[	This parameter enables or disables the USB flash drive. The default value is NO. • YES – enables the USB flash drive • NO – disables the USB flash drive (default). **Note:** If the default value is acceptable, the USB_MEMORY_STICK configuration command is not required to be in the device configuration file. If change is required, the USB_MEMORY_STICK configuration command must be placed in the device configuration file with the new value.
ATA_REGION [reg_string]	This parameter specifies the region for an ATA USB-device. The supported values are: • NA

	• EU1 • EU2 • AusNZ The default value is NA.
HOTLINE_ENABLE [YES | NO]	This parameter indicates if Hotline Service is enabled or disabled. The default value is NO. • YES – enables Hotline Service • NO – disables Hotline Service (default). **Note:** If a service package is enabled then this value is overridden by the value in the service package.
HOTLINE_URL	This parameter is used as To field of INVITE message by the SIP IP Deskphone to notify the Proxy Server that this is a call from a Hotline Phone. The HOTLINE_URL is not a real URL of the Hotline target. The IP Deskphone has no idea about the Hotline target. The Proxy server replaces the To field of INVITE request message with a real Hotline target when it receives an INVITE request from the Hotline Phone. The default value is Hotline.
SESSION_TIMER_ENABLE [YES | NO]	This parameter indicates if the session timer service is enabled or disabled. The default value is YES. • YES – the Session Timer Service for the IP Deskphone is enabled, and the behavior of the IP Deskphone complies with RFC4028. • NO – the Session Timer Service is disabled.
SESSION_TIMER_DEFAULT_SE [seconds]	This parameter indicates the default session expiration in seconds. The Session-Expires header, in a request, informs the terminating endpoint and proxies of the Session-Expires interval value that the originating endpoint requires for the session timer duration, in units of delta seconds. The default value is 1800.
SESSION_TIMER_MIN_SE [seconds]	This parameter indicates the minimum session expiration in seconds. The default value is 1800.

SET_REQ_REFRESHER [x]	This parameter indicates what refresher value is configured in the initial session request. The values are 0, 1, and 2. The default value is 0. • 0 – indicates that the refresher is omitted • 1– indicates that the refresher is configured to UAC • 2– indicates that the refresher is configured to UAS
SET_RESP_REFRESHER [x]	This parameter indicates what refresher value is configured in the 200 OK response. The values are 0, 1, and 2. The default value is 2. • 0– indicates that the refresher is omitted (only valid when SET_REQ_REFRESHER is not equal to 0) • 1– indicates that the refresher is configured to UAS • 2– indicates that the refresher is configured to UAC
PORT_MIRROR_ENABLE [YES| NO]	This parameter enables or disables the Port Mirroring feature. The default value is NO. • YES – the Port Mirroring prompt in the Advanced Diag Tools dialog is enabled and can be turned on or off. **Note:** If enabled, the Port Mirroring setting survives a reboot of the IP Deskhone, but not a power off. If the IP Deskphone is powered off, Port Mirroring becomes disabled. • NO – the Port Mirroring prompt in the Advanced Diag Tools dialog is permanently disabled (dimmed) and cannot be modified.
MEMCHECK_PERIOD [seconds]	This parameter determines the time period in seconds when the Memory monitor wakes up (after re-start or the last memory check attempt). The values are 1800 (0.5 hrs) to 86400 (24 hrs). The default value is 86400 (24 hrs).
DOS_PACKET_RATE [pps]	This parameter determines the maximum number of packets per second that is allowed.
DOS_MAX_LIMIT [pps]	This parameter specifies how many packets past the DOS_PACKET_RATE the IP Deskphone can receive before packets are dropped. If packets are received at a rate of DOS_PACKET_RATE +1, then packets are

	dropped after the time specified in DOS_MAX_LIMIT (in seconds).
DOS_LOCK_TIME [seconds]	This parameter specifies the amount of time (in seconds) that the IP Deskphone stops processing packets after DOS_MAX_LIMIT is reached. If DOS_PACKET_RATE is < 1, other values are ignored and packets are not dropped.
LOGSIP_ENABLE [YES | NO]	This parameter enables or disable SIP-logging. The default value is NO. • YES – the SIP-logging Manager is active and starts to log SIP incoming and outgoing packages into the log file in FFS. • NO – the SIP-logging Manager is not active and cannot log SIP incoming and outgoing packages into the log file in FFS.
USER_FILE_ENABLE [YES |NO]	This parameter is used to determine if the user.cfg file is downloaded when the user logs on and when they check for updates. The default is NO. • YES – the user.cfg file is downloaded when the user logs on and when they check for updates. • NO – the user.cfg file is not downloaded (default). For more information, see Roaming profiles on page 194.
USER_FILE_PATH /<path>	This parameter defines the location of the configuration file for each user which contains the path to custom keys file.
DEFAULT_ADDRESSBOOK_FILE [filename]	This parameter is the default filename used when downloading the provisioning files. Default names are overwritten by names specified in the user.cfg file. For more information, see Roaming profiles on page 194.
DEFAULT_SPEEDDIALLIST_FILE [filename]	This parameter is the default filename used when downloading the provisioning files. Default names are overwritten by names specified in the user.cfg file. For more information, see Roaming profiles on page 194.
DEFAULT_CUSTOMKEYS_FILE [filename]	This parameter is the default filename used when downloading the provisioning files. Default names are overwritten by names specified in the user.cfg file. For more information, see Roaming profiles on page 194.

TECH_SUPPORT_LABEL [label_string]	This parameter configures the label used for the Support soft key on the licensing screen. The user can call the Technical Support service by pressing this soft key. The default value of the label is "Support". — label_string - label characters. Maximum length of the string is 6 alpha-numerics characters. **Note:** The label appears if the TECH_SUPPORT_ADDRESS parameter is defined.
TECH_SUPPORT_ADDRESS [addr_string]	This parameter configures the URI of the Technical.Support service. If the IP Deskphone licensing verification fails, then special dialog appears where the IP Deskphone user can press the **Support** soft key to call to the Technical Support service (see the preceding command TECH_SUPPORT_LABEL). The default value is **notset@invalid.invalid**.
DOD_ENABLE [YES | NO]	This parameter identifies whether it is a DoD ARTS network. The default value is NO. • YES – Call Forwarding Reminder service subscribes to its own dialog event. • NO – Call Forwarding Reminder service subscribes to network-redirection-reminder event package.
MLPP_NETWORK_DOMAIN [xx]	This parameter is the network domain of the user to be added to the INVITE message of outgoing calls. It can specify any MLPP Network Domain Name. The default value is DSN.
MLPP_PRECEDENCE_DOMAIN [x]	This parameter is the local precedence domain of the user to be added to the INVITE message of outgoing calls. The default value is 000000.
CALL_WAITING_TONE [0|1]	This parameter configures the call waiting tone. The default value is 0. • 0 – single buzz tone (default). • 1 – two-beep periodic tone.

DISABLE_SPKRPHN [YES | NO]	This parameter disables the speakerphone for all non-911 calls. This is intended for DoD. The default value is NO. • YES– disables the speakerphone. • NO – enables the speakerphone .
CALL_ORIGIN_BUSY [YES |NO]	This parameter determines if the user is presented with an incoming call when entering the address of an outbound call. This is intended for DoD. The default value is NO. • YES– user is not presented with an incoming call . • NO – user is presented with an incoming call (default).
FAST_EARLY_MEDIA_ENABLE [YES|NO]	This parameter allows the administrator to activate and deactivate the Fast Early Media option (according to RFC 3264). The default value is NO. • YES - activate the Fast Early Media option. When set to YES, SRTP is not supported. • NO - deactivate the Fast Early Media option
SLOW_START_200OK [YES |NO]	This parameter determines if the session description is always sent in the 200 OK message in response to an incoming call with SDP. The default value is NO. • YES – local administration UI is configured. • NO – local administration UI is not configured (default).
ENABLE_LOCAL_ADMIN_UI [YES | NO]	This parameter configures the availability of the local administration User Interface (UI) on the IP Deskphone. The default value is YES. • YES – local administration UI is configured (default). • NO – local administration UI is not configured.
LOGINALPHA_ENABLE [YES | NO]	This parameter allows the system administrator to configure the initial login and logout of the IP Deskphone to be in either alphanumeric mode or numeric mode. The default is NO. • YES – initial login and logout is alphanumeric. • NO – initial login and logout is numeric (default).

FIPS_MODE [YES | NO]	FIPS mode is used in a Federal environment. This parameter verifies that the IP Deskphone is in Federal Information Processing Standards (FIPS) certified mode. **Note:** The FIPS mode parameter has an intereaction with the IM_MODE parameter. Refer to the IM_MODE parameter for more information.
ENABLE_ANSWER_MODE [YES | NO]	This parameter allows the administrator to specify if Answer-Mode is supported when registering with the proxy. The default value is NO. • YES - the Answer-Mode is allowed. The IP Deskphone adds the "answermode" tag to the Support header in the REGISTER request. • NO - the Answer-Mode is not supported (default).
ANSWER_MODE_MAXALLOWADDR [max_addr]	This parameter specifies the maximum number of addresses that can be white-listed for Answer-Mode support. The allowed values are from 0 to 200. The default value is 100. — max_addr - maximum number of addresses
ANSWER_MODE_MICMUTE [YES | NO]	This parameter specifies if the microphone is muted when a call is auto-answered by the Answer-Mode functionality. • YES - mute the microphone • NO - do not mute the microphone (default value)
PRIMARY_SERVER_PROFILE [FILENAME]	This parameter is the set of Server Profile configuration parameters to be applied for the Primary (S1) SIP server. - filename — is the name of the Server Profile file to be applied for the Primary server; for example, profile01.dat
SECONDARY_SERVER_PROFILE [FILENAME]	This parameter is the set of Server Profile configuration parameters to be applied for the Secondary (S2) SIP server. - filename — is the name of the Server Profile file to be applied for the Secondary server; for example, profile02.dat

AUDIO_PROFILE <rating id>	This parameter applies an audio tuning parameter for the 1165E IP Deskphone. The rating id values are: • DEFAULT — TIA audio tuning parameters are applied (default value) • S004 — S004 standard (Australia and New Zealand) audio tuning parameters are applied
PREFER_CUSTOMIZED_RBT [YES | NO]	This parameter configures the opportunity to not stop the customized ringback tone when a 180 Ringing message is received. • YES – after receiving a 180 Ringing message without SDP body, the media stream is not closed and the customized ringback tone continues to play. • NO – after receiving a 180 Ringing message without SDP body, the media stream is closed and local ringback tone is generated (default).
RPID_PRESENCE_ENABLE [YES | NO]	This parameter configures RPID-based presence with Avaya Presence Services. RPID is required for Avaya Presence Services. The defailt is NO. • YES — if Avaya Presence Services with Avaya Aura Session Manager/Communication Manager are used . • NO — if Avaya Presence Services with Avaya Aura Session Manager/Communication Manager are not used (default).
PRES_SERVER_IP <IP address of Presence Server>	This parameter is the IP address of Avaya Presence Server. It is required if Avaya Presence Services are used. Default value is <empty>.
USE_DEFAULT_DEV_CERT [YES | NO]	This parameter controls the use of the default device certificate for HTTPS/TLS connections to Avaya Aura®. The default value is NO. It can be configured through the device configuration file. • YES – Use the default device certificate if no customer device certificate is installed. • NO – Do not use the default device certificate.
AVAYA_AURA_MODE_ENABLE [YES | NO]	This parameter is a command that specifies if Avaya Aura®-specific features are active on the IP Deskphone

	or not. The default value is NO. It can be configured through the device configuration file and through server profiles. • YES – Avaya Aura®-specific features are active. • NO – Avaya Aura®-specific features are not active.
LINE_KEY_SCROLLING [YES | NO]	This parameter defines whether scrolling for long line key labels is enabled. The default value is NO. • YES – scroll long line key labels • NO – do not scroll long line key labels
USE_CONTACT_IN_REFERTO [YES | NO]	This parameter defines which transfer target address should be used in Refer-To header of REFER SIP request on attended transfer. The default value is YES. • YES – use Contact URI of the transfer target in Refer-To header of REFER SIP request • NO – use To URI of the transfer target in Refer-To header of REFER SIP request

QoS and ToS commands

AVAYA_AUTOMATIC_QoS [YES | NO]	This parameter provides a better treatment for signaling and media packets after you deploy the IP Deskphones with the Avaya switches. All the devices use private Differentiated Services Code Point (DSCP) values to give better treatment to the traffic coming from peer Avaya devices. • YES — the IP Deskphone uses private DSCP values, unless overridden. • NO — the IP Deskphone uses either one of the configured DSCP values or the system default values.
DSCP_CONTROL [x]	This parameter uses a value entered in decimal format between -1 and 63. If the value is -1, the DSCP value is picked up by the Service Package. The default value is 40. • x — a value from -1 to 63 indicating the DSCP value.
802.1P_CONTROL [x]	This parameter uses a value entered in decimal format between -1 and 7 representing the 802.1P value in the SIP signaling

	packets. If the value is -1, the 802.1P value is retrieved from the Service Package. The default value is 6. • x — the value from -1 to 7 indicating the 802.1P value.
DSCP_MEDIA [x]	This parameter uses a value entered in decimal format between -1 and 63 representing the DSCP value in the Real-time Transfer Protocol packets. If the value is -1, the DSCP value is retrieved from the Service Package. The default value is 44. • x — a value from -1 to 63 indicating the DSCP value.
802.1P_MEDIA [x]	This parameter uses a value entered in decimal format between -1 and 7 representing the 802.1P value in the IP Deskphone Media (RTP) packets. If the value is -1 then the 802.1P value is retrieved from the Service Package is the 802.1 setting for media Real-time Transport Protocol (RTP). The default value is -1. • x —a value from -1 to 7 indicating the 802.1P value.
DSCP_DATA [x]	This parameter uses a value entered in decimal format between -1 and 63 representing the DSCP value in the provisioning packets. If the value is -1, the DSCP value is retrieved from the Service Package. The default value is 40. • x —a value from -1 to 63 indicating the DSCP value.
802.1P_DATA [x]	This parameter uses a value entered in decimal format between -1 and 7 representing the 802.1P value in the provisioning packets. If the value is -1, the 802.1P value is retrieved from the Service Package. The default value is 6. • x —a value from -1 to 7 indicating the 802.1P value.
DSCP_MEDIA_FLASHOVERRIDE [x]	This parameter uses a value entered in decimal format between -1 and 63 representing the DSCP value in the provisioning packets for flash override precedence and priority level voice call. If the value is -1, the DSCP value is retrieved from the Service Package. The default value is 41. • x — a value from -1 to 63 indicating the DSCP value.
DSCP_MEDIA_FLASH [x]	This parameter uses a value entered in decimal format between -1 and 63 representing the DSCP value in the provisioning packets for flash precedence and priority level

	voice call. If the value is -1, the DSCP value is retrieved from the Service Package. The default value is 42. • x — a value from -1 to 63 indicating the DSCP value.
DSCP_MEDIA_IMMEDIATE [x]	This parameter uses a value entered in decimal format between -1 and 63 representing the DSCP value in the provisioning packets for immediate precedence and priority level voice call. If the value is -1, the DSCP value is retrieved from the Service Package. The default value is 44. • x — a value from -1 to 63 indicating the DSCP value.
DSCP_MEDIA_PRIORITY [x]	This parameter uses a value entered in decimal format between -1 and 63 representing the DSCP value in the provisioning packets for priority precedence and priority level voice call. If the value is -1, the DSCP value is retrieved from the Service Package. The default value is 45. • x — a value from -1 to 63 indicating the DSCP value.
DSCP_OAM [x]	This parameter uses a value entered in decimal format between -1 and 63 representing the DSCP value in the provisioning packets for OA&M precedence and priority level voice call. If the value is -1, the DSCP value is retrieved from the Service Package. The default value is 18. • x — a value from -1 to 63 indicating the DSCP value.

Tone configuration commands

DIAL_TONE [frequency1 | frequency2 | on_time | off_time]	This parameter selects the tone advising the caller that the exchange is ready to receive call information and invites the user to start sending call information. You can select the country-specific tone. The default tone is the North American tone. • frequency1 – the frequency of tone 1. • frequency2 – the frequency of tone 2. • on_time – the duration of the tone when it is on. A -1 indicates a continuous tone. • off_time – the duration when no tone is played. For example, 350,440;-1 (350 and 440 Hz continuous tone).

RINGING_TONE [frequency1 | frequency2 | on_time | off_time]	This parameter selects the tone advising the caller that a connection is made and a calling signal is applied to a telephone number or service point. You can select the country-specific tone. The default tone is the North American tone. • frequency1 – the frequency of tone 1. • frequency2 – the frequency of tone 2. • on_time – the duration of the tone when it is on. A -1 indicates a continuous tone. • off_time – the duration when no tone is played. For example, 440,480; 2000,4000 (440 and 480 Hz with 2 seconds on, 4 seconds off)
BUSY_TONE [frequency1 | frequency2 | on_time | off_time]	This parameter selects the tone advising the caller that the telephone number is busy. You can select the country-specific tone. The default tone is the North American tone. • frequency1 – the frequency of tone 1. • frequency2 – the frequency of tone 2. • on_time – the duration of the tone when it is on. A -1 indicates a continuous tone. • off_time – the duration when no tone is played.
FASTBUSY_TONE [frequency1 | frequency2 | on_time | off_time]	This parameter selects the tone advising the caller that the telephone number is busy. It is fast in cadence or frequency. You can select the country-specific tone. The default tone is the North American tone. • frequency1 – the frequency of tone 1. • frequency2 – the frequency of tone 2. • on_time – the duration of the tone when it is on. A -1 indicates a continuous tone. • off_time – the duration when no tone is played.
CONGESTION_TONE [frequency1 | frequency2 | on_time | off_time]	This parameter selects the tone advising the caller that the groups of lines or switching equipment necessary for setting up the required call, or for the use of a specific service, are temporarily engaged. You can select the country-specific tone. The default tone is the North American tone. • frequency1 – the frequency of tone 1. • frequency2 – the frequency of tone 2.

- on_time – the duration of the tone when it is on. A -1 indicates a continuous tone.
- off_time – the duration when no tone is played.

The IP Deskphone supports using WAV files to replace the ringtone Frequency/Cadence pattern. For a system-wide setting, the country default values can be used.

NAT configuration commands

NAT_SIGNALLING [NONE | SIP_PING | STUN]

This parameter indicates the type of protocol used for NAT traversal in the signaling port. The IP Deskphone with SIP Software supports two methods of NAT traversal of the signaling path: SIP_PING and STUN.

- NONE – if the value is not configured as None, this parameter overrides the value of the parameter SIP_PING in the device configuration file.
- SIP_PING – an Avaya proprietary NAT traversal protocol. Note that SIP_PING only supports NAT traversal in the signaling port.
- STUN – the most common NAT traversal method.

NAT_MEDIA [NONE | STUN]

This parameter indicates the type of protocol used for NAT traversal in the media ports. The default is NONE.

- NONE – is the default and disables NAT_MEDIA.
- STUN – the most common NAT traversal protocol for the media (RTP and Real-time Control Protocol [RTCP]) port.
- x – is the binding lifetime in seconds.

Important:

NAT_TTL [x] is used for future development. Currently, the default value is 2 minutes (120 seconds) and IP Deskphones do not process or use the value defined in NAT_TTL [x]. The IP Deskphones always ping the ports at regular intervals of 60 seconds regardless of the NAT_TTL value.

STUN_SERVER_IP1[ip_address]	NAT traversal using STUN protocol requires a STUN server in the public internet. Two STUN server IP addresses can be provisioned. • ip_address – is the IP address of STUN server 1.
STUN_SERVER_IP2[ip_address]	NAT traversal using STUN protocol requires a STUN server in the public internet. Two STUN server IP addresses can be provisioned. • ip_address – is the IP address of STUN server 2.
STUN_SERVER_PORT1[port_number]	This parameter is the port number used corresponding to STUN_SERVER_IP1. The default port number is 3478. • port_number– is the port number.
STUN_SERVER_PORT2[port_number]	This parameter is the port number used corresponding to STUN_SERVER_IP2. The default port number is 3478. • port_number– is the port number.

VQMon configuration commands

Important:

Ensure you read How VQMon works on page 166 before configuring the VQMON parameters.

VQMON_PUBLISH [YES | NO]	This parameter enables or disables the publish message containing the voice quality monitoring metrics sent to the Proactive Voice Quality Monitoring (PVQMoN) collecting server. The default value is NO. • YES – enables VQMoN publish message. • NO – disables VQMoN publish message.
VQMON_PUBLISH_IP [xxx.xxx.xxx.xxx]	This parameter configures the IP address of the PVQMoN server that collects voice quality monitoring metrics from the publish message. This IP address is used only within the report.
LISTENING_R_ENABLE [YES | NO]	This parameter enables or disables the alerts based on the Listening R Minor and Major Thresholds. The default value is vocoder-dependent, using a scale from 1 (lowest quality) to 100

(highest quality). Currently, default values are used based on VOCODER on a per-call basis as summarized below.

- YES – enables the sending of the alert report based on the Listening R Value.
- NO – disables the sending of the alert report based on the Listening R Value.

VOCODER_G711_ULAW VOCODER_G711_ULAWPLP	LISTENING_R_WARN = 80 LISTENING_R_EXCE = 70
VOCODER_G723 VOCODER_FLAG_G723_RATE_53 VOCODER_FLAG_G723_RATE_63	LISTENING_R_WARN = 60 LISTENING_R_EXCE = 50
VOCODER_G729 VOCODER_G722 VOCODER_PCM16 VOCODER_PCM8 vqmonVocoderTypeUnknown	LISTENING_R_WARN = 70 (default if not configured and unknown type) LISTENING_R_EXCE = 60

LISTENING_R_WARN [xx]

This parameter is the threshold to send a report on Listening R less than [xx]. The default value is 70. Using a value of **0** resets it to the defaul,t based on the far-end VOCODER.

- xx – is an INTEGER value used as the threshold.

LISTENING_R_EXCE [xx]

This parameter is the threshold to send a report on Listening R less than [xx]. The default value is 60. Using a value of **0** resets it to the default, based on the far-end VOCODER.

- xx – is an INTEGER value used as the threshold.

PACKET_LOSS_ENABLE [YES | NO]

This parameter is used to enable or disable the alerts based on the packet loss thresholds. Packet loss is the fraction of RTP data packets from the source lost since the beginning of reception. The value is an integer scaled by 256. The range is 1 to 25600.

- YES – enables the sending of alert report based on the packet loss.
- NO – disables the sending of alert report based on the packet loss.

PACKET_LOSS_WARN [xx]	This parameter is the threshold to send a report on Packet Loss greater than [xx]. The default is 256 (1%). Using a value of **0** resets the threshold to the default value. • xx – is an INTEGER value scaled by 256 that is used as the threshold. The range is 1 to 25600.
PACKET_LOSS_EXCE [xx]	This parameter is the threshold to send a report on Packet Loss greater than [xx]. The default is 1280 (5%). Using a value of **0** resets the threshold to the default value. • xx – is an INTEGER value scaled by 256 that is used as the threshold. The range is 1 to 25600.
JITTER_ENABLE [YES | NO]	This parameter enables or disables alerts based on the inter-arrival Jitter on incoming RTP packets inter-arrival time. The value is represented in 1/65536 of a second. • YES – enables the sending of an alert report based on jitter detection • NO – disables the sending of an alert report based on jitter detection
JITTER_WARN [xx]	This parameter is the threshold to send a report on Inter-arrival Jitter greater than [xx]. 1 second is broken up into 65535 (0xffff hex) parts. [xx] / 65535 is the threshold in seconds. The default is 3276 (50 ms). Using a value of **0** resets the threshold to the default value. • xx – is an INTEGER value used as threshold
JITTER_EXCE [xx]	This parameter is the threshold to send a report on Inter-arrival Jitter greater than [xx]. 1 second is broken up into 65535 (0xffff hex) parts. [xx] / 65535 is the threshold in seconds. The default is 32760 (500 ms). Using a value of **0** resets the threshold to the default value. • xx – is an INTEGER value used as threshold
DELAY_ENABLE [YES | NO]	This parameter enables or disables the alerts based on the excessive delay detection. This is the one-way delay (including system delay) for the call, measured in milliseconds. • YES – enables Excessive delay detection. • NO – disables Excessive delay detection.

DELAY_WARN [xx]

This parameter is the threshold to give warning on Excessive Delay greater than [xx]. The default is 150 ms. Using a value of **0** resets the threshold to the default value.

- xx – is an INTEGER value used as a threshold measured in 1/1000 of a second.

DELAY_EXCE [xx]

This parameter is the threshold to report unacceptable Excessive Delay greater than [xx]. The default is 175 ms. Using a value of **0** resets the threshold to the default value.

- xx – is an INTEGER value used as a threshold measured in 1/1000 of a second.

SESSION_RPT_EN [YES | NO]

This parameter enables or disables periodic VQMon session reports. The default is disabled (NO).
Both session report enable (SESSION_RPT_EN) and session report interval (SESSION_RPT_INT) must be configured if the IP Deskphone software has been upgraded to SIP Release 3.0 or later. Otherwise, the SESSION_RPT_INT default of 60 seconds is used automatically. The default value is NO.

- YES – enables periodic VQMon session reports.
- NO – disables periodic VQMon session reports.

SESSION_RPT_INT [xx]

This parameter specifies the interval for the periodic VQMon session report in seconds. The minimum acceptable value is 60 seconds. The maximum acceptable value is 600 seconds. The default is 60 seconds.

- xx – is an INTEGER value in seconds.

System commands

ADMIN_PASSWORD [password]

This parameter changes the default administrator password of the IP Deskphone that is used for unlocking network menus. The default is 26567*738.

- password – the administrator password

ADMIN_PASSWORD_EXPIRY [seconds]

This parameter configures the date when the ADMIN_PWD is no longer valid and requires a new password to be downloaded from the provisioning server.

Note:

The value specifies expiry date in seconds (Unix Timestamp format).

A simple converter is available at the following site:

www.unixtimestamp.org/

To reset the expiry date value, use the following format: ADMIN_PASSWORD_EXPIRY 0

HASHED_ADMIN_PASSWORD [YES | NO]	This parameter indicates whether the Admin password is hashed or not. The default value is NO. • YES – Admin password is hashed. • NO – Admin password is not hashed.

Phone bug logging/recovery commands

RECOVERY_LEVEL [x]	This parameter controls IP Deskphone recovery if the IP Deskphone hits any Major or Critical error. The following values are used for configuring the recovery level on the IP Deskphone: • 0 - IP Deskphone never recovers from any error • 1 - IP Deskphone recovers from Critical error • 2 - IP Deskphone recovers from Major and Critical errors The default is 255, which is equivalent to the recovery level of 2.
LOG_LEVEL [x]	This parameter defines which IP Deskphone bugs are logged in the ECR file. The following values are used for configuring the logging level on the IP Deskphone. x - level of bugs from 0 to 255. The default value is 2. • 0 - logging is blocked • 1 - log only Critical bugs • 2 - log Critical / Major bugs • 3 - log Critical / Major / Minor bugs • >= 4 – log all information and bugs

Important:

LOG_LEVEL 4 is intended for debug purposes only. Do not set LOG_LEVEL to 4 or a higher value unless you are instructed to do so by Avaya support.

User Login commands

AUTOLOGIN_ID_KEY[nn] [userID@domain name]	This parameter is located within the IP Deskphone-specific configuration file. This is the ID the IP Deskphone uses to register. The default user ID is the MAC ID of the IP Deskphone. • nn — where nn = 01 to the maximum number of keys supported on the IP Deskphone • userID@domain name — the user ID must be followed by the domain name; for example, jsmith@company_name.com; example, 2247@company_name.com **Note:** To provision AUTOLOGIN_ID_KEY[nn] [userID@domain name], the IP Deskphone must be rebooted after the IP Deskphone configuration file is updated.
AUTOLOGIN_PASSWD_KEY[nn] [xx]	This parameter is located within the IP Deskphone-specific configuration file. There is no default password. If this is blank and AUTOLOGIN_ENABLE is configured to USE_AUTOLOGIN_ID (or 2) in the device configuration file, the IP Deskphone does not log on. • [nn] = the key number (01 – maximum number of keys supported on the IP Deskphone) • [xx] = the password for that key's login **Note:** To provision AUTOLOGIN_PASSWD_KEY[nn] [xx], the IP Deskphone must be rebooted after the IP Deskphone configuration file is updated.
PROMPT_AUTHNAME_ENABLE [YES | NO]	This parameter causes the user to be prompted to enter an authentication name when they log on to the IP Deskphone. For a CS 1000 system, it is necessary to configure an authentication name when configuring IP Deskphone features. • YES — prompt the user to enter an authentication name. • NO — authentication name is not configured.

AUTOLOGIN_AUTHID_KEY[nn][xx]	This parameter specifies the authentication name to be used for a specific key. • [nn] = the key number (01 – maximum number of keys supported on the IP Deskphone) • [xx] = the authorization ID for that key's login

•

Create the IP Deskphone-specific configuration file

If the IP Deskphone encounters a [USER_CONFIG] section while parsing the 11xxeSIP.cfg configuration file, the IP Deskphone downloads the IP Deskphone-specific configuration file SIP<MAC id>.cfg.

IP Deskphone-specific configuration files support customizing the IP Deskphone on a IP Deskphone/user level. Parameters in the device configuration file can be overwritten with a IP Deskphone-specific configuration file.

Most of the parameters in the IP Deskphone configuration file are saved on the IP Deskphone. Removing a parameter from the IP Deskphone configuration file does not change the parameters saved on a configured IP Deskphone. If a parameter is configured only in the IP Deskphone-specific configuration file, removing the IP Deskphone-specific configuration file does not clear the setting.

Important:

If the 11xxeSIP.cfg configuration file contains a [USER_CONFIG] section, Avaya recommends that DOWNLOAD_MODE be configured as FORCED. This is a global setting for all IP Deskphones used to determine if the MAC id file should be read. Alternatively, if the user wants to use DOWNLOAD_MODE configured to AUTO, then when a change is made to any MAC id file the version number should be incremented so that all IP Deskphones read the file.

Create the Dialing Plan file

If the IP Deskphone encounters a [DIALING_PLAN] section while parsing the 11xxeSIP.cfg configuration file, the IP Deskphone downloads the specified dialing plan configuration file from the provisioning server.

A dialing plan essentially describes the number and pattern of digits that a user dials to reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the number of digits dialed are all part of a dialing plan.

The purpose of the dialing plan is so that the end user does not have to press the send or pound key (#) to have the IP Deskphone with SIP Software send the initial message to start the call.

Dialing a telephone number on an IP Deskphone that supports SIP can be different than dialing a number from a traditional telephone. SIP signaling is communicated through a SIP URI to get to the far end. For example, you can key in the SIP address, *jsmith@yourcompany.com* to reach John Smith. When the IP Deskphone with SIP Software receives this address, the dialing plan is bypassed and the IP Deskphone uses the SIP URI to send a SIP INVITE to jsmith@yourcompany.com (INVITE sip: jsmith@yourcompany.com).

Entering a SIP URI address, however, is inconvenient on an IP Deskphone with SIP Software unless a USB keyboard is attached. Also, the user must explicitly press the **Send** key (or use some method to indicate the end of the URI) to indicate the completion of the SIP address. This is not something that the user is accustomed to in a traditional PBX environment.

The alternative is to use a URI where numbers are used to reach the far end. Using different access codes, the IP Deskphone with SIP Software translates the digits entered into something that the server can understand and remaps the number entered into different URIs. Some of the numbers are mapped as intercom calls, some numbers are mapped as local Public Switched Telephone Network (PSTN) calls, and some numbers are mapped as public long-distance calls.

The issue is that until the IP Deskphone itself can determine the type of call, no SIP INVITE message is sent. This is where the dialing plan comes into effect. The call type is determined by the dialing plan. Based on the rules defined in the dialing plan, once a match has been identified, the IP Deskphone with SIP Software sends the invite without the need to press the send key. This behavior closely matches the traditional PBX operation.

The IP Deskphone with SIP Software design places no restriction in the format of the SIP URI. The dialing plan is a scheme to match the user experience with traditional PBX operation. It does not restrict the type of URI that the user can use.

The IP Deskphone with SIP Software uses a dialing plan to recognize a call as an call when it sends an INVITE. The dialing plan can have multiple emergency numbers. See the chapter Emergency Services on page 215 for information on the handling of Emergency calls by the IP Deskphone with SIP software.

The following is an example of a dialing plan.

```
/* ------------------------------------------- */
/* A simple dial plan                          */
/* ------------------------------------------- */
$n="mycompany.com"
$t=300

%%

/* DIGITMAP: Operator call */


(0)|(0)#                  && sip:$$@$n;user=phone           &&


/* DIGITMAP: Emergency call */
(911)|(911)#              && sip:$$@$n;user=phone        && t=100|emergency


/* DIGITMAP: Avaya Aura Feature Access Code, *nn */
(*x{2})|(*x{2})#        && sip:$$@$n;user=phone           && t=100


/* DIGITMAP: Private internal call, 4 digit extensions starting with 4 */
(4x{3})|(4x{3})#        && sip:$$@$n;user=phone           &&


/* DIGITMAP: Private intra-location call, no access code */
```

```
([^4960]x{3})|([^4960]x{3})#      && sip:$$@$n;user=phone          &&

/* DIGITMAP: Private intra-company call, access code 6 */
(6[^10]x{6})|(6[^10]x{6})#        && sip:$$@$n;user=phone          &&

/* DIGITMAP: Public local call, access code 9 */
(9[^1]x{9})|(9[^1]x{9})#          && sip:$$@$n;user=phone          &&

/* DIGITMAP: Public national call, access code 61 */
(61x{10})|(61x{10})#                && sip:$$@$n;user=phone          &&

/* DIGITMAP: Public international call, access code 6011 */
(6011x{7,15})|(6011x{7,15})#      && sip:$$@$n;user=phone          && t=8000

/* End of Dial Plan */
```

Tip:

When repeating a pattern to add a trailing #, cut and paste the first pattern to ensure the patterns are identical (minimizes typing errors).

Dialing function description

Dialing plan

If the IP Deskphone encounters a [DIALING_PLAN] section while parsing the 11xxeSIP.cfg configuration file, the IP Deskphone downloads the specified dialing plan configuration file.

As most phone users are used to dialing digits to indicate the address of the destination, there is a need to specify the rule by which digits are transformed into a URI. The IP Deskphone with SIP Software dialing plan contains two sections delimited by two percent signs (%%).

```
+-------------------------+----------------------------------------+
| declarations section    | user pre define variables and parameters |
| %%                      | section separator                      |
| digit maps              | list of digit maps                     |
+------------------------------------------------------------------+
```

Figure 6: Sample dialing plan declarations section

In the declaration section, the administrator can define the variables. The variables must start with a dollar ($) sign, followed by a number or a character, such as $1 or $a. There are two variables that are reserved by system. They are as follows:

$$: used for the collected digits if they match the pattern

$t : default timer

There must be a domain name defined and the domain name can be represented by any variable. In the example given in Create the Dialing Plan file on page 123, the domain name is represented by $n.

The variable definitions take the form:

```
+-------------------------------------------+
| Name = value                              |
+-------------------------------------------+
```

Figure 7: Sample dialing plan variable definitions

For example:

$1="avaya.com"

$2="Avaya"

$3="."

$4="com"

$5="Avaya.com"

$t=10000 (default timer is 10 seconds)

$a=Avaya.com

The second section of dialing plan contains the digit map. The digit map section has three subsections that are divided by a separator of two ampersands (&&).

```
+---------------------------------------------------------------+
| patterns &&  destination string && dialing action attributes      |
+---------------------------------------------------------------+
```

Figure 8: Sample dialing plan digit map section

The first part of a dialing plan contains a pattern defined with DRegex, which is used for matching the dialed number. The patterns are separated by the pipe (|) sign. The second part contains the result string used in the dial step. The third part defines the parameters used by UA in dialing action.

The following parameter is currently defined:

t=xxxx: After this timer expires, the number entered is automatically dialed. The timer starts after the first digit is entered and after it expires, the collected digits are automatically dialed out. xxxx is a decimal number in msec. The default timer is used when t is not specified in the digit map.

For example:

X{4} && sip:$$; phone-context=avaya.com;user=phone && t=7000

When the user presses any 4 digits, such as 4567, the following SIP URIs are generated because of the translation rule:

Sip:4567; phone-context=avaya.com;user=phone. The timeout of stopping the collection of digits is 7 seconds.

The pound sign (#) at the end of the digit map causes the IP Deskphone to dial the matched dialing plan immediately.

DRegex

The Digit Regular Expression (DRegex) syntax is a telephony-oriented mapping of Portable Operating System Interface (POSIX) Extended Regular Expressions (ERE). Users must take care not to confuse the DRegex syntax with POSI EREs, as they are not identical. In particular, there are many features of POSIX EREs that DRegex does not support. The dialing plan uses DRegex instead of ERE. The following rules demonstrate the use of DRegex.

Table 7: DRegex rules

Entity	Matches
Character	Digits 0-9, *, #, and A-D (case insensitive, A-D only for military requirements)
*	The * character
#	The **#** character
[character selector]	Any character in selector
[^digit selector]	Any digit (0-9) not in selector
[range1-range2]	Any character in range from **range1** to **range2**, inclusive
x	Any digit 0-9
{m}	**m** repetitions of previous pattern
{m,}	**m** or more repetitions of previous pattern
{,n}	At most **n** (including zero) repetitions of previous pattern
{m,n}	At least **m** and at most **n** repetitions of previous pattern
()	Provide “captures” for back reference variable **$$**
$$	Back reference “matches” text previously matched within parentheses or the “matches” if parentheses are not specified
/* comments line */	Comments

DRegex notation example

Example	Description
1	Matches the digit **1**
[179]	Matches 1,7, or 9
[2-9]	Matches 2,3,4,5,6,7,8,9
[^15]	Matches 0,2,3,4,6,7,8,9
[02-46-9A-D]	Matches 0,2,3,4,6,7,8,9,A,B,C,D
x	Matches 0,1,2,3,4,5,6,7,8,9

Table continues…

Example	Description
*6[179#]	Matches *61, *67, *69, or *6#
x{10}	Matches ten digits
011x{7,15}	Matches 011 followed by seven to fifteen digits
91(x{10})	Matches 91 followed by ten digits • (x{10}) specifies the back reference variable, so $$ collects only ten digits (does not include the 91) • Example: 911234567890 is dialed $$=1234567890
(91x{10})	Matches 91 followed by ten digits • (91x{10}) specifies the back reference variable, so $$ collects all twelve digits • Example: 911234567890 is dialed $$=911234567890

Downloadable WAV files

If the IP Deskphone encounters a [TONES] section while parsing the 11xxeSIP.cfg file, the IP Deskphone downloads the specified tones configuration file.

It is possible to customize the ring tones on the IP Deskphone. Up to five special ring tones can be downloaded from the provisioning server and stored on the IP Deskphone. The end user can select which ring tone they would like to implement.

In order to download these special files, the files must reside on the provisioning server and be specified in the SIP provisioning file. For more information, see Download the SIP Software on page 46. The WAV files have a maximum size of 512 KB each for the IP Deskphone.

The file format is restricted to ITU-T A-law or u-law (8.0 kHz, 8-bit, mono or 16.0 kHz, 16 bit mono).

After the WAV files are downloaded to the IP Deskphone, the WAV file names appear in **Pref > Audio > Tones > Ring Pattern** (1 to 8 are standard ring tones, and 9 and above are WAV ring tones) and the WAV ring tones can then be selected to replace the standard ring tones.

For further information about downloadable WAV files, see the applicable IP Deskphone User Guide.

Chapter 7: Configure the DHCP Server

The Avaya IP Deskphones support two basic Dynamic Host Configuration Protocol (DHCP) mechanisms to provide configuration information to the IP Deskphones. These mechanisms are the following:

- Normal DHCP
- DHCP VLAN phase

Normal DHCP

The normal DHCP is used to configure standard IP parameters such as IP address, NetMask, default gateway, and DHCP lease parameters. The message sequence consists of Discover, Offer, Request, and Acknowledge. The IP Deskphones can also insert an optional phase. To include an optional phase, the first phase is used to discover and configure the voice VLAN using a Avaya proprietary method. The second phase then proceeds normally on the discovered VLAN. If the DHCP VLAN discovery is not used, then there is only a single phase.

DHCP VLAN Phase

The DHCP site and vendor specific options contain VLAN information to configure VLANs. The VLAN parameters are text string embedded in the standard DHCP Vendor and Site Specific options. You can acquire the VLAN parameters using 802.1ab and acquire IP address parameters using DHCP.

If the IP Deskphone does not contain VLAN configuration provisioned manually or through LLDP, the IP Deskphone attempts to determine the VLAN during DHCP VLAN Phase. If the IP Deskphone does find a VLAN configuration, it proceeds to the DHCP Configuration Phase. If the VLAN Phase (VLAN configured through DHCP) is successful, then the VLAN Phase finishes with a final DHCP. A release message appears after the completion of the Configuration Phase.

The following is the procedure to configure the Voice VLAN using DHCP, assuming VLAN is not configured using any other method:

1. The IP Deskphone sends a DHCP request using an untagged (no VLAN) packet during any of the following scenarios:
   - The customer network is configured to handle untagged packets; for example, retag them to a specific VLAN.

- The DHCP request contains standard IP Deskphone IP DHCP option requests from the point when the IP Deskphone does not receive the VLAN information. These options include the Vendor Specific and all Site Specific options.

2. The DHCP server receives the request. If the server is configured, the DHCP server returns a DHCP Offer message with a special text string in the Vendor Specific option or one of the Site Specific options.

   The following is the format of the text in the option:

   VLAN-A:XXX+YYY+ZZZ+…

   where VLAN-A is a substring followed with VLAN information. XXX, YYY, ZZZ are the numbers of the supported VLANs. There can be from 1 to 10 different VLANs. Each VLAN is separated with a symbol +.
3. After receiving the DHCP Offer message, the IP Deskphone scans each Vendor and Site Specific option for the VLAN-A string.
4. If the IP Deskphone finds the VLAN-A string, it tries each VLAN and in turn XXX, YYY, ZZZ searches for a DHCP server.
5. The search is done by sending a DHCP Discover message looking for a DHCP Offer message as a response.
6. If the IP Deskphone finds a response, it discontinues its DHCP exchange on the untagged channel and continues its DHCP exchange on the “discovered” VLAN.
7. If there is no response, the initial untagged Discover message assumes there is no VLAN configuration information available from the DHCP server and continues using untagged packets. When the IP Deskphone sends its first DHCP Discover message, it does not know if it can find VLAN configuration information. If it does discover VLAN information, it continues the VLAN configuration as described above. If it does not find any VLAN information, it assumes there is only a Configuration Phase.

DHCP options

The DHCP protocol provides options mechanisms for the client and server to exchange information in addition to the standard Bootstrap Protocol (BOOTP) information. This section describes the client and server options supported by the IP Deskphone.

- IP Deskphone to Server options on page 130
- Server to IP Deskphone options on page 131

IP Deskphone to Server options

When a DHCP client sends DHCP Discover and Request messages, it includes a list of options as part of the request. The IP Deskphone DHCP client sends the following options:

Option	Description
12	Specifies the Hostname. By default, the Hostname is “T”+MAC Address; for example, T001765FDBF1D. The Hostname can be manually provisioned using the keypad.
53	Specifies the DHCP Message Type.
55	Specifies the messages to tell the server which options the IP Deskphone is requesting. It appears in the Discover and Request. The SIP software requests the following options • 1 - IPv4 Subnet Mask • 3 - Router • 6 - Domain Name Server • 15 - Domain Name • 28 - Broadcast Address • 43 - Vendor Specific Information • 58 - Renewal Time • 59 - Rebinding Time • 66 - TFTP Server Name. The client treats this more generically as a request for the provisioning server name and protocol. • 99 - Must not be included • 128, 131, 144, 157, 188, 191, 205, 219, 223 - Specifies old site specific options. Recovered by IANA according to RFC 3942 and must not be used for new installations. • 224, 227, 230, 232, 235, 238, 241, 244, 247, 249, 251, 254- Specifies site specific options.
57	Specifies maximum DHCP message size. The maximum message size is 1190 bytes.
60	Sends “Nortel-SIP-Phone-A” as the Vendor Identifier.
61	Specifies Client Identifier (MAC Address).

Server to IP Deskphone options

The DHCP server can send any option to the IP Deskphone as part of the DHCP Offer message. The IP Deskphone accepts the following options:

	DHCP Option	Description
IPv4 Address		
Net mask	1	

Table continues…

	DHCP Option	Description
Router Option	3	
Domain Name Server	6	Accepts the first two DNS addresses.
Domain Name	15	
Broadcast Address	28	This is the broadcast address of the subnet. The IP Deskphone automatically calculates the broadcast address if it is not provided.
Vendor Specific Option	43	
DHCP Renewal Time	58	
DHCP Rebinding Time	59	
TFTP Server Name	66	Two forms of the server name are supported. If a dotted-decimal IP address is returned, it is assumed to point to a TFTP server. A full URL can also be provided to specify a protocol and FQDN.
Old Site Specific Options	128, 131, 144, 157, 188, 191, 205, 219, 223	Options are supported, but not recommended for new installations. These options are reclaimed according to RFC 3942.
Site Specific Options	224, 227, 230, 232, 235, 238, 241, 244, 247, 249, 251, 254	New site specific options which are recommended to be used.

The Vendor (43) or site specific options allows a vendor-encapsulated or site-specific option (or both) to transport the “Nortel-SIP-Phone-B” option string with auto-provisioning parameters to the IP Deskphone. The administrator must use one of the site-specific or vendor-encapsulated option codes; the method used depends on the DHCP server's capabilities and what options are already in use for other vendor devices.

Multiple DHCP Servers

It is possible that two or more DHCP servers can respond to the DHCP Discover message. When the IP Deskphone sends a Discover message, it waits for 1 second to collect all the responses. If there is more than one response, the IP Deskphone selects the response with the longest lease time. If the lease time is identical, the first response is selected.

Configure the DHCP server to support SIP IP Deskphone class identifier

After the DHCP server is configured to recognize the IP Deskphone with SIP Software as a unique IP Deskphone, the DHCP server can treat the IP Deskphone differently than other DHCP

Deskphones. An IP Deskphone-aware DHCP server can automatically configure IP Deskphones by sending all information that the IP Deskphone requires.

The IP Deskphone and the DHCP server communicate using a unique class identifier. After the IP Deskphone first sends the DHCP DISCOVER, it includes the Nortel-SIP-Phone-A ASCII string within the Vendor Class Identifier (Option 60). The DHCP server recognizes this special Vendor Class Identifier (Option 60) and sends back OFFER, which also includes the same Vendor Class Identifier. This makes it possible to notify the IP Deskphone with SIP Software that the server is IP Deskphone-aware, and that it is safe to accept the offer from the server.

Every IP Deskphone with SIP Software fills in the Vendor Class ID option of the DHCPDISCOVER and DHCPREQUEST messages with the null-terminated, ASCII-encoded string Nortel-SIP-Phone-A, where A identifies the version number of the information format of the IP Deskphone.

The Class Identifier Nortel-SIP-Phone-A must be unique in the DHCP server domain.

The unique DHCP configuration is required to allow the DHCP server to respond with a unique Option 66 parameter to the IP Deskphone with SIP Software.

Note:

The DHCP standard defines Option 66 as the bootp server address in a string. The meaning of the bootp server address is extended in Avaya IP Deskphone with SIP Software to include the provisioning server address. The string in the DHCP offer for Option 66 can be the numeric IP address or name of the Provisioning server or the URI (if FTP, HTTP, or HTTPS protocol is used) of the provisioning server in the form of

<protocol>://<provisioning server URL>.

For example:

http://mydomain.com/SIP_phone.

If provisioning server authentication is required, the user credential must be embedded in the URI in the form of

<protocol>://<userid>;<password>@<provisioning server URL>[:port][/path].

For example:

ftp://www.mydomain.com/ABC

or

ftp://myuserid:mypass@ftp.mydomain.com:21/ABC

Configuring the DHCP server to support the vendor class identifier is not mandatory but is one way to segregate network configuration data for the SIP phones from that for other devices. Below is an example of the Linux dhcpd DHCPv4 server configuration file modifications for the phone’s vendor class id when you want to have specific handling for different phone types.

dhcpd.conf

```
...
# Custom options for Avaya 1100 and 1200 phones
class "11xx12xxUNIStim" {
    match if substring(option vendor-class-identifier, 0, 14) = “Nortel-i2004-A”;
    option tftp-server-name “http://< IP address>/”;
}
```

```
class "11xx12xxSIP" {
    match if substring(option vendor-class-identifier, 0, 18) = "Nortel-SIP-Phone-A";
    option tftp-server-name "http://< IP address>/ ";
}
...
pool {
    range 192.168.xxx.xxx 192.168.xxx.xxx;
    allow members of "11xx12xxUNIStim";
    allow members of "11xx12xxSIP";
}
...
```

The following is an example of the similar handling but for the Open DHCP Server's configuration file.

`OpenDHCPServer.ini`

```
…
[GLOBAL_OPTIONS]
SubnetMask=255.255.255.0
Router=192.168.1.101
TFTPServerName="tftp://192.168.1.169"

# Custom options for Avaya 1100 and 1200 SIP phones
[RANGE_SET]
FilterVendorClass="Nortel-SIP-Phone-A"
DHCPRange=192.168.1.210-192.168.1.220
TFTPServerName="http://192.168.1.188"

# Custom options for Avaya 1100 and 1200 UNIStim phones
[RANGE_SET]
FilterVendorClass="Nortel-i2004-A"
DHCPRange=192.168.1.230-192.168.1.240
TFTPServerName="tftp://192.168.1.188"
…
```

Refer to your DHCP server's documentation for specifically how to configure a vender class id.

Configure DHCP Server with auto-provision data

The network items found in the IP Deskphone's Device Settings menu can be auto-provisioned using DHCP. The parameters are sent to the phone in the DHCP OFFER and DHCP ACK messages by adding them in either a vendor or site specific option.

The option text begins with "Nortel-SIP-Phone-B," followed by parameter/value pairs separated by semi-colons. The option string syntax is shown below:

```
"Nortel-SIP-Phone-B, <param>=<value>;<param>=<value>;… <param>=<value>;"
```

See section Configuration parameters on page 135 for a list of the auto-provision parameters and their syntax. Be sure any parameters being sent in the DHCP option string are set to "AUTO" mode in the Device Settings menu; if they are set as MANUAL then the manual values will override them and they will not take effect. For more details on how to setup automatic vs. manual configuration parameters, see Provisioning the IP Deskphones on page 153.

Below is an example of the Linux dhcpd DHCPv4 server configuration file containing an example of site-specific option 224. The example option's data configures the phone to enable the Bluetooth radio, disable the PC port, disable the USB interface and disable LLDP.

`dhcpd.conf`

```
…
# This line sets the tag Avaya-Custom-Phone to the numeric option
option Avaya-Custom-Phone code 224 = string;
...
class "Avaya11xx12xxSIP" {
    # This limits this option to the 11xx12xx SIP phones
    match if substring(option vendor-class-identifier, 0, 18) = "Nortel-SIP-Phone-A";

    # This line puts the auto-provisioning parameters in the option
    option Avaya-Custom-Phone "Nortel-SIP-Phone-B,bt=y;pc=n;usb=n;lldp=n;";
    …
}
…
```

The following is an example of the similar handling but for the Open DHCP Server's configuration file.

`OpenDHCPServer.ini`

```
# Custom options for Avaya 1100 and 1200 SIP phones
[RANGE_SET]
# This filter limits the items in this [RANGE_SET] to the 11xx12xx SIP phones
FilterVendorClass="Nortel-SIP-Phone-A"

# This line defines the auto-provisioning parameters in option 224
224="Nortel-SIP-Phone-B,bt=y;pc=n;usb=n;lldp=n;"
…
```

Refer to your DHCP server's documentation for specifically how to configure a vendor or site option and its data.

Configuration parameters

The IP Deskphones can receive the auto-provision parameters shown in the following table:

Table 8: Provisioning info block format

Parameter	Value	Description
EAP (802.1x)		
eap	dis for disable md5 for EAP-MD5 peap for EAP-PEAP tls for EAP-TLS	Disable or select an EAP authentication method.

Table continues…

Parameter	Value	Description
	Caution: Changing this parameter can impact network connectivity and can require manual correction. **Important:** Information is transferred in clear text when you provision this parameter using DHCP.	
eapid1	Character string from 4 to 20 characters	802.1x (EAP) device ID1.
	Caution: Changing this parameter can impact network connectivity and can require manual correction. **Important:** Information is transferred in clear text when you provision this parameter using DHCP.	
eapid2	Character string from 4 to 20 characters	802.1x (EAP) device ID2.
	Caution: Changing this parameter can impact network connectivity and can require manual correction. **Important:** Information is transferred in clear text when you provision this parameter using DHCP.	
eappwd	Character string from 4 to 12 characters	802.1x (EAP) password.
	Caution: Changing this parameter can impact network connectivity and can require manual correction. **Important:** Information is transferred in clear text when you provision this parameter using DHCP.	
Other networking		
ca	Character string with a maximum of 80 characters	The URL of the Certificate Authority (CA) server
cahost	Character string with a maximum of 32 characters	The Certificate Authority (CA) host name assigned to the IP Deskphone.
cadomain	Character string with a maximum of 50 characters	The Certificate Authority (CA) domain name to which the IP Deskphone is a member of.
dns	Character string with a maximum of 50 characters	Primary DNS server URL

Table continues…

Parameter	Value	Description
dns2	Character string with a maximum of 50 characters	Secondary DNS server URL
lldp	y for yes n for no	Enable 802.1ab LLDP.
	Caution: Changing this parameter can impact network connectivity and can require manual correction.	
prov	Character string with a maximum of 50 characters	Provisioning server URL. For an HTTP server, you must include "http://" in the URL.
st	y for yes n for no	Enable stickiness.
cachedip	y for yes n for no	Enable cached IP.
dhcp	y for yes n for no	Enable Dynamic Host Configuration Protocol (DHCP).
ntqos	y for yes n for no	Enable Avaya Automatic QoS
igarp	y for yes n no	Ignore GARP.
srtp	y for yes n for no	Enable SRTP-PSK.
srtpid	96 (default) 115 120	Payload type ID
Voice VLAN		
vq	y for yes n for no	Enable 802.1Q for voice.
	Caution: Changing this parameter can impact network connectivity and can require manual correction.	
vcp	Value from 0 to 8	802.1Q control p bit for voice stream.
vmp	Value from 0 to 8	802.1Q media p bit for voice stream
vlanf	y for yes n for no	Enable VLAN filter on voice stream.
vvsource	n for no VLAN	Source of VLAN information.

Table continues…

Parameter	Value	Description
	a for auto VLAN using DHCP lv for auto VLAN using VLAN Name TLV lm for auto VLAN using Network Policy TLV	
PC Port		
nis	a for automatic negotiation 10 for 10 Mbps 100 for 100 Mbps	Network port speed.
	⚠ **Caution:** Changing this parameter can impact network connectivity and can require manual correction. **Important:** You must select automatic negotiation when using Gigabit Ethernet (GigE) on Avaya 1120E/1140E/1150E IP Deskphone.	
nid	a for automatic negotiation f for full duplex h for half duplex	Network port duplex.
	⚠ **Caution:** Changing this parameter can impact network connectivity and can require manual correction.	
pc	y for yes n for no	Enable PC port. This parameter does not apply to the 2001 IP Phone.
pcs	a for automatic negotiation 10 for 10 Mbps 100 for 100 Mbps	PC port speed.
pcd	a for automatic negotiation f for full duplex h for half duplex	PC port duplex.
Data VLAN		
dq	y for yes n for no	Enable 802.1Q for PC port.
dv	y for yes n for no	Enable VLAN for data. This parameter does not apply to the 2001 IP Phone.
dvid	Value from 0 to 4095	VLAN ID for data VLAN.

Table continues…

Parameter	Value	Description
dp	Value from 0 to 8	802.1Q p bit for data stream.
Diffserv Codepoint		
cdiff	Value from 0 to 255	Diffserv code points for control messages.
mdiff	Value from 0 to 255	DiffServ code point for media packets.
pcuntag	y for yes n for no	Enable tag stripping on packets forwarded to PC port.
dscpovr	y for yes n for no	DSCP Precedence Override
Miscellaneous		
bt (1100 only)	y for yes n for no	Enable Bluetooth® (Avaya 1140E/1165E IP Deskphone only).
hd (1100 only)	w for wired b for Bluetooth® (1140E and 1165E only) u for USB, n for none	Headset type (Avaya 1120E/1140E/ 1165E IP Deskphone)
menulock	f for full lock p for partial u for unlock	Menu lock mode.
unid	Character string up to 32 characters	Unique network identification.
usb	y for yes n for no	Enable USB port. (Avaya 1165E IP Deskphone only)
usbm	y for yes n for no	Enable USB mouse device on USB port. (Avaya 1165E IP Deskphone only)
usbk	y for yes n for no	Enable USB keyboard device on USB port. (Avaya 1165E IP Deskphone only)
usbh	y for yes n for no	Enable USB headset device on USB port. (Avaya 1165E IP Deskphone only)
usbms	y for yes n for no	Enable USB flash drive device on USB port. (Avaya 1165E IP Deskphone only)
Display control		
ct	Value from 0 to 15 (Avaya 1100 Series IP Deskphones) Value from 0 to 39 (for Avaya 2007 IP Deskphone)	Contrast value.
br	Value from 0 to 15	Brightness value (Avaya 2007 IP Deskphone).

Table continues…

Parameter	Value	Description
blt	Value from 0 to 6 0 = 5 seconds 1 = 1 minute 2 = 5 minutes 3 = 10 minutes 4 = 15 minutes 5 = 30 minutes 6 = 1 hour 7 = 2 hours 8 = always on	Backlight timer (Avaya 1100 Series IP Deskphones and Avaya 2007 IP Deskphone).
bold	y for yes n for no	Enable bold font on phone and Expansion Module (Avaya 1100 Series IP Deskphones)
dim	y for yes n for no	Enable screen dimmer (Avaya 1100 Series IP Deskphones only)
Error logging		
ar	y for yes n for no	Enable automatic recovery.
arl	cr for critical ma for major mi for minor	Auto recovery level.
ll	cr for critical ma for major mi for minor in for information	Log level.
Security		
ssh	y for yes n for no	Enable Secure Shell (SSH).
sshid	4 to 12 characters	SSH ID.
	Important: Information is transferred in clear text when you provision this parameter using DHCP.	
sshpwd	4 to 12 characters	SSH password.

Table continues…

Parameter	Value	Description
	Important: Information is transferred in clear text when you provision this parameter using DHCP.	

Warning:

The provisioning data is transferred by DHCP, which is an unsecured protocol.

Warning:

Changing this parameter could impact the network connectivity and may require manual correction.

The following table shows the dependencies between provisioning options.

Table 9: Dependencies

Primary provisioning option	Rules
VQ	If VQ is present and configured to N, then VCP, VMP, and VLANF are ignored if they are present.
DQ	If DQ is present and configured to N, then DV and DP are ignored if they are present.
PC	If PC is present and configured to N, then PCS, PCD, and PCUNTAG are ignored if they are present.
PCS	If PCS is present and configured to A, then PCD is ignored if it is present.

Chapter 8: Install the IP Deskphone

Complete instructions to install the IP Deskphone, including detailed figures and applicable warnings, are given in the IP Deskphones User Guides.

The steps for installing the IP Deskphone are summarized in the following procedure.

Installing the IP Deskphone

1. Remove the stand cover. Pull upward on the center catch and remove the stand cover. The cable routing tracks are now accessible.
2. Connect the AC power adapter (optional). Connect the adapter to the AC adapter jack in the bottom of the IP Deskphone. Form a small bend in the cable, and then thread the adapter cord through the channels in the stand.
3. Install the handset. Connect the end of the handset cable with the short straight section into the handset. Connect the end of the handset cable with the long straight section to the back of the IP Deskphone, using the RJ-9 handset jack. Form a small bend in the cable, and then thread the handset cord through the channels in the stand so that it exits behind the handset on the right side, in the handset cord exit in the stand base.
4. Install the headset (optional). If installing a headset, plug the connector into the RJ-9 headset jack on the back of the IP Deskphone, and thread the headset cord along with the handset cord through the channels in the stand, so that the headset cord exits the channel.
5. Install the Ethernet cable. Connect one end of the supplied Ethernet cable to the back of the IP Deskphone using the RJ-45 connector and thread the network cable through the channel.
6. Install the Ethernet cable connecting the PC to the IP Deskphone (optional). If connecting PC Ethernet through the IP Deskphone, connect one end of the PC Ethernet cable to the IP Deskphone using the RJ-45 connector and thread it through the channel. Connect the other end to the LAN connector on the back of the PC.
7. Install additional cables. If applicable, plug in optional USB devices. Connect the Ethernet cable to the LAN Ethernet connection. If using an AC power adapter, plug the adapter into an AC outlet.
8. Wall-mount the IP Deskphone (optional). The IP Deskphone can be mounted either by: (method A) using the mounting holes on the bottom of the IP Deskphone stand, or (method B) using a traditional-style wall-mount box with RJ-45 connector and 15-cm (6-inch) RJ-45 cord (not provided).
9. Replace the stand cover. Ensure that all cables are neatly routed and press the stand cover into place until a click is heard.
10. Put the IP Deskphone in the wall-mount position (optional). If the IP Deskphone is to be mounted on the wall, put it in the wall-mount position by holding the tilt lever and pressing the IP Deskphone towards the base until the IP Deskphone is parallel with the base.

Release the tilt lever and continue to push the IP Deskphone towards the base until an audible click is heard. Ensure the IP Deskphone is securely locked in position.

The following figure shows the connections on the IP Deskphone.

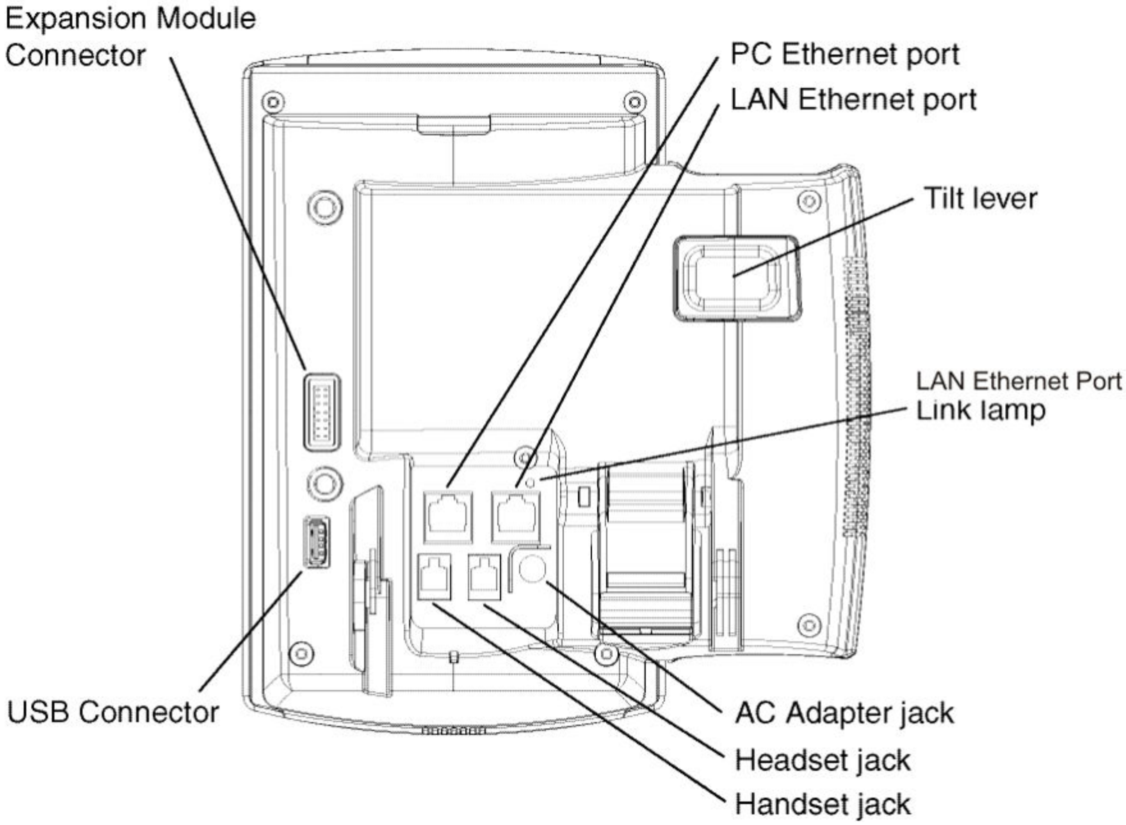


Figure 9: IP Deskphone connections

Chapter 9: Upgrade and convert the IP Deskphone software

This chapter describes how to upgrade an IP Deskphone with UNIStim software to SIP Software.

In order to upgrade an IP Deskphone with UNIStim software, first determine if you have the minimum UNIStim software release on the IP Deskphone (0625C39). If your IP Deskphone is installed with the minimum version of UNIStim software, proceed to the section Convert UNIStim software to SIP Software on the IP Deskphone on page 150. If your IP Deskphone is not installed with the minimum version of UNIStim Software, proceed to the section Upgrade UNIStim software to the minimum required UNIStim software on page 147.

To convert the firmware on the IP Deskphone from SIP to UNIStim, see the section Convert SIP Software to UNIStim Software on page 151.

Upgrade the SIP Software on the IP Deskphone

Use the following procedures to upgrade existing SIP Software to new SIP Software on the IP Deskphone.

Download the SIP Software

To download the SIP Software from the Avaya web site, perform the following procedure.

Downloading SIP Software for the IP Deskphone

1. Go to http://www.avaya.com/support.

   The **Avaya Support** page appears.
2. Click **Downloads & Documents** in the menu at the top of the page.
3. Enter the IP Deskphone type in the **Enter Your Product Here** box.
4. From the **Choose Release** drop down list, select the desired release of SIP software.
5. In the **Select a content type** pane, click the **Downloads** radio button and click **Enter**.
6. From the search results, select the desired release of the SIP Software for the IP Deskphone.

   A new window opens.

7. Scroll down the page and click the desired version of software; for example, SIP1165e04.04.09.00.bin.

   The **File Download** window opens.
8. Click **Save**.

   The **Save As** window opens.
9. Select the location to save the file and click **Save**.
10. After the file has downloaded, place the file in the correct directory on the provisioning server.

Modify the SIP provisioning file

Use the following procedure to modify the SIP Provisioning file on the provisioning server.

Modifying the SIP provisioning file

1. Under the firmware [FW] section of the SIP Provisioning file, increase the VERSION number (for example SIP1165e04.04.09.00).
2. Under the firmware [FW] section of the SIP Provisioning file, modify the FILENAME of the new file you want to upload to the IP Deskphone.

   Important:

   The VERSION number must be the same as the FILENAME (do not include the .bin extension).

   For example, if the FILENAME is SIP1165e04.04.09.00.bin, then the VERSION must be SIP1165e04.04.09.00.
3. Invoke the upgrade mechanism.

   Use one of the next three methods to invoke a software upgrade on the IP Deskphone with SIP Software.

   a. Power off and power on the IP Deskphone.
   b. Select **Services > Check For Updates** on the IP Deskphone.
   c. Allow for an automatic check for updates to occur. (See AUTO_UPDATE under Feature configuration commands on page 73).

   Any of these actions causes the IP Deskphone to contact the provisioning server and attempt to read the Provisioning file. A soft reset (**Services > System > Reset Phone**) does not cause the IP Deskphone to retrieve the Provisioning file and therefore does not cause a software upgrade.

Upgrade to the minimum UNIStim Software

The IP Deskphone can be ordered with UNIStim software installed or with SIP Software installed. You can convert the software on an IP Deskphone from UNIStim to SIP. To successfully convert the software from UNIStim to SIP, the UNIStim software version on your IP Deskphone must be 0625C39 or higher.

Identify the current version of UNIStim software

Checking the UNIStim software version on a new IP Deskphone

1. After assembling the IP Deskphone and turning it on, the display on the IP Deskphone goes through the following sequence:
   - Avaya splash screen appears
   - Avaya sonic sound plays
   - Avaya banner appears

   Following the Avaya banner, the software version appears in the display (F/W version).
2. Note the UNIStim software version number and write it down. Compare the version number to the minimum-required UNIStim software version (0625C39).

   UNIStim software version names contain numbers and letters. Use the last three characters in a version to compare the version of UNIStim on an IP Deskphone (0625C39) with the minimum required version for the upgrade. Note that D23 is greater than C39 and C1B is less than C39.

   If the version number is equal to or higher than 0625C39, see Convert UNIStim software to SIP Software on the IP Deskphone on page 150.

   If the number is lower than 0625C39, go to the section Upgrade UNIStim software to the minimum required UNIStim software on page 147 and follow the instructions to upgrade an IP Deskphone to the minimum-required version of UNIStim software before a conversion to SIP Software.

Checking the UNIStim software version on an IP Deskphone already in use

1. Press the **Services** key on the IP Deskphone twice quickly.

   If the Admin password prompt appears, enter the password **26567*738**

   The Local Tools menu appears:

   Table 10: Local Tools menu

1. Preferences
2. Local Diagnostics
3. Network Configuration
4. Lock Menu

2. To make a selection, press the number associated with the menu item, or use the Navigation key cluster to scroll through the menu items. Press the **Select** key to select the highlighted menu item.

Table 11: Using the Navigation key cluster to navigate in the Local Tools menu

Key	Action
Down	Moves highlight down
Up	Moves highlight up
Right	Selected current menu item
Left	Closes menu
Select key (center of cluster)	Selects current menu item

To close this menu, press the **Quit** key.

3. Select **2. Local Diagnostics** in the Local Tools menu by pressing the key in the Navigation key cluster or by pressing the number **2**.
4. Select **IP Set Information** by pressing the **Select** key in the Navigation key cluster or by pressing the number .
5. Use the down arrow in the Navigation key cluster to scroll down the menu to Software Version.
6. Note the UNIStim software version number and write it down.

   Compare the version number to the minimum-required UNIStim software version (0625C39).

   UNIStim software version names contain numbers and letters. Use the last three characters in a version to compare the version of UNIStim on an IP Deskphone (0625C39) with the minimum required version for the upgrade. Note that C23 is greater than C39 and C1B is less than C39.

If the version number is equal to or higher than 0625C39, go to the section Convert UNIStim software to SIP Software on the IP Deskphone on page 150.

If the number is lower than 0625C39, see Upgrade UNIStim software to the minimum required UNIStim software on page 147 and follow the instructions to upgrade an IP Deskphone to the minimum-required version of UNIStim software before you convert to SIP Software.

Upgrade UNIStim software to the minimum required UNIStim software

Use either of the following two methods to upgrade UNIStim software.

1. UFTP download initiated by the server if the server supports this method of upgrading UNIStim software. Refer to the appropriate documentation for your Call Server for instructions on using this method.
2. TFTP download on bootup.

If necessary, use the following procedure to configure the TFTP server.

Configuring the TFTP server

1. The IP Deskphone always executes the TFTP download at bootup if a TFTP IP address is configured on the IP Deskphone after being initiated by the telephony Call Server.
2. Go to the TFTP server and create the 11xxe.cfg provisioning file (for example; 1140e.cfg for 1140E IP Deskphones, 1120e.cfg for 1120E IP Deskphones). The 11xxe.cfg provisioning file is a clear text file. Create the provisioning file as shown in the next table.

   Table 12: Sample 11xxe.cfg provisioning file

[FW]
DOWNLOAD_MODE FORCED
VERSION 0625C23
FILENAME 0625C23.bin

   This configuration file forces the software download of 0625C23.bin.
3. Download and copy the software to the TFTP server directory.

   To download the UNIStim software for the IP Deskphone from the Avaya Web site:

   a. Go to http://www.avaya.com/support.

      The **Avaya Support** page appears.

   b. Click **Downloads & Documents** in the menu at the top of the page.
   c. Enter the IP Deskphone type in the **Enter Your Product Here** box.
   d. From the **Choose Release** drop down list, select the desired release of UNIStim software.
   e. In the **Select a content type** pane, click the **Downloads** radio button and click **Enter**.
   f. From the search results, select the desired release of the UNIStim software for the IP Deskphone.

      A new window opens.

   g. Scroll down the page and click the desired version of software; for example, Avaya 1165E IP Deskphone Release 0625C23.

      The **File Download** window opens.

   h. Click **Save**.

      The **Save As** window opens.

   i. Select the location to save the file and click **Save**.
   j. After the file has downloaded, place the file in the correct directory on the provisioning server.
4. In the IP Deskphone **Network Configuration** menu, change the TFTP server address and enter the correct Provisioning server IP address.

   This can be the Provisioning server as defined in the chapter Creating the provisioning files on page 45.

5. Press the **Apply** context-sensitive soft key to save the configurations and reset the IP Deskphone.

   The IP Deskphone downloads the software file. The display shows **[FW] reading…**

   If the download is successful, the display shows **[FW] writing…** and the blue LED flashes.

   After the software image is downloaded to the IP Deskphone, the display shows **[FW] finished...**, the blue LED stops flashing, and the IP Deskphone resets.

   The IP Deskphone registers to the TPS with the new software version.

   If the upgrade is unsuccessful, see the chapter Diagnostics and troubleshooting on page 341 in the section titled "**Download failures**".

Follow the next procedure to download the minimum required version of UNIStim software automatically through TFTP on bootup.

Downloading UNIStim software automatically through TFTP on bootup (1120E and 1140E IP Deskphones only)

1. Double press the **Services** key on the IP Deskphone quickly.

   If the admin password prompt appears, enter the password **26567*738**

   The Local Tools menu appears:

   Table 13: Local Tools menu

1. Preferences
2. Local Diagnostics
3. Network Configuration
4. Lock Menu

2. Select **3. Network Configuration** from the **Local Tools** menu.

   The **Network Configuration** screen appears.

3. If you are using DHCP, select **Yes**.

   If you are manually configuring the IP address, netmask, and gateway address, select **No**.

4. If the DHCP option is configured, the IP address is automatically obtained.

5. Configure the TFTP IP address within the IP Deskphone Device Settings menu.

   This can be the provisioning server as defined in the chapter Creating the provisioning files on page 45.

6. Select the **Apply** context-sensitive soft key to save the settings and reset the IP Deskphone.

   The IP Deskphone downloads the software file. The display shows `[FW] reading…`

   If the download is successful, the display shows `[FW] writing…` and the blue LED flashes.

   After the software image is downloaded to the IP Deskphone, the display shows `[FW] finished...` the blue LED stops flashing, and the IP Deskphone resets.

   If the upgrade is unsuccessful, see IP Deskphone diagnostics on page 341.

Convert UNIStim software to SIP Software on the IP Deskphone

The IP Deskphone can be ordered with UNIStim software installed or with SIP Software installed. If an IP Deskphone is installed with UNIStim software, it runs with SIP Software only if the software is converted from UNIStim to SIP. If the procedure to determine the UNIStim version number is completed, and, if necessary, the procedure to upgrade the UNIStim software is completed, an IP Deskphone can be converted from UNIStim software to SIP Software.

Compare the version number to the minimum required UNIStim software version (0625C39).

UNIStim software version names contain numbers and letters. Use the last three characters in a version to compare the version of UNIStim on an IP Deskphone (0625C39) with the minimum required version for the upgrade. Note that D23 is greater than C39 and C1B is less than C39.

The conversion must be performed using TFTP.

Warning:

The TFTP download and upgrade of the Flash memory on the IP Deskphone can take a significant amount of time (possibly up to 10 minutes). Do not unplug or reboot the IP Deskphone during the process.

The following procedure explains how to download the SIP Software from the Avaya Web site.

Downloading SIP Software for the IP Deskphone from the Avaya Web site

1. Go to http://www.avaya.com/support.

   The **Avaya Support** page appears.
2. Click **Downloads & Documents** in the menu at the top of the page.
3. Enter the IP Deskphone type in the **Enter Your Product Here** box.
4. From the **Choose Release** drop down list, select the desired release of SIP software.
5. In the **Select a content type** pane, click the **Downloads** radio button and click **Enter**.
6. From the search results, select the desired release of the SIP Software for the IP Deskphone.

   A new window opens.
7. Scroll down the page and click the desired version of software; for example, SIP1165e04.04.09.00.bin.

   The **File Download** window opens.
8. Click **Save**.

   The **Save As** window opens.
9. Select the location to save the file and click **Save**.
10. After the file has downloaded, place the file in the correct directory on the provisioning server.

Perform the following procedure to convert the UNIStim software to SIP Software on the IP Deskphone.

Converting UNIStim software to SIP Software using TFTP

1. Run the TFTP server (for example Tftpd32.exe).
2. Place software and configuration files in the folder of the TFTP server (for example 11xxe.img F/W file and 11xxe.cfg file) that contains the following lines:

   Table 14: Sample 11xxe.cfg configuration file

[FW]
DOWNLOAD_MODE FORCED
PROTOCOL TFTP
VERSION 06C25D26.bin
FILENAME 11xxe.img

3. In the **Network Configuration** menu, configure the TFTP IP address field with the IP address of your TFTP server.

   After you are finished the configuration, the IP Deskphone reboots and sends a request to the TFTP server.
4. Select the **Apply** context-sensitive soft key to save the settings and reset the IP Deskphone.

   The following messages display on the IP Deskphone as the IP Deskphone cycles through the conversion process, one after the other:

   a. `[FW] Reading...`
   b. `[FW] Writing...`
   c. `[FW] Finished...`

   The IP Deskphone then boots up with SIP Software.

1. TFTP file transfer takes approximately 15 seconds.
2. File writing takes 2.5 minutes. The IP Deskphone displays the message `[FW] writing…` and the blue Data Waiting LED flashes.
3. After the new SIP Software writing is finished, the blue LED stops flashing and the IP Deskphone displays `[FW] finished` and then reboots.
4. The first time the SIP Software boots, the SIP Software performs a Flash File System conversion that takes 2.5 minutes.

Convert SIP Software to UNIStim Software

The IP Deskphone can be ordered with UNIStim software installed or with SIP software installed. If you have an IP Deskphone with UNIStim software, and you convert the software from UNIStim to

SIP, the UNIStim software is overwritten. To convert an IP Deskphone from SIP software to UNIStim software, a software reload is required.

Reloading UNIStim software

1. Determine the appropriate UNIStim version to match the hardware release number of your IP Deskphone.

   There are different versions of UNIStim software available for download. Which version you choose depends on the hardware release number of your particular IP Deskphone.

   If the hardware release number of your IP Deskphone is among the following hardware release numbers, download UNIStim software version release 0625C39 or higher (the hardware release number is the Product Engineering Code [PEC] followed by the release number):

   - NTYS05ACE6 20
   - NTYS05BCE6 20
   - NTYS05BCGSE6 04

   If the hardware release number of your IP Deskphone is not among the previous list, download UNIStim version release 0625C23 or higher.

   Note:

   UNIStim software version names contain numbers and letters. Use the last three characters in a version to determine the minimum required version for the conversion. For example, C39 is greater than C23.

2. Download the appropriate UNIStim software file to your provisioning server.
3. Create an 1xxxeSIP.cfg file (for example, 1140eSIP.cfg for the 1140E IP Deskphone) containing the following information:

   [FW]

   DOWNLOAD_MODE FORCED

   PROTOCOL TFTP (if using TFTP)

   VERSION xxx

   FILENAME yyy.bin

   where xxx is the UNIStim version number appropriate for the hardware release of your IP Deskphone, for example, 0625C23, and yyy.bin is the filename containing the version number, for example, 0625C23.bin.

4. Power the IP Deskphone off and on. The IP Deskphone reboots and contacts the provisioning server upon bootup and downloads the new UNIStim software.

Chapter 10: Provisioning the IP Deskphone Device Settings

For provisioning the Device Settings parameters, the IP Deskphones support the following provisioning modes:

- Manual provisioning
- Automatic provisioning

The IP Deskphone obtains configuration parameters that are defined as AUTO in the Auto Provisioning page from an 802.1ab switch (LLDP) or DHCP server. For more information, see Parameter source precedence rules on page 163.

Manual provisioning

The manual provisioning of IP Deskphone parameters overrides the configuration of parameters by any other provisioning source. Technicians can use manual provisioning to override system wide parameters for troubleshooting purposes or to provide special needs configurations for a small group of users.

Automatic provisioning

The Automatic provisioning feature creates a flexible provisioning method, which

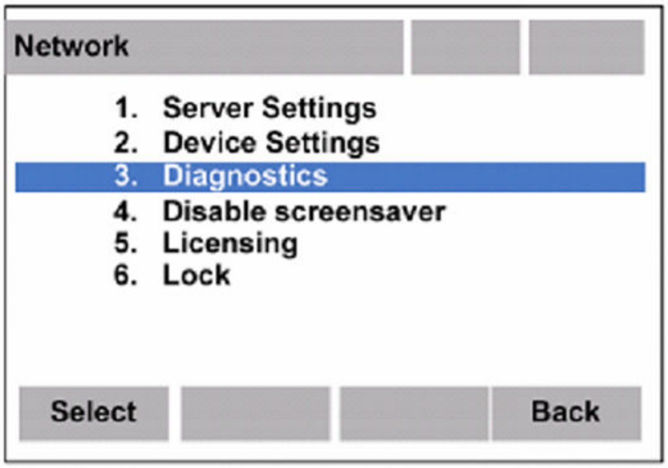
- covers the existing provisioning parameters
- supports the extension of the provisioning parameters
- supports provisioning parameters in automatic provisioning modes, when possible
- creates a common provisioning information format that supports DHCP provisioning

You can store common provisioning parameters in a managed central server, such as a DHCP server. You can configure the IP Deskphone to automatically or manually obtain the provisioning parameters from the various provisioning sources. By default, the IP Deskphone automatically provisions most parameters.

For automatic provisioning, the IP Deskphone receives the parameters from the provisioning server. You can switch between automatic provisioning to manual provisioning on the **Auto Provisioning** page. You enter parameter information on the **Configuration** page.

Provisioning IP Deskphone parameters

By default, the IP Deskphone can automatically provision most parameters. However, you can manually provision parameters. The Auto Provisioning page provides the selection to manually override the parameter. Use the **Device Settings** menu item to configure IP Deskphone parameters. Double-press the **Globe** key to open the Network menu and press **2** on the dial pad to open the **Device Settings** menu.



The **Configuration** page appears when you select the **Device Settings** menu item. Any automatic provisioned parameters appear dimmed.

The Device Settings menu shows the configuration parameters that are configured as Manual on the Auto Provisioning page. Use the Up and Down navigation keys to scroll through the main configuration options and the Right or Left navigation keys to scroll through the sub configuration options.

For all supported IP Deskphones, you can press the **Auto** soft key to switch to the **Auto Provisioning** page to define parameters that you can obtain automatically or manually. Then from the Auto Provisioning page, you can press the **Cfg** soft key to switch to the **Device Settings** option.

Configuring parameters manually for the IP Deskphone

Procedure

1. Press **Auto** on the Configuration page to switch to the Auto Provisioning page.
2. Perform one of the following actions:
   - Press the **AllMan** soft key to change all parameters to be manually provisioned.
   - Use the dial pad to enter the number associated with the parameter, or use the navigation keys to scroll and highlight the specific parameter (up/down navigation takes you from

group to group, while left/right navigation takes you from item to item). Press the **Enter** key to uncheck the parameter, making it "Manual" provisioned.

3. To exit and save, press the **Config** key to return to the Device Settings page, then press **Apply**.

Configuring parameters automatically for the IP Deskphone

About this task

Perform the following procedures to configure all parameters or specific parameters using automatic provisioning.

Procedure

1. Press **Auto** on the Configuration page to switch to the Auto Provisioning page.
2. Perform one of the following actions:
   - Press the **AllMan** soft key to change all parameters to be auto-provisioned.
   - Use the dial pad to enter the number associated with the parameter, or use the navigation keys to scroll and highlight the specific parameter (up/down navigation takes you from group to group, while left/right navigation takes you from item to item). Press the **Enter** key to check the parameter, making it "Auto" provisioned.
3. To exit and save, press the **Config** key to return to the Device Settings page, then press **Apply**.

Auto Provisioning parameters

Use the keys in the following table to provision the parameters for the IP Deskphones.

Table 15: Keys and descriptions

Key	Description
[ ]	Check box, select or clear: Auto-checked, Manual-unchecked.
Dial pad	Enter number of index to jump to option
Up	Move up a group index
Down	Move down a group index
Right	Go to next item.

Table continues…

Key	Description
Left	Go to previous item.
Enter	Select or clear the check box for item or group.
Config	Return to manual configuration page.
AllMan / AllAut	Context-sensitive. Set all items to manual (clear checkboxes) or auto (check all boxes).
Cancel	Exit Device Settings.

The **Auto** page provides control over the auto-provisioning of the **Device Settings** parameters. The page's items in order of appearance:

```
01. EAP Settings
02. LLDP Enable
        DHCP Enable
03. Primary DNS IP
        Secondary DNS IP
04. Certificate Server
        Domain Name
        Hostname
05. Ntwk Port Speed
        Ntwk Port Duplex
06. Voice 802.1Q
        Voice VLAN Source
        Voice VLAN Filter
        Voice Control pBits
        Voice Media pBits
        Avaya Auto QoS
        Voice Ctrl DSCP
        Voice Media DSCP
07. PC Port Enable
        PC Port Speed
        PC Port Duplex
        PC Port UntagAll
08. Data 802.1Q
        Data VLAN
        Data Priority Bits
09. Provision Server
10. PVQMon
11. NAT Signal
        NAT Media
        NAT Config
        STUN S1 IP
        STUN S2 IP
12. Stickiness
        Cached IP
        Ignore GARP
13. Menu Lock Enable
14. Auto Recover Flag
15. Screen Contrast
        Screen Backlight (1100 series only)
16. Headset Type
17. SRTP Enabled
        SRTP Mode
        SRTP Cipher1
        SRTP Cipher2
18. SSH Enable
        SSH User ID
        SSH Password
        SFTP Enable
19. Sip UDP Port
```

```
        Sip TCP Port
        Sip TLS Port
20. Keep Alive Type
        Connection Keep Alive
21. Register Retry Time
        Register Retry Max Time
22. Login Notify
        Login Notify With Time
23. IPv6 Enable
24. FIPS Enable
```

Manual provisioning parameters

Use the Device Settings menu to manually provision the IP Deskphones. Double-press the Services key. You can press the number associated with the menu item or you can use the navigation keys to scroll through the list of items.

Use the keys in the following table to provision the parameters for the IP Deskphones.

Table 16: Keys and descriptions

Key	Description
Up	Main dialog: Scroll dialog up (highlight does not move) In list: move highlight up an item.
Down	Main dialog: Scroll dialog down (highlight does not move) In list: move highlight down an item
Right	Move highlight down an item In list: close list
Left	Move highlight up an item
Enter	Highlight on list item: open list In list: select highlighted item and close list Highlight on editable item: start edit mode Highlight on checkbox item: toggle checkbox state
Apply	Save changes and reboot IP Deskphone.
Auto	Go to Auto provision page.
Config	Return to manual configuration page.
AllMan / AllAut	Context-sensitive. Set all items to manual (clear checkboxes) or auto (check all boxes).
Cancel	Exit Device Settings without saving changes.
In edit mode	
Up	Scroll dialog up (highlight does not move).
DownScroll dialog down (highlight does not move)	Exits Edit mode, moves highlight up an item.
Left	Moves edit cursor to the left.
Right	Moves edit cursor to the right.

Table continues…

Key	Description
Enter	Exit edit mode.
OK	Exit edit mode.
BkSpc	Backspace: delete highlighted characters or character to the left
Clear	Clear input field.
Cancel	Exit edit mode without saving changes.

Table 17: Provisioning parameters legend

Configuration menu item	List each configuration parameter in the order it appears in the menu.
Options or input	Lists every choice available for the parameter and the minimum and maximum number of characters or digits allowed.
Dependency	Show any dependency that controls when that option is enabled or can be used. If the prompt has a dependency, the dependency appears on the same line as the prompt, and input options start on the next line of the table. If an option has a dependency, the dependency appears on same line as the option and applies only to that option. If both the prompt and the option have dependencies, they are cumulative between the prompt and the option and is used to show multiple dependencies.

The parameters list in order of appearance.

Config option	Options or input	Description
Enable 802.1x (EAP)	MD5	MD5 encryption.
	PEAP	PEAP encryption.
	TLS	TLS encryption.
ID 1	4 to 8 characters	EAP ID.
ID 2	4 to 8 characters	EAP ID.
Password	4 to 12 characters	EAP password.
Enable 802.1ab (LLDP)	Checked	LLDP enabled.
	Unchecked	LLDP disabled.
Enable IPv6	Checked	IPv4 and IPv6 enabled (dual-mode).
	Unchecked	IPv6 disabled.
DHCP	Yes	DHCP used.
	No	Static IP and config used.

Table continues…

Config option	Options or input	Description
Phone IP	IP address	IPv4 and IPv6 IP address. **Note:** Maximum of 2 Phone IP addresses can be configured (1 IPv4 and 1 IPv6).
Net Mask	Subnet mask	IP Deskphone subnet mask. **Note:** IPv6 does not support Net Mask, however Net Mask is required for the IPv4 address in a dual mode.
Gateway	IP address	IP Deskphone gateway IPv4 and IPv6 IP address.
DNS IP1	IP address	DNS server 1 IPv4 and IPv6 IP address. **Note:** Maximum of 2 DNS IP addresses can be configured.
DNS IP2	IP address	DNS server 2 IPv4 and IPv6 IP address.
SIP Server IP	IP address	SIP proxy server IPv4 and IPv6 IP address. **Note:** Maximum of 2 SIP proxy IP addresses per domain can be configured.
CA Server	IP address	Certificate Server IP address.
Domain Name	4 to 12 characters	IP Deskphone domain name.
Hostname	4 to 12 characters	IP Deskphone host name.
Ntwk Port Speed	Auto	Auto sense.
	10BT	Forced 10BT.
	100BT	Forced 100BT.
Ntwk Port Duplex	Auto	Auto negotiate.
	Force Full	Forced full duplex.
	Force Half	Forced half duplex.
Enable Voice 802.1Q	Checked	802.1Q header and features used.
	Unchecked	802.1Q not used.

Table continues…

Config option	Options or input	Description
Voice VLAN	No VLAN	VLAN not used.
	Auto	All telephony traffic transmitted on the telephony port is forwarded untagged. Includes: • DHCP—VLAN ID from DHCP Auto VLAN • LLDP VLAN Name—VLAN ID from LLDP VLAN Name TLV • LLDP MED—VLAN ID from Network Policy Discovery TLV.
	Manual	VLAN ID entered 1 to 4094.
VLAN Filter	checked	Filter frames without Voice VLAN tag.
	Unchecked	Process all frames.
Voice Control pBits	Auto	Use value from received LLDP Network Policy TLV, SIP, or default value of 1.
	0 to 7	Force signalling related priority bits to chosen value.
Voice Media pBits	Auto	Use value from received LLDP Network Policy TLV, SIP, or default value of 1.
	0 to 7	Force media related priority bits to chosen value.
DSCP	0 to 63	: DSCP marking to be applied to IP packets for QoS classification.
Avaya Auto QoS	Checked	Enable automatic QoS provisioning by Avaya applications.
	Unchecked	Disable automatic QOS provisioning by Avaya applications.
Enable PC Port	Checked	PC port active.
	Unchecked	PC port disabled.
PC Port Speed	Auto	Auto sense.
	10BT	Forced 10 BT.
	100BT	Forced 100 BT.
PC Port Duplex	Auto	Auto negotiate.
	Force Full	Forced full duplex.

Table continues…

Config option	Options or input	Description
	Force Half	Forced half duplex.
Enable Data 802.1Q	Checked	802.1Q header and features used.
	Unchecked	802.1Q not used.
Data VLAN	No VLAN	Data VLAN not used.
	Enter VLAN ID	VLAN ID entered 1 to 4094.
Data Priority bits	Auto	Use value from the info block or default of 7.
	0 to 7	Force all priority bits to chosen value.
PC-Port Untag all	Checked	Removes the 802.1Q header from a packet before it forwards to the IP Deskphone PC port.
	Unchecked	Leave 802.1Q header on packets destined to the PC port.
Cached IP	Checked	Last IP Deskphone IP address info received is used if DHCP server not reached.
	Unchecked	Must receive response to assign IP Deskphone IP address.
Ignore GARP	Checked	IP Deskphone ignores Gratuitous ARP requests.
	Unchecked	IP Deskphone responds to Gratuitous ARP requests.
Provisioning	Server URL	Provisioning server IPv4 or IPv6 IP address. **Note:** Maximum of 1 Provisioning Server IP address can be configured.
	Protocol: • TFTP • FTP • HTTP • HTTPS	Provisioning protocols. **Note:** If IPv6 is enabled, only FTP protocol can be used.
	Device ID	ID used by provisioning server to authenticate the IP Deskphone. Enter the User ID as the Device ID. TFTP does not require Device ID.

Table continues…

Config option	Options or input	Description
	Password	Password used by provisioning server to authenticate the IP Deskphone. Maximum number of characters is 99.
PVQMon IP	IP address	PVQM server IPv4 or IPv6 IP address. **Note:** Maximum of 1 PVQM server can be configured.
NAT Traversal	NAT Signal • None • STUN	NAT method for SIP signaling. **Note:** IPv4 mode only (IPv6 disabled).
	NAT Media • None • STUN	NAT method for media signaling.
	NAT TTL (sec)	Value from 0 to 65535.
STUN S1 IP	IP address	IP address of STUN S1 device.
STUN S2 IP	IP address	IP address of STUN S2 device.
Media Security	Enable SRTP	SRTP enabled.
	SRTP Mode • BE-Cap Neg • BE-2M Lines • SecureOnly	SRTP configuration values.
	Cipher1 • AES_128_SHA1_80 • AES_128_SHA1 32	Preferred order for SRTP cipher offers.
SIP UDP Port	Integer	Value from 1024 to 65535.
SIP TCP Port	Integer	Value from 1024 to 65535.
SIP TLS Port	Integer	Value from 1024 to 65535.
Connection Timers	OS keep-alive	
Keep-Alive	Integer	Value from 5 to 1800.
Register Retry	Integer	Value from 30 to 1800.
Register Max Retry	Integer	Value from 600 to 1800.
Login Notify	Off	Configuration values for login banner notification.
	Success	

Table continues…

Config option	Options or input	Description
	Failure	
	Both	
Login Notify With Time	Checked	Configuration values for login banner with time notification.
	Unchecked	
Enable Bluetooth (1120E/1140/1165E only)	Checked	Bluetooth is enabled.
	Unchecked	Bluetooth is disabled.
SSH-SFTP	Checked	SSH-SFTP is enabled.
	Unchecked	SSH-SFTP is disabled.
Enable SSH	Checked	SSH is enabled.
	Unchecked	SSH is disabled.
UserID	Maximum of 11 characters	
Password	Maximum of 11 characters	
Enable SFTP	Checked	SFTP is enabled.
	Unchecked	SFTP is disabled.
Enable FIPS	Checked	FIPS is enabled.
	Unchecked	FIPS is disabled.

Parameter source precedence rules

The 1100-series SIP IP Deskphones can obtain provisioning information from many sources at various times. A precedence rule can resolve the possible conflict when different values are specified in various sources for one parameter. The IP Deskphone considers the obtained parameters in the following priority, from highest to lowest:

- Manual provisioning
- Automatic provisioning using 802.1ab switch (LLDP)
- Automatic provisioning using DHCP, including Provisioning Info Block data from the Nortel-SIP-Phone-B or Nortel-SIP-Phone-A DHCP options
- Automatic provisioning using TFTP/HTTP/HTTPS downloaded configuration files
- Last auto received value
- Factory default

Provisioning information from a provisioning source with high priority can overwrite the provisioning information from a provisioning source with low priority. The manual provisioning has highest priority. The other provisioning sources are auto-provisioning sources. Automatic provisioning defines provisioning control for each parameter. You can either manually or automatically provision each parameter. Each provisioning parameter provides an attribute that specifies if the parameter was previously provisioned manually or automatically.

The default value of the stickiness attribute is AUTO. If the provisioning parameter is AUTO, the IP Deskphone can receive the value from automatic provisioning sources based on the precedence rule. If you manually change the parameter, the attribute value is MANUAL. If the attribute is MANUAL, the provisioning information from automatic provisioning sources is ignored, except for the standard DHCP parameters. The AllAut softkey in the Device Setting’s Auto dialog will return all parameters to AUTO. The Set to Factory Default function returns all parameters to AUTO as well as resetting their value to the factory default value.

If you enable DHCP, then the IP address, the subnet mask, and the default gateway, which the IP Deskphone obtains from the DHCP server, overwrites the manually configured value. The value for EAP device ID and password can also overwrite the manually configured value. If you configure stickiness and the current provisioning source does not provide the provisioning information for the particular parameter, the last received provisioning value is used.

Chapter 11: Features

This chapter describes the features that are supported on the Avaya 1100 Series IP Deskphones with SIP Software.

Voice Quality Monitoring

Feature overview

Proactive Voice Quality Monitoring (PVQMon or VQMon) allows the IP Deskphone with SIP Software to report voice quality statistics to a server in the network. The IP Deskphone with SIP Software collects various voice quality statistics, for example, packet loss, and sends the voice quality statistics to the server at regular intervals during a call. A subset of these statistics is also available for the user to view on the IP Deskphone by selecting the **Audio** soft key and then the **Monitor Audio Quality** menu item.

VQMon set-up

Configure the following parameters on the IP Deskphone with SIP Software to connect to the server and send the PVQMon statistics.

1. Enable the feature. To enable the feature, configure the VQMON_PUBLISH parameter in the device configuration file (see VQMon configuration commands on page 117).
2. Configure the IP address of the PVQMon server. Configure the IP address of the PVQMon server in either of the following settings:
    a. Configure VQMON_PUBLISH_IP through the device configuration file (see VQMon configuration commands on page 117).
    b. Configure PVQMon IP in Device Settings (see Manual provisioning parameters on page 157)
3. Configure the remainder of the VQMon parameters in the device configuration file (see VQMon configuration commands on page 117). These parameters provide threshold information to the IP Deskphone with SIP Software. A report is sent to the server when these thresholds are exceeded.

Server set-up

The IP Deskphone with SIP Software works with Telchemy server software. The name of the software is SQmediator and is available through Telchemy (http://www.telchemy.com). The minimum version required is release 1.0.

How VQMon works

The IP Deskphone with SIP Software gathers statistics about the current call when VQMon is enabled. Statistics are also gathered regarding the quality metrics of the current call. The call-related statistics contain condensed information about the SIP Session Description Protocol (SDP), the Call ID, the local and remote address, voice quality-related statistics, Zulu times for start-time and the time the report was sent.

The voice quality-related statistics include jitter, packet loss, delay, burst gap loss, listening R-factor, R-LQ, R-CQ, MOS-LQ and MOS-CQ. See Table 18: Glossary of RTCP XR metrics on page 166. More information on each of these metrics is provided in RFC3611 “RTP Control Protocol Extended Reports (RTCP XR)”.

When the IP Deskphone detects that a particular voice quality metric has exceeded a threshold (defined in the device configuration file), the IP Deskphone sends a message to the server indicating that there is an issue. If the issue persists, then the IP Deskphone reports another message at regular intervals indicating that there is an exceeded value. This happens continuously until the voice quality metric falls below the threshold value. As well, the IP Deskphone can send regular reports of the voice quality at time intervals defined in the device configuration file.

Table 18: Glossary of RTCP XR metrics

Metric	Description
Burst	A period of high packet losses and / or discards. A burst is calculated in milliseconds.
Conversational R-factor	Voice quality metric based on burst packet loss and vocoder selection.
Delay	One way delay which includes end-to-end delay, jitter buffer delay and packetization delay. Delay is calculated in milliseconds.
Inter-arrival jitter	The variation in packet arrival times due to transmission (routing, queuing delay) through the network. Jitter is calculated in milliseconds.
Listening R-factor	Voice quality metric based on burst packet loss, transmission delay and burst loss.
MIU	Media Information Unit. MIU is a concept from VQMon. An MIU can be any size down to a 10

Table continues…

Metric	Description
	millisecond (8 sample) block. An MIU means a frame in the i200x implementation.
MOS	Mean Opinion Score. A subjective measurement of the voice quality of a voice call.
MOS_CQ	The VQMon conversational quality MOS score calculated for a call channel.
MOS_LQ	The VQMon listening quality MOS score calculated for a call channel.
Packet loss rate	The percentage of total packets loss versus packets received.
R-factor	A measurement of voice quality based on network impairments including burst packet loss, delay and encoding/decoding algorithm selection.

End of call report

The IP Deskphone sends a report using VQMON Publish message to the proxy. The proxy redirects the publish ID described within the report. An end-of-call report is always generated if VQMON is enabled. IP Deskphones do not negotiate or exchange messages with the device defined using PUBLISH_IP options.

Session interval report

The IP Deskphone can send voice quality reports at time intervals defined in the device configuration file. The minimum and default time interval is 60 seconds. If the IP Deskphone sends session interval reports more frequently, then a threshold violation has occurred.

Alert interval report

When an IP Deskphone detects that a voice quality metric has exceeded a threshold, then the IP Deskphone initiates a timer which sends a message to the server every 5 seconds. When all voice quality metrics fall below the threshold values, the IP Deskphonestops sending VQMON Publish messages with the report. The alert interval report does not differ from the session interval reports or end-of-call reports.

Multiuser

The Multiuser feature allows multiple SIP user accounts to be in use on the IP Deskphone at the same time. Multiple users, each with their own account, can share a single IP Deskphone allowing each user to receive calls without logging off other users. One user can have multiple user accounts (for example, a work account and a personal account) active at the same time on the same IP Deskphone. You can register each account to a different server, and for each account, the IP Deskphone exposes the functionality available to that account.

One account is considered a primary account and is used by default for most IP Deskphone operations. Each account is associated to a line key; the primary account is always on the bottom right line key of the IP Deskphone (this is the first key, Key 01), and an arbitrary key (including a key on an Expansion Module) can be selected for additional accounts.

You can use the line key to do the following:

- start dialing
- place a call using the corresponding user account
- to answer an incoming call targeted to that account

Initiating a call without pressing a line key (for example, by dialing digits at the idle screen and lifting the handset) uses the primary account.

A running IP Deskphone is associated to a single profile that represents one configuration of the IP Deskphone with all relevant persistent data such as preferences and call logs. A different profile is associated to each account used as a primary account. The IP Deskphone can store up to five different profiles; the IP Deskphone takes data from the profile associated to the current primary account. A number of configurations are independent of profiles and tied directly to an account making them available to that account regardless of the primary account you use (for example, voice mail ID).

The IP Deskphone receives and answers calls targeted at any of the registered accounts; the incoming call screen indicates who the call is for. You can place an outgoing call using any of the accounts; the account that you use is displayed on the dialing screen. When a call is active, information from both local and remote parties appear on the screen.

Regardless of which account receives the call, incoming call logs, outgoing call logs, and instant messages appear in a single list. The IP Deskphone indicates the local user in the detailed view of the entry.

Some features are only available to the primary account, such as instant messaging, retrieving parked calls by token, and establishing ad-hoc conference calls.

If you log off of the primary account, the IP Deskphone unregisters all other accounts at the same time. These accounts are registered automatically after you log on the primary account (it is possible to use a different primary account to log on) again. When the IP Deskphone restarts, all accounts that were logged in before the IP Deskphone restarted, are automatically logged back on. The provisioning server can also configure the users who are allowed to log on to the IP Deskphone.

Configuration

Depending on server policy, the Multiuser feature can require you to configure the **PROMPT_AUTHNAME_ENABLE** value to **YES** in the device configuration file. This enables a prompt that requires you to enter an Authentication ID that is different from the Login ID. For example, CS 1000 requires an Authentication ID to find a corresponding TN and a Login ID to find a key; enabling **PROMPT_AUTHNAME_ENABLE** creates a prompt for the authentication ID.

When you configure Multiuser, consider the following parameters:

- **MAX_LOGINS** represents the number of user accounts that can log on at the same time. Configure **MAX_LOGINS** to any value greater than one; the default is 24.

- Configure **DOD_ENABLE** to **NO**; a secondary user cannot log on if **DOD_ENABLE** is enabled. The default value is **NO**.
- The **SELECT_LAST_INCOMING** parameter determines call selection when multiple calls are in the **Ringing** state. If you configure **SELECT_LAST_INCOMING** to **NO**, the first selected call remains the selected call as new calls are added to or drop from the list of ringing calls. If you configure this value to **YES**, the selected call becomes the ringing call last added to the list. The default value is **NO**.

Initial logon

To log on for the first time, you must enter a user name and password, and specify if the logon is permanent or not. On the logon screen, you can choose which domain you want to access, and change the language you want to use. You can use the Domain key only to select a domain from the configured list; you cannot modify domains.

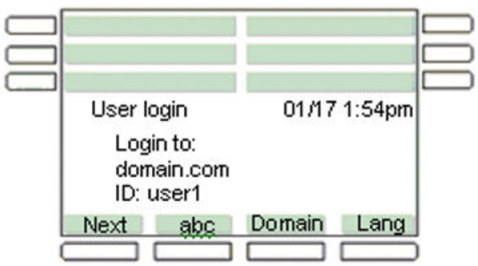


Figure 10: Primary logon screen

After you log on, the idle screen appears on the IP Deskphone. If there is no profile for the primary account, the IP Deskphone automatically creates a profile. You can create up to five profiles. If you exceed the limit of five profiles, the IP Deskphone automatically deletes the least recently-used profile.

Similarly, configurations for each user of the primary account are loaded after a user logs on to the IP Deskphone. The configurations are independent of the profile; if the account you use is registered as the secondary account (not the primary account), then the IP Deskphone uses the configurations of the primary account. The IP Deskphone keeps up to 24 sets of configurations (one set for each user). If you exceed the limit of 24 sets of configurations, the IP Deskphone automatically deletes the least recently-used set, and a new account is registered.

Additional logons

The Login command in the System menu allows you to register additional accounts. If you log on as a secondary user, you cannot change the language selection.

The following figure shows the secondary logon screens.

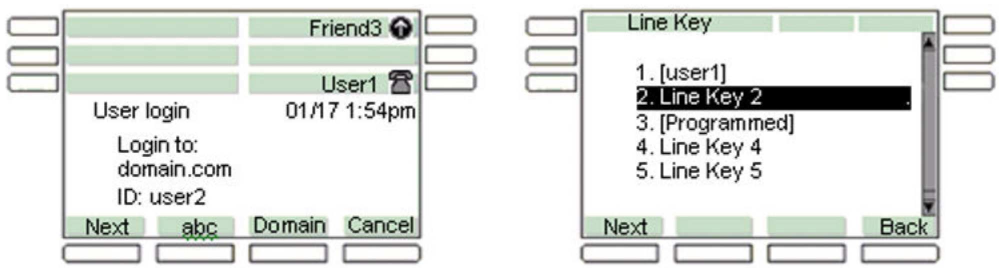


Figure 11: Example of secondary logon screens

You can specify a Line Key for a new account. By default, the IP Deskphone selects the first unused key. If the IP Deskphone reaches the configured limit on concurrent logons and you select the **Login** command, an error message appears.

During the logon operation, a `Logging in user` message appears on the IP Deskphone screen. The IP Deskphone can receive calls for user accounts that are registered; however, other features are not available until the logon process is complete. The IP Deskphone does not display a profile selection prompt and does not create a profile for the secondary account.

Automatic logon

Use the following configuration options to determine the behavior of the automatic logon feature:

- **`AUTOLOGIN_ENABLE NO (or 0)`**: This configuration requires you to enter the Login ID, Authentication ID, and password for each user every time there is a restart of the IP Deskphone.
- **`AUTOLOGIN_ENABLE YES (or 1)`**: If the IP Deskphone is switched off, you are automatically logged back on when you restart the IP Deskphone. If multiple users are logged on when the IP Deskphone is switched off, the IP Deskphone automatically logs all users back on when you restart the IP Deskphone.
- **`AUTOLOGIN_ENABLE USE_AUTOLOGIN_ID (or 2)`**: You do not enter user credentials; the system administrator pre-configures the IP Deskphone using an IP Deskphone-specific file. The following example shows a SIP provisioning file:

`[USER_CONFIG]`
`DOWNLOAD_MODE FORCED`
`VERSION 000001`
`PROMPT NO`
	IP Deskphone-specific configuration file

`AUTOLOGIN_ID_KEY01 8010@avaya.com`
`AUTOLOGIN_AUTHID_KEY01 user1`
`AUTOLOGIN_PASSWD_KEY01 1234`
 	
`AUTOLOGIN_ID_KEY02 8050@avaya.com`
`AUTOLOGIN_AUTHID_KEY02 user1`
`AUTOLOGIN_PASSWD_KEY02 1234`
	The IP Deskphone uploads a phone-specific file in the format SIP{MAC Id}.cfg

Logging off

The Logout command in the System submenu, prompts you to select an account, asks for confirmation, and then proceeds to log off the account. Logging off an account frees the corresponding Line key and does not require a password.

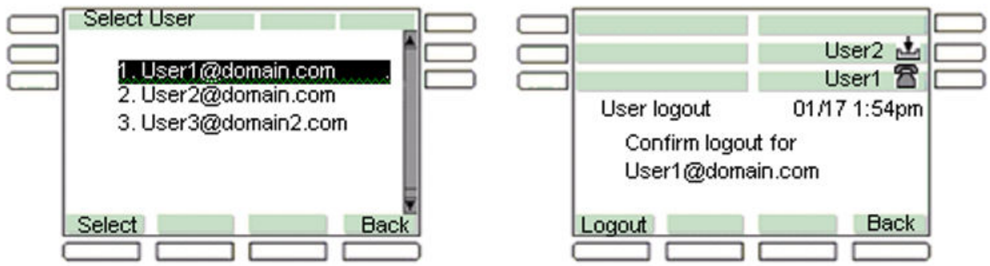


Figure 12: Example of log off screens

Consider the following when logging out of an IP Deskphone:

- Unless the parameter LOGOUT_WITHOUT_PASSWORD is set to YES (default is NO), the phone prompts you for the User Password before logging off an account. When there are multiple accounts logged in and the “All accounts” option is chosen, the administrative password must be entered.
- The administrative password can be entered instead of the user password to log off an individual login account.

Primary account logout

Logging off the primary account causes all other accounts to log off automatically and the IP Deskphone to display the logon screen. The IP Deskphone logs back in the secondary accounts automatically after you register a new primary account or the same primary account.

If you restart the IP Deskphone after you logged off the primary account, the logon screen appears on the IP Deskphone. Logging on a new primary account leads to automatic logon of the secondary accounts.

The list of programmed feature keys is part of the IP Deskphone profile. Logging off one primary account and logging on a different account can change the set of feature keys. If a secondary account is assigned to a key that is also in the new set of feature keys, the secondary account takes precedence; the secondary account is logged on and the feature key acts as a Line key. If the account is logged off manually, the programmed feature key becomes available.

Secondary account logout

If you log off a secondary account by selecting the secondary account in the **Logout Select User** screen, the IP Deskphone removes the secondary account from the autologon list. After you restart the IP Deskphone, the IP Deskphone does not log on the secondary account.

Server failover

If the connection to your account proxy is lost, the IP Deskphone notifies your account and periodically attempts to reconnect. Some features, such as incoming calls, remain accessible for other accounts, but other features are not available until connection is reestablished or you cancel the reconnection. Cancelling the connection to your account is the same as logging off. If you are using the primary account, the IP Deskphone returns you to the initial logon screen. If you are using a secondary account, that secondary account is removed from the list of secondary accounts that are logged on automatically.

If more than one account loses connection, the IP Deskphone attempts to reconnect to each account in sequence. The IP Deskphone tries to reconnect the first account to lose connection until that account reregisters or you cancel the attempt. Then the IP Deskphone attempts to reconnect the next account that lost connection. Cancelling the reconnection of the primary account immediately abandons reconnection of all other accounts, logs off secondary accounts that are still connected, and returns the IP Deskphone to the logon screen.

The IP Deskphone uses a single logon queue for automatic logons and failover. This means that if automatic logons are still pending when an account cannot connect, a reconnection attempt for that account can only begin after all automatic logons are complete or cancelled.

Cable unplugged

If the IP Deskphone detects that the network cable is unplugged while accounts are logged on, the IP Deskphone assumes that all accounts have lost their connection to the server. When the cable is reconnected, the IP Deskphone proceeds to reregister all accounts, starting with the primary account.

Line keys

Each registered user is associated to a separate line key. Each line key displays the name of the registered account and some basic state information for the account.

The primary account is associated to the first bottom-right line key of the IP Deskphone. If you are using a secondary account, the order of the next available line key is from bottom to top and right to left on the IP Deskphone, followed by the keys on the Expansion Module from bottom to top and right to left. You can select a different available line key for secondary accounts during the logon process.

The following figure is an example of the IP Deskphone with and Expansion Module and multiple accounts.

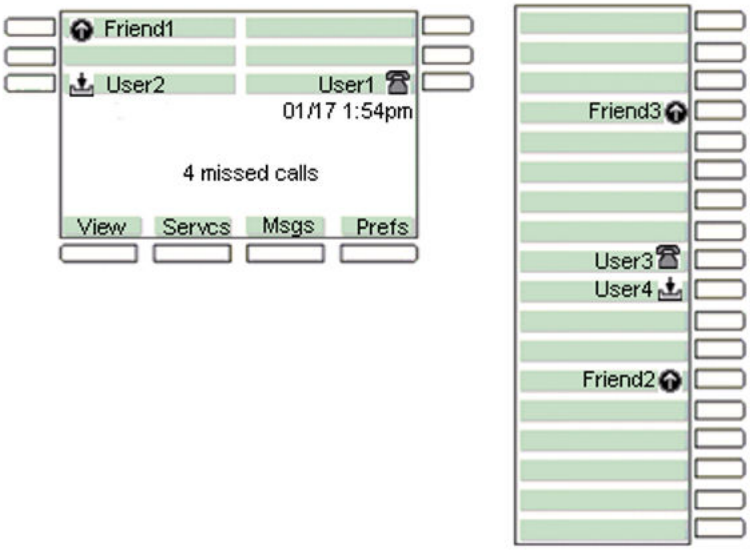


Figure 13: IP Deskphone with Expansion Module and multiple accounts

Pressing a line key brings up a dialing prompt, initiates a call to a preselected target, or answers an incoming call. See Making a call on page 173.

At select account prompts, such as the Logout screen or User Settings screen, pressing a line key highlights the corresponding account. See Account selection on page 181.

The icon for each line key reflects the state of the account associated with that line key.

- If there is a call for the account, a phone icon displays the state of the call, such as when the call is on hold or is ringing.
- If there is more than one call, the state of the most active call is displayed.
- Missed incoming calls and new voice mail messages for the account are indicated with an icon. The icon supplements the `NN missed calls` message on the idle screen and the red LED which cannot provide per-account information.
- The MADN, do-not-disturb, and call forwarding features also affect the appropriate line key icon of the account.

Making a call

You can place a call using any of the registered user accounts. The account that you select determines:

- the proxy used
- the domain name used for the call target (if none was specified)
- the caller the target sees is calling
- the service-package-dependent features that are available

Receiving a call

When you receive an incoming call, the account that the call is intended for is displayed on the IP Deskphone. The line key of that account displays the icon for an incoming call. You cannot use a different account to answer the call.

If you are receiving multiple calls at the same time, a list of all active and incoming calls appears. If you select a specific call in the list, you can choose to answer or process that specific call. The IP Deskphone sorts the list by the most recent incoming call first. If there are numerous calls to process, you can configure the selected call to automatically select the last incoming call to make it easier to answer, or to leave the selected call static. The selected call does not jump as new calls come in, but remains on the same call, as new calls are added, to make it easier for the user to process that call.

If the calls are for different accounts, the line keys associates with the accounts receiving the incoming calls display an incoming-call icon.

Being in a call

When a single call is active, the screen displays the local account in use and the remote user. If multiple calls are active, each call appears on a single line. The local account for the active call appears on the context line. Each line key reflects the most active call state of the account the line key is associated with.

The active call is affected by operations such as transfer or call parking. One exception is the New Call action which uses the primary account by default, but can be overridden by pressing another line key to initiate a call.

You can use your account to transfer or park an active call that is received on that account. The exception is the New Call action because it uses the primary account by default. You can override the New Call action by pressing another line key to initiate a call.

Joining calls into an ad-hoc conference always uses the conference server of the primary account. Calls that are on accounts that cannot access the server cannot be joined. After you create an ad-hoc conference, you can join additional calls into the same conference. You cannot create more than one ad-hoc conference at a time.

You can join any two calls with the 3-way call feature, regardless of the account. The service package of the account to which a call is associated determines which operations, such as Call Park, are available on that call. After you establish a 3-way call, the join functionality becomes unavailable until the 3-way call is terminated.

The following figure is an example of the IP Deskphone with one call.

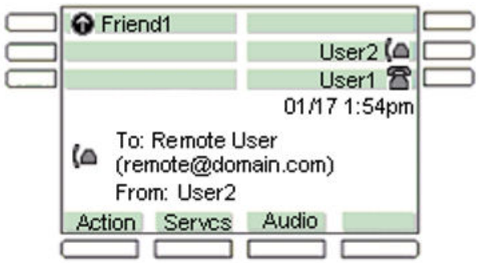


Figure 14: Example of the IP Deskphone with one call

The following figure is an example of the IP Deskphone with multiple calls.

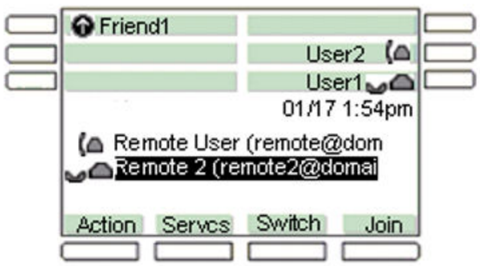


Figure 15: Example of the IP Deskphone with multiple calls

Instant messages

You can only receive or send instant messages from the primary account. Incoming messages for secondary accounts are rejected, are not displayed on the screen, and are not added to the instant message logs.

Menu features

The menus displayed on the IP Deskphone are customized to match the service package of the active account that is accessing the menu. Menus are accessed from the Idle screen when the primary account is active. For example, you can only use the Retrve Context-sensitive soft key to retrieve a parked call if call parking is allowed by the service package of the primary user.

Similarly, accessing the Address Book through the Directory hard key displays the Address Book of the primary account. However, accessing the address book in select mode (for example, while dialing or selecting an item for a speed dial key) accesses the address book of the user account that is in use on the address-input screen.

Modifying settings

Preferences, such as Voice Mail and IM settings, are available for each account. The main Preferences menu includes a **User Settings** entry. If you select **User Settings**, you are prompted to select a registered account. After you select a registered account, a menu appears that lets you modify the settings of the account you selected.

Per-account call notification options

The Call Settings entry in the User Settings menu provides you with a number of configuration options relating to how incoming calls for a particular account are treated.

The configuration options are:

- what kind of audio alert you want to use (ring tone, beep, or nothing)
- whether you want the red LED to blink
- whether you want the call to be added to the Incoming Call logs

IM Settings

IM Settings is located in the User Settings menu. Any change in settings on the primary account takes effect immediately. You can also modify settings for a secondary account, but the modifications do not take effect until you register the secondary account as the primary account.

Voice Mail settings

Voice Mail Settings is located in theUser Settings menu. You can program different voice mail addresses and IDs for each account. To access the voice mail of a secondary account, press the line key of the secondary account to obtain a dial prompt, and then press the VMail Context-sensitive soft key.

Waiting messages are reported in the following two ways:

- The red LED lights up if any account has a waiting message.
- A shaded envelope icon appears on the line key of each account that has a waiting message (unless the account is in a call).

Remembering settings after logout

The IP Deskphone remembers up to 24 sets of configurations for each profile. If you configure settings for an account and you log off the account, the settings are restored after you log back onto the account (as either a primary account or a secondary account).

If you log on an account that you did not save the settings in a profile for, the IP Deskphone creates a new set of default settings for that account. If there are already 24 sets of configurations in the profile, the IP Deskphone discards one set that is not currently registered with the account, and replaces the discarded set with the new set that is saved in the account profile.

Programmable keys

You cannot use a line key associated with a registered account for programmable features. The Program Key screen lists all the line keys associated to an account. If you select a line key associated to an account, an error message appears.

The Do Not Disturb, Call Forward, and Presence keys are associated to a specific user account that you create, and determine which account status to affect. See User status on page 178.

By default, pressing a Speed Dial programmed key initiates a call using the primary account. If you press a line key to obtain a dialing prompt, and then press a speed dial key, the IP Deskphone uses the account associated with that line key. When accounts are registered on different domains, you can program and use speed dial keys with targets that are only reachable on the domain of a secondary account.

Important:

The Speed Dial keys always use the primary account to determine the presence state of the target.

The Instant Message keys always use the primary account, because IM support is disabled for secondary accounts.

Inbox, outbox, and instant message log

Each profile has a single inbox, a single outbox and a single instant message log. The detailed view of the call log entry indicates the local account associated to each entry; that is, the source of outgoing calls and the target of received call.

The following figure is an example of the Inbox call details view.

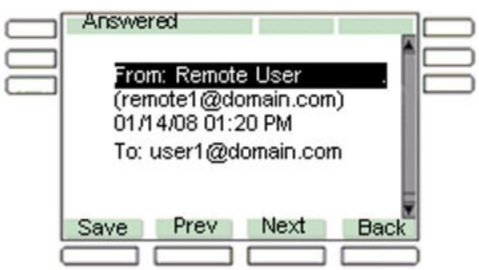


Figure 16: Example of the Inbox call details

Call logs and IM logs provide many ways of initiating a call to the address identified by the selected entry, such as lifting the handset. In most cases, the primary account is used. However, if you press a line key to initiate the call, the call uses the account associated with the line key.

If call logs and IM logs are invoked in the **selection** mode, you cannot initiate a call directly because the **Select** soft key populates a dial prompt or other input field with the selected target. The operation already in progress determines which account you can use.

For example:

If you press the line key to obtain a dial prompt, press the **Inbox** key to select a target, press **Select**, and then press **Send**; the line key that you originally pressed determines the account you can use.

Address Books with Multiuser

Each registered account can have a network-based Address Book. Each profile contains a local Address Book that is independent from all network Address Books.

Accessing the Address Books, by pressing the **Directory** hard key from the Idle screen, displays the Address Book of the primary account. If the primary account does not have a network Address Book, the local Address Book is accessed.

Accessing the Address Book in **Selection** mode always accesses the Address Book of the current account. For example, after obtaining a dial prompt by pressing Line Key 2, you can press the Directory key to access the Address Book of the account associated to Line Key 2. You can access the network-based directory of the appropriate account if it is available; otherwise, the IP Deskphone accesses the Address Book.

You can only access the network-based Address Book of secondary users in Selection mode. You cannot modify the Address Book of a secondary account on the IP Deskphone. However, modifications that you make to the Address Book remotely, such as using a different client of the Personal Agent, are reflected on the IP Deskphone.

The local Address Book is shared by all accounts that do not have a network-based Address Book. You can modify the local Address Book if the primary account does not have a network-based Address Book. Changes to the network-based Address Book of the primary account are not reflected in the local Address Book.

If you use the Friends view, you can always access and modify the Address Book of the primary account (local or network-based). There is no Selection mode for the Friends view. You can only monitor and view the presence information of Friends of the primary account in the Friends view.

User status

The features associated with the User status include the following:

- Do Not Disturb
- Call Forwarding
- Presence

Do Not Disturb

Selecting the Do Not Disturb (DND) command from the Services menu prompts you to specify which account you want to place in the DND mode. The option **all** allows you to place all accounts in the DND mode (the all option is highlighted by default). By selecting an option, the IP Deskphone prompts you to confirm the operation before proceeding.

Activating DND for a specific account automatically causes calls to that account to be rejected with a busy signal. However, the IP Deskphone can still receive calls to other accounts. After DND mode is active for an account, the label of the account line key periodically displays a DND indicator.

The following scenarios apply to DND.

- If you select a single account that is in DND mode, the IP Deskphone displays a prompt that asks if you want to deactivate the DND mode.
- If you select a single account that has Call Forwarding active, an error message appears to indicate that DND cannot be activated.
- If you select the option **all**, and at least one account is not in DND mode, DND mode is activated for all accounts. If an account is in Call Forward mode, Call Forward is disabled.
- If you select all and all accounts are in DND mode, DND mode is deactivated for all accounts.

If you use a programmed DND feature key, the account that is affected by the DND feature key is determined when the feature key is configured. After you press the DND feature key, the IP Deskphone behaves as described in the preceding scenarios, except that there is no confirmation prompt displayed. The IP Deskphone performs the operation immediately, and a message appears to indicate what was done.

The DND mode for each account is persistent. If you restart the IP Deskphone, or log off the account and log the account back on, the account maintains the original state.

Call Forwarding

After you select the Call Forward command from the Services menu, the IP Deskphone prompts you to specify the account that you want to place in Call Forward mode. The option **forward all** places all accounts in Call Forward mode in one operation, and the option **forward none** deactivates Call Forward for all accounts at the same time.

The following scenarios apply to Call Forward:

- If you activate call forwarding for a specific account, the IP Deskphone automatically redirects all calls to the selected account to the address that you specify. The target address must be reachable from the domain of the account. Other accounts can still receive calls. The line key label periodically indicates that Call Forward mode is active.
- If you select a single account that does not have Call Forward or DND active on it, the IP Deskphone prompts you to specify a forwarding target, and the mode you select is then enabled. If DND is already active, a message appears indicating that Call Forward cannot be activated. If Call Forward is already active, a message appears asking you if you want to deactivate Call Forward.
- If you select the **forward all** option, all accounts are in Call Forward mode using the provided target, and DND is deactivated for all accounts. If accounts are already in Call Forward mode for a different target, the accounts are updated to use the new target.
- If you select the **forward none** option, the Call Forward feature is deactivated for all accounts for which the Call Forward feature is currently active.

After you press a single account Call Forward programmed key:

- If the account is already forwarding calls to the programmed target, call forwarding is deactivated.

- If the account is not forwarding calls to the programmed target, the account is set to forward calls to the given target, disabling DND if necessary, and overriding any other call forward target that is active for the account.

After you press a forward all programmed key:

- If all accounts are already set to forward calls to the key target, call forward is disabled for all accounts (behaves like the **forward all** option).
- If all accounts are not configured to forward calls to the key target, call forwarding is activated for all accounts using the key target (behaves like the **forward none** option).

If you do not perform any Call forwarding or DND operations, you can press the **single** and **all** keys to switch one or all accounts between **forwarding to key's target** and **not forwarding** states.

The Call Forward mode and target is persistent for each account. If you restart the IP Deskphone, or log off the account and log the account back on, the account maintains the original state.

Presence

After you select the Presence command from the Services menu, you are prompted to specify which presence state of the account you want to modify. The **all** option lets you set all accounts to the same presence in one operation.

If you select a single account, the current state of the account is displayed. You can change the current state of the account by entering the new presence state and note. After you confirm the operation, the new presence state is applied.

If the **all** option is selected, no current state is displayed, and you are immediately prompted to select the new state. The new state is applied to all registered accounts.

If you use a programmed Presence feature key, the account that is impacted by the Presence feature key is determined after the feature key is configured.

After you press a **single account** Presence programmed key:

- If the account is already set to the programmed presence state, the account is set back to the **Connected** presence state.
- If the account is not already set to the programmed presence state, the account is set to the programmed presence state.

After you press the **all accounts** Presence programmed key:

- If all accounts are already set to the programmed presence state, all accounts are set to the **Connected** presence state.
- If all accounts are not already set to the programmed presence state, all accounts are set to the programmed presence state.

As like the Call Forwarding keys, if you do not perform any Presence operation, you can use the **single** and **all** keys as toggles. However, the presence states are not entirely under your control. Some states are applied automatically (for example, On The Phone), and all states are applied by sending a message to the SIP proxy which can choose to not accept the change. As a result, it is possible for a set all presence operation to not configure all accounts to the programmed presence; if you press the **Presence** key again, another attempt is made to apply the programmed presence to all accounts. It is more effective to program a separate Presence key to set all accounts to the Connected state.

Events that update presence states automatically occur for each account. For example, the On The Phone state is applied to any account that has at least one call active.

Account presence is not retained after logging off or restarting the IP Deskphone.

Notifications

The IP Deskphone can spontaneously display messages on the screen to report events that you did not initiate. This includes events such as failure to retrieve a service package and availability of a new location list.

These spontaneous notifications do not indicate which account is affected by the event. A message appears to indicate the affected account.

The following figure is an example of an account notification.

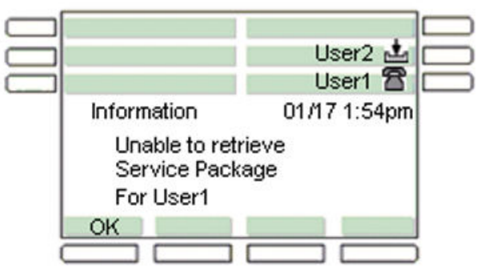


Figure 17: Example of an account notification

It is possible for the same event to occur for multiple accounts at the same time, or in quick succession. In the preceding figure, the accounts are displayed one after the other.

Account selection

There are a number of scenarios where you are prompted to select an account (for example, logoff, per-account settings, programming keys).

The scenarios fall into the following two categories:

- Prompts where you must select exactly one account. If only one account is logged on, the prompt does not appear. The IP Deskphone selects the single account automatically, and immediately displays the next screen. Otherwise, the primary account is always at the top of the list, and is highlighted when the prompt first appears.
- Prompts where an all or none option is available.

Pressing an account line key highlights the corresponding item in the account list. If no selection is made in a certain amount of time, the prompt acts as if you pressed the **Back** context-sensitive soft key, canceling whichever operation required selection of an account.

Feature dependencies and restrictions

The number of line keys on the IP Deskphone limits the number of accounts that you can register simultaneously. The IP Deskphone is limited to six accounts. Connecting an Expansion Module to the IP Deskphone increases the limit by 18, allowing for 24 registered accounts. Additional Expansion Modules do not increase the limit further.

These are hard limits. Further restrictions may be imposed by the administrative policy.

Performance characteristics

Because the multiuser feature can allow the IP Deskphone to have multiple users logged on to the IP Deskphone at the same time, the chances of numerous multiple calls increase. The IP Deskphone can handle five simultaneous incoming calls at a time without any noticeable impact. But as the number of simultaneous incoming calls increase, there is a noticeable delay in ringing and updating the display to present all the calls to the user. It may take up to five seconds for 10 simultaneous incoming calls, and this time increases as the IP Deskphone receives more simultaneous incoming calls.

CS 1000: Several keys with the same DN on a TN

CS 1000 allows you to simultaneously make or receive a maximum of 2 calls. To overcome this limitation you can configure several Multiple Call Ringing (MCR) keys with the same DN on one TN and register from the IP Deskphone to each configured key. This applies to systems using Meridian Communications Adapter (MCA) – Multiple Appearance DN (MADN).

Each registration must have the same Login ID and Authentication ID. The first registration maps to the lowest numbered DN key. Subsequent registrations are assigned DN keys in ascending order of the key numbers.

The following example shows several MCR keys configured on the same DN, on one TN:

```
TN 100 0 0 1
UEXT/SIPL

With:
SIPU user1
SCPW xxxx
KEY 0 MCR 5000
KEY 1 HOT U xxxx
KEY 2 MCR 5000
KEY 3 MCR 5000
```

Multiple Appearance Directory Number

The Multiple Appearance Directory Number (MADN) feature operates differently depending on the type of Communication Server. For instance, the MADN feature operates differently on the Communication Server 2000 than the Communication Server 1000.

Communication Server 1000

CS 1000 Multiple Appearance Directory Numbers (MADN) provides the following features:

- Several devices (TNs) share a common Directory Number (DN).
- When the DN receives a call, all devices ring.
- You can configure two call arrangements; Single Call Arrangement (SCA) and Multiple Call Arrangement (MCA).

Single Call Arrangement

Single Call Arrangement (SCA) MADN allows only a single active call on the DN, regardless of the number of DN appearances:

- A call on a DN appearance makes all other appearances busy (they cannot receive or make calls).
- Activity on one DN appearance reflects on other appearances; this is achieved by using the Event Dialog SIP feature. For more information, refer to RFC 4235.
- SCA MADN provides Automatic Privacy for telephones that share a DN. When a call is in progress on the DN, no other telephone on which the DN appears can bridge into the call, unless the call is put on hold
- Telephones with a Privacy Override Allowed (POA) Class of Service can bridge into an established call on an SCA MADN. However, you cannot bridge into a call until the call establishes.
- Any user with the MADN SCA feature can put a call on hold. Any other user in the group can pick up the held call by accessing the line key with SCA provisioned.
- The state of the user's group is reflected in the line key icon. Three states are available; idle, active, and held. For more information about line key icons, see the applicable IP Deskphone User Guide.

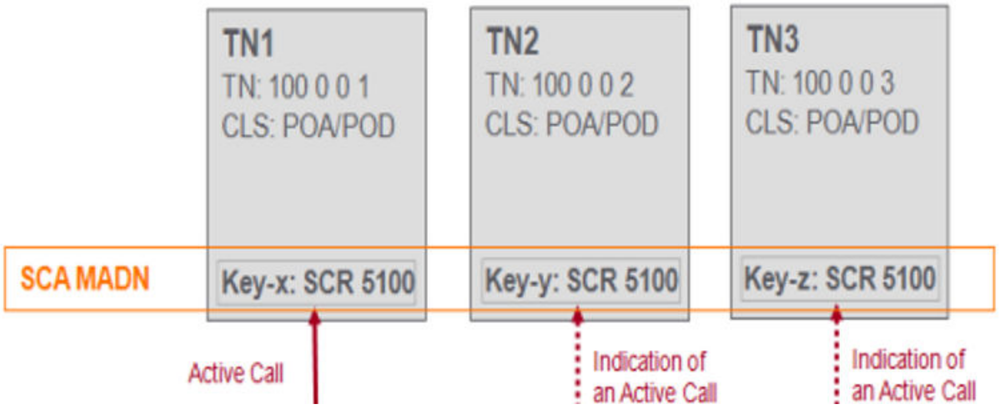


Figure 18: SCA MADN

Multiple Call Arrangement

Multiple Call Arrangement (MCA) MADN allows as in-progress calls as there are appearances of the DN:

- A call on a DN appearance does not make other appearances busy (they can receive or make calls).
- Activity on one DN appearance does not reflect on other appearances.
- There is no simple method for a DN appearance to bridge into or pick up a call on another DN appearance.

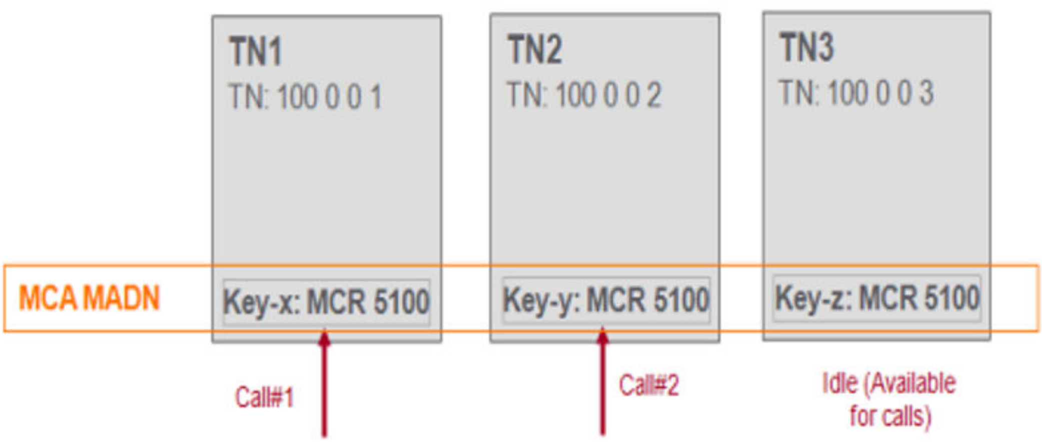


Figure 19: MCA MADN

The MADN SCA feature for CS 1000 requires you to configure PROMPT_AUTHNAME_ENABLE to YES in the device configuration file. This prompts the end user to enter an Authentication ID that is different from the Login ID.

The following example shows a TN configured for SCA MADN:

```
TN 100 0 0 1
UEXT/SIPL

With:
SIPU user1
SCPW xxxx
```

```
KEY 0 SCR 8000
KEY 1 HOT U xxxx
```

The following example shows a TN configured for MCA MADN:

```
TN 100 0 0 2
UEXT/SIPL

With:
SIPU user2
SCPW xxxx
KEY 0 MCR 8001
KEY 1 HOT U xxxx
```

Note:

You must enter 8000/8001 as the Login ID and user1/user2 as the Authentication ID when you register to a corresponding user on an IP Deskphone.

Communication Server 2000 and Communication Server 2100

The Multiple Appearance Directory Number (MADN) feature allows a Directory Number (DN) to appear on more than one IP Deskphone with SIP Software. The MADN with Single Call Arrangement (SCA) feature allows multiple IP Deskphones to appear as a single line to a caller. Any one of the IP Deskphone phones in a group with MADN can initiate or answer a call, but only one call can be active at any given time. Any other user in the group can join the active call by picking up the handset of the IP Deskphone with SIP Software.

With the MADN SCA feature configured on multiple phones of different registered SIP users, the phones share one single DN. An incoming call to this DN causes all the phones in the group to ring.

Any user of an IP Deskphone with the MADN SCA feature can put a call on hold or can prevent others from joining in the active call.

If a user's group is active (as seen by line icon being off-hook) and the user picks up the handset, the user is automatically joined to an ongoing MADN call (unless the server restricts this feature for privacy or other factors).

Vertical services

Vertical services are CS 2000 and CS 2100 features that can be activated or deactivated by dialing a defined code, for example, Privacy. Even though no more than one active session can be established for the MADN SCA group, members of the group can still enter certain vertical services.

Currently, the available vertical service is Privacy.

Privacy

A user can activate the privacy service by putting the current session on hold and dialing the privacy code. The CS 2000 connects the IP Deskphone to the Avaya Media Server (MS) to hear a confirmation for its request and terminates the session. The user takes the original session off hold.

Privacy access codes

The privacy access codes are: PRV, PRLA, PRLC. For example: PRV = 191 PRLA = 192 PRLC = 193 If the initial state of the MADN group is nonprivate , the PRV access code is used to toggle between privacy on and privacy off. If the initial state of the MADN group is private, the PRLA access code allows bridging and PRLC closes it.

Images for the Avaya 1100 Series IP Deskphones

The Avaya 1100 Series IP Deskphones provide a graphical, high-resolution LCD display, which is capable of displaying screensavers, slideshows, and background images.

Screensaver

The Avaya 1100 Series IP Deskphones can display an image on the screen when the IP Deskphone is idle.

The screensaver feature allows the administrator and the user to upload images from the provisioning server or the Universal Serial Bus (USB) memory stick to the IP Deskphone and have the selected image display when the IP Deskphone is idle.

A number of images can be uploaded to the IP Deskphone from which the end user can select a particular image.

You can specify the interval between when the IP Deskphone becomes idle and when the screensaver displays.

Slideshow

Screensaver images that have been uploaded to the IP Deskphone can be displayed in a slideshow format.

It is possible to display all of the screensaver images that have been uploaded into the IP Deskphone in a slideshow format, whereby an image displays momentarily and then the next image displays.

Different groups can of images can display independently. In order for this feature to work, the files must be named with the following syntax:

ss [x] [image_name].png

where x specifies the number of the slide group and image_name specifies the name of the image. For example:

- ss01clouds.png
- ss01sky,png

- ss01sun.png
- ss02boat.png
- ss02ship.png
- ss02sailboat.png

These files are loaded into the IP Deskphone through a Universal Serial Bus (USB) flash drive or through the provisioning server and the 11xxeSIP.cfg file. See Create the SIP provisioning file on the provisioning server on page 46 for an example of the IMAGES section of the 11xxeSIP.cfg.

Image file size

Individual images cannot exceed 512 KB for the Avaya 1140E IP Deskphone and Avaya 1165E IP Deskphone.

Images cannot exceed 128 KB for the Avaya 1120E IP Deskphone.

Image size

The IP Deskphone is not capable of resizing image files. Therefore, images must be sized according to the following table prior to loading them on the IP Deskphone.

Table 19: Image size

IP Deskphone	Image size
1120E	240 x 88
1140E	320 x 160
1165E	320 x 240

Animated screensaver for the Avaya 1165E IP Deskphone

Several images can be loaded and quickly displayed, one after the other on the Avaya 1165E IP Deskphone.

The Avaya 1165E IP Deskphone provides the ability to display several images (for example 100 images) in quick succession giving the impression of a moving image on the display screen.

A background can be loaded and displayed behind the animated screensaver.

In order for this functionality to work, the syntax of the image must be as follows:

ABIG [x]_[image_name] [xyy].png	• x – the number of the animated screensaver group • image_name – the name of the image • xyy – the sequence number of the image
ABIG [x]_bckrrnd_[image_name].png	• x – the number of the animated background group • image_name – the name of the image

For example:

- abig1_sunset001.png
- abig1_sunset002.png
- abig1_sunset003.png
- abig1_sunset004.png
- abig1_sunset005.png
- abig1_sunset006.png
- abig1_bckgrnd_sunset.png

Speed Dial List

When configured by provisioning, a feature key can be used as a "Speed Dial List". The feature key and the contents of the Speed Dial List must be specified by the provisioning mechanism. The user cannot modify or delete the feature key used by the Speed Dial List and cannot modify the content of the Speed Dial List.

Invocation of the Speed Dial List is similar to any other feature key invocation. The Speed Dial List key causes a full screen list to appear on the IP Deskphone and the user can automatically dial one of the offered choices. The Speed Dial List supports up to 30 entries.

The contents of the Speed Dial List can vary (context-sensitive) based on the current call state of the IP Deskphone and the type of Speed Dial List entry configured. Only entries in the Speed Dial List can be context-sensitive; not all speed dial keys or individual features keys are context-sensitive.

A Speed Dial key, or one included in a Speed Dial List, can cause any call that it placed on hold (when invoked) to be unheld automatically when the call completes, based on a new value that must be configured when a Speed Dial key is created or configured.

Administration and use of the Speed Dial List feature

Provisioning the device configuration provides the IP Deskphone with the following features:

- Index of key to use as Speed Dial List. You can use the following flag to disable the Speed Dial List feature by configuring the key index to less than two (2).

  SPEEDLIST_KEY_INDEX <key index>

- Label to use for the Speed Dial List key.

  SPEEDLIST_LABEL <text>

The IP Deskphone retrieves the device configuration through provisioning, and if the SPEEDLIST_KEY_INDEX flag is configured to a valid programmable key that can be used for the feature (greater than one (1) and less than or equal to the available number of programmable keys), the following events occur:

1. The IP Deskphone checks for a previously loaded "Speed Dial List" file (a file containing the contents of the speed dial list), which must be properly configured and uploaded to the IP Deskphone through provisioning.
2. The IP Deskphone parses the file, and configures the feature key specified by SPEEDLIST_KEY_INDEX to hold the Speed Dial List.
3. If the key defined for use by the Speed Dial List is already in use, the defined key is overwritten and is assigned Speed Dial List functionality.
4. The Speed Dial List feature key uses the label that is provided in SPEEDLIST_LABEL, and cannot be modified by the end user.

The following screen describes the feature key used by the Speed Dial List in the feature key programming interface.

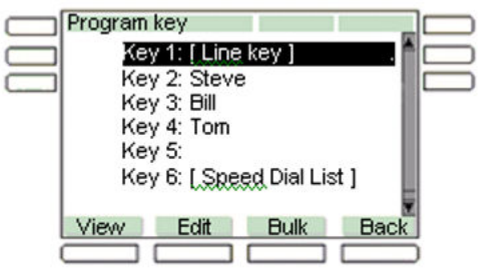


Figure 20: Main feature key programming screen showing Speed Dial List provisioned on key 6

A feature key provisioned for use as a Speed Dial List has a similar appearance to all other programmed feature keys on the idle screen (or in-call screen). The label used for that key is provided through provisioning.

When the user presses the feature key provisioned as a Speed Dial List, the list of speed dials configured appears on the screen, and the user can select an item from the list to invoke Speed Dial.

If the Speed Dial List is empty, or ends up empty due to context-sensitive hiding of contents, the error message "Not available" is displayed on the screen with a "Dial List" context line.

Speed Dial List screen

The Speed Dial List screen for the IP Deskphone is where the user can select or invoke one of the provisioned Speed Dial List entries.

The following image is an example of the screen that appears after the user presses the feature key that is provisioned as the Speed Dial List for the IP Deskphone.

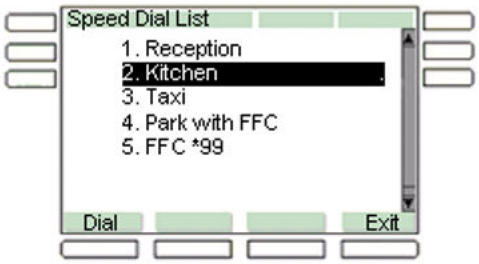


Figure 21: Example of a Speed Dial List

The Speed Dial List screen displays all the Speed Dial List entries provisioned for the user. The listed items displayed are based on the provisioned list as well as the current Idle or Mid-call state of the IP Deskphone. When the Speed Dial List is invoked while the IP Deskphone is idle, only Speed Dial List entries that are configured as IDLE are displayed. Similarly, only items marked as MID CALL are displayed if the Speed Dial List is invoked while the IP Deskphone is in a call.

The following table describes the function of the context-sensitive soft keys for the Speed Dial List screen.

Table 20: Context-sensitive soft keys for the Speed Dial List screen

Context-sensitive soft key	Action
Dial	Invokes the selected speed dial.
Exit	The screen is dismissed without invoking a Speed Dial List entry.

Auto Retrieve flag

Because the Auto Retrieve behavior is added to the regular speed dial keys (programmed keys) instead of just speed dial list entries, the Auto Retrieve flag is configured for programmed speed dial keys.

The following screen appears as the last step, after the "Enter Subject" prompt, in the creation or modification of a Speed Dial key to allow the user to configure the Auto Retrieve behavior for the Speed Dial function.

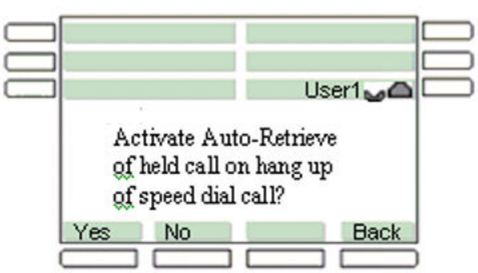


Figure 22: Speed Dial Key creation — last step

The following table describes the function of the context-sensitive soft keys for the **Auto Retrieve** screen.

Table 21: Context-sensitive soft keys for the Auto Retrieve screen

Context-sensitive soft key	Action
Yes	Enables the Speed Dial Auto Retrieve behavior.
No	Disables the Speed Dial Auto Retrieve behavior.
Back	Dismisses the screen and returns you to the previous key programming screen.

If the Auto Retrieve behavior is enabled on a Speed Dial key (programmed keys) or Speed Dial List entry that is invoked, and a call is placed on hold to invoke the current key or entry, the IP Deskphone attempts to remove the call on hold after the key or entry call is complete.

The following is a description of how the Auto Retrieve function operates.

1. A is talking to B when A invokes the Speed Dial List and selects an entry.
2. The call between A and B is placed on hold, and A places another outgoing call to C (a URI specified in the Speed Dial List entry).
3. When the call between A and C is complete, if the Auto Retrieve flag is enabled for the Speed Dial, then the IP Deskphone attempts to take the call between A and B off hold.

   If another call comes in during the call between A and C, or if the state of the call between A and B changes when the call between A and C is active, the re-connection of the call between A and B may not always happen.

The following is an example of a Speed Dial List file (for example, a file named speedDialList.txt) that must be loaded through provisioning.

```
[key]
label=S1
target=s1@avaya.com
retrieve=YES
mode=MidCallOnly
type=spdial

[key]
label=S2
retrieve=NO
mode=IdleOnly
subject=subject2
target=s2@avaya.com
type=spdial

[key]
label=S3
retrieve=NO
target=s3@avaya.com
```

Address Book

Overview

The IP Deskphone with SIP software supports two modes of the Address Book:

1. NETWORK — In this mode, the IP Deskphone downloads the user's Address Book from the network. New Address Book entries are uploaded to the network
2. LOCAL — In this mode, the Address Book is created and stored locally on the IP Deskphone. A part of the Address Book can be downloaded from the network and added to the content of the local Address Book

The size of the Address Book is specified by the MAX_ADDR_BOOK_ENTRIES parameter. The MAX_ADDR_BOOK_ENTRIES parameter limits the total number of entries in the Address Book (including both downloaded records and records added manually). The default value of this parameter is 1000 (permitted values are 0 to 1000).

Note:

The MAX_ADDR_BOOK_ENTRIES parameter only applies to LOCAL Address Book mode. In NETWORK Address Book mode, the size of the Address Book is controlled through a service package.

The MAX_DOWNLOAD_ADDR_BOOK_ENTRIES parameter specifies the maximum number of Address Book entries that can be downloaded from the network in LOCAL Address Book mode. The default value of this parameter is 1000 (permitted values are 0 to 1000).

In LOCAL Address Book mode, if MAX_DOWNLOAD_ADDR_BOOK_ENTRIES is larger than MAX_ADDR_BOOK_ENTRIES then only MAX_ADDR_BOOK_ENTRIES are downloaded from the network.

Address Book operation in LOCAL mode

The local Address Book is stored in the IP Deskphone flash memory in the file named *directory.txt*. At phone startup, the content of this file is loaded into the IP Deskphone memory and forms a working copy of the local Address Book.

There are two ways of downloading the Address Book from the network in LOCAL mode:

1. Downloading the Address Book from the Provisioning Server

   The Address Book to be downloaded is specified in the device configuration file (or in the user.cfg file when roaming profiles are used). The IP Deskphone downloads the specified Address Book file, extracts Address Book entries up to the value of the MAX_DOWNLOAD_ADDR_BOOK_ENTRIES (or MAX_ADDR_BOOK_ENTRIES if it is less than MAX_DOWNLOAD_ADDR_BOOK_ENTRIES) parameter and saves them to the local Address Book file. The existing content of the *directory.txt* file is replaced by the entries downloaded from the Provisioning Server. The maximum number of entries in the *directory.txt* file is limited by the MAX_ADDR_BOOK_ENTRIES parameter

2. Downloading the Address Book from IP Office (requires the IP Deskphone to be configured to register on IP Office)

   The download of the Address Book file(s) is initiated by IP Office. The IP Deskphone downloads the Address Book file(s) from IP Office, extracts Address Book entries up to the value of the MAX_DOWNLOAD_ADDR_BOOK_ENTRIES (or MAX_ADDR_BOOK_ENTRIES if it is less than MAX_DOWNLOAD_ADDR_BOOK_ENTRIES) parameter and saves them to the *extdirectory.txt* file in the IP Deskphone flash memory. The existing content of the *extdirectory.txt* file is replaced by new entries downloaded from IP Office. Then the content of the *extdirectory.txt* file is merged to the local Address Book in memory according to the following rules:

   a. If an entry does not exist in the Address Book in the IP Deskphone memory, it is added

   b. If an entry already exists in the Address Book in memory, the existing entry is retained

   The maximum number of entries in the local Address Book in memory is limited by the MAX_ADDR_BOOK_ENTRIES parameter.

IP Deskphone users can add manual entries to the local Address Book as long as the number of entries in the Address Book does not exceed MAX_ADDR_BOOK_ENTRIES. The number of entries that can be added manually is the difference between MAX_ADDR_BOOK_ENTRIES and MAX_DOWNLOAD_ADDR_BOOK_ENTRIES. Manually-added entries are saved to the *directory.txt* file.

Example

The following is an example of the Address Book section of the device configuration file.

#------Address book

USER_FILE_ENABLE Y

ADDR_BOOK_MODE LOCAL

MAX_ADDR_BOOK_ENTRIES 1000

MAX_DOWNLOADED_ADDR_BOOK_ENTRIES 1000

DEFAULT_ADDRESSBOOK_FILE /Addressbook/addressbook.txt

Roaming profiles

Roaming profiles enable the user to obtain the same settings when they are logged on to multiple IP Deskphones for features such as Address Book, Programmable keys, and Speed Dial List.

The updatable data is split into 3 text files for these features.

- address book
- custom keys
- speed dial list

The user configuration file is used to specify the specific names of the feature files to be downloaded. The IP Deskphone requests a user configuration file using the name <username@domain>.cfg, where <username@domain> is the address of the primary user, for example lpg@abc_company.com.cfg.

The USER_FILE_ENABLE device configuration file parameter is used to determine whether to download the user.cfg file on user login and to check for updates.

Filemames to be downloaded are specified in a [files] section. An example of the syntax is provided below:

```
[files]

addressbook=abook.txt
customkeys=keys.txt
speeddiallist=sdl.txt
```

For more information about the device configuration file, see Feature configuration commands on page 73.

Address Book file

The Address Book file represents each contact [contact] and each group [group] (name only). A contact provides attributes to specify a nickname, SIP address, group and whether the contact is a friend. The following is an example of the syntax.

```
[version]
id=12345

[contact]
nickname=lpg
address=lpg@abc_company.com
group=abc_company
buddy=1

[group]
name=macadamian
```

Custom keys file

The Custom keys file enables programmable keys to be provisioned for the IP Deskphone. This file consists of multiple sections:

- index — index of the physical key on which the feature is made available. This uses the same numbering as on the IP Deskphone user interface (right hand keys, then left hand keys, then Expansion Module keys).
- label — the text which appears next to the key on the IP Deskphone screen.
- type — the feature programmed on the key.
- audiocodecs — priority-order list of codecs
- autoanswer — allowed addresses for acceptance of auto-answer requests
- key — configuration for programmable keys
- prefs — main profile preferences
- reasons — list of reject reasons
- subjects — list of call subjects
- versions

The sections in the custom keys file can be in any order. Each section contains parameters and values. All parameters should contain values, except for the following:

- banner
- screensvrText
- screensvrImage
- backgroundImage
- hotlineURL

If a parameter has no value, its previous value is restored. For parameters which are allowed blank values, if the parameter is blank then the value is cleared.

The custom keys file supports sections which contain user preferences. This file has the same format as the prefs.txt file which is stored on the flash of the IP Deskphone. After downloading the custom keys file, this information is merged with information from the user profile (file prefs.txt). If the parameter has a new value in the custom keys file, then the old value is replaced. If any parameter is not provisioned through the custom keys file, the old parameter with its corresponding value is used. After the merge, the new data is written on the flash to the prefs.txt file. This information is then used by the profile manager.

Note:

The label for a programmable key can be modified by the IP Deskphone end-user through the phone UI in the **Feature Options > Feature Keys** menu. If the end-user enters a blank label for a key that has a default label defined in the custom keys file, then that default label overrides the blank label and is applied to the key

The following table describes the sections and keys, and provides examples.

Section name	Key	Value example	Description
[audiocodecs]			The priority-ordered list of codecs
	str-0	PCMU	The key consists of prefix “str-“ and the sequence number 0,1… The value can be any supported codec.
	str-1	G729	
[autoanswer]			
	str-0	3007@mycompany.com	The list of allowed addresses from whom auto-answer requests should be accepted.
[key]			Contains special section(s) for describing configuration for the programmable keys.
	icon	5	Icon number; codes are defined in the “Tab. 1. Icon definition”

Table continues…

Section name	Key	Value example	Description
	index	3	Key number; sequential, starting with the IP Deskphone, then the Expansion Module(s)
	label	CallForward	Text to be displayed for the key
	target	*4	Information number to be sent to IP Office
	type	feature	Key type
[prefs]			Contains the main profile preferences.
	alertPattern	4	Default ringtone pattern, 0-7
	alertVolume	6	Volume of ringtones, 0-7
	handsetVolume	8	In-call volume of handset, 0-19
	handsfreeVolume	10	In-call volume of handsfree speaker, 0-19
	headsetVolume	8	In-call volume of headset, 0-19
	pagingVolume	3	Volume of beeps, 0-7
	alphaDialing	0	Defines if dial prompt should start up in Alpha mode (0 – digits mode, 1 – alpha mode)
	autoAnswerMode	0	Determines when to accept auto-answer requests in calls. 0 = autoAnswerWhiteList only
	autoClearMissedCalls	0	Determines if entering the inbox (without selecting each missed call) clears the "xx new calls" message
	backgroundImage		Filename of image to use for the background (can be blank)
	backlightTimeout	60	Time to wait before dimming screen, in minutes
	banner	Avaya	Text to show on idle screen (can be blank)
	dateFmt	2	Display format for dates 2 –m/d/y, 3 – d/m/y
	timeFmt	0	Display format for time 0 – 12hrs (5:45pm), 1 – 24hrs (17:45), 2 – 24hrs French (5h45)
	globalIgnore	0	Designates whether the Ignore key terminate all forks of a call. Value = 0 or 1

Table continues…

Section name	Key	Value example	Description
	hotlineURL	2600@mycountry.gov	Target url for a hotline call.
	language	English	User interface language. Value = language filename without extension
	menuAutoBackout	30	Delay before the menus timeout Valid values: 0,15,30,60,120,200,600 seconds
	notifyCallForward	0	Specifies whether server-forwarded calls make the IP Deskphone beep Value = 0 or 1

	octEndsDialing	1	Specifies if # causees dial prompts to place call
			Value = 0 or 1

	outgoingPrivacy	0	Anonymization setting to use for outgoing messages 0 = none
	incomingPrivacy	0	Anonymization setting for remote user information 0 = none
	publicScaHold	0	Specifies whether others can retrieve calls a user pus on hold Value = 0 or 1
	screensvrActive	0	Specifies if screensaver is activated immediately on auto login Value = 0 or 1
	screensvrDelay	10	Time to wait before displaying the screensaver, in minutes
	screensvrImage		Filename of image to use for the screensaver (can be blank)
	screensvrMode	0	0=ssmDISABLE 1=ssmENABLE_NO_PASS 2=ssmENABLE_PASS
	screensvrText	My Company	Text to show on screensaver screen (may be blank)
	searchMethod	0	Search mode for searchable menus Values: 0 = UKNOWN_SEARCH 1 = INDEX_SEARCH

Table continues…

Section name	Key	Value example	Description
			2 = FIRST_CHARCTER_SEARCH 3 = NAME_SEARCH
[reasons]			This section contains the list of reject reasons
	str-1	Out of office	The key consists of prefix “str-“and the sequence number 0, 1… The value can be any string.
	str-2	Busy	
[subjects]			
	str-0	Hello!!	The key consists of prefix “str-“and the sequence number 0, 1… The value can be any string.
	str-1	Hi!	

The following rules apply to the [key] section:

1. In non-IP Office mode, any keys defined as “feature” have no effect and are ignored.
2. If the “type” field is omitted, the key is considered as the “spdial” key by default.
3. If the [type] field has the incorrect paramete,r the [key] section is considered to be incorrect and is ignored (appropriate ECR record is registered in the ECR file).

Feature key types

The following attributes depend on the type of key being programmed:

- spdial – Speed Dial key
- cfwd – Call Forward key
- dnd – Do Not Disturb key
- im – Send an Instant Message key
- presence – Change-my-presence key

The following attributes are type-specific attributes:

- target – for cfwd, spdial, im keys. The SIP address to target when the key is pressed. This is a mandatory attribute for spdial and im. Omitting this attribute from a cfwd key creates a "disable call forward" key.
- user – for cfwd, dnd, presence keys. The SIP address of the logged-in user whose state should be modified. Omitting this attribute creates "apply to all users" key.
- subject – for spdial. Optional. This is for the call subject to send on the call.
- retrieve – for spdial key. Optional. If this key is configured to Yes, the autoretrieve mode is enabled.
- state – for presence keys. Mandatory. The state to apply when the key is pressed; CONNECTED or UNAVAILABLE.

- note – for presence keys. Optional. The note to configure when the presence is changed; arbitrary text.

An example of the syntax is provided below:

```
[key]
index=2
label=label1
target=lpgp@macmcs.madadamian.com
type=spdial
subject=my first call subject

[key]
index=4
label=label22
note=on vacation
state=UNAVAILABLE
type=presence
```

Speed Dial List file

The Speed Dial List file is used to populate the menu which appears when a Speed Dial List custom key is pressed.

The SDL key itself is provisioned using the device configuration file, not the custom keys file.

The Speed Dial List file format is similar to Custom keys file format, except for the following:

- Only keys of type spdial are supported; the "type=" attribute can be omitted.
- The index attribute is ignored.
- Mode attributed is supported to specifies in which context the SDL entry should be visible. The value options are IdleOnly, MidCall, and Always (default).

An example of the syntax is as follows:

```
[key]
label=label11
target=lpgp@macmcs.madadamian.com
retrieve=YES
subject=my second call subject
mode=MidCall
```

Roaming profile limitations

Roaming profiles have the following limitations:

- Changes made on the IP Deskphone cannot be uploaded to the Call Server.
- The user cannot edit the downloaded Speed Dial List.
- Profiles are downloaded for the primary user only.
- If a file is downloaded that places a custom key on a key that is already in use as a user’s login Line key, the Line key takes precedence. The custom key is restored if the user logs off.

- If a file is downloaded that places a custom key on a non-existent key - for example, Key 10 - and the IP Deskphone does not have an Expansion Module attached, then the key is not shown. The key appears only when an Expansion Module is attached.

Roaming profiles and service packages

If the IP Deskphone supports roaming profiles that have a service package and that service package has the network address book enabled, then when the service package arrives, the service package-enabled network address book replaces the Address Book. The roaming profile and the network address book are mutually exclusive. To prevent this from happening, disable the network address book in the user's service package.

Default names

Default names can also be provisioned in the Device configuration file if per-user files are not required. Default names are overridden by names specified in the user.cfg file.

- DEFAULT_ADDRESSBOOK_FILE
- DEFAULT_SPEEDDIALLIST_FILE
- DEFAULT_CUSTOMKEYS_FILE

For more information about the device configuration file, see Feature configuration commands on page 73.

Customizable banner for login

SIP Software allows the IP Deskphone to display a customizable banner when you log on to the IP Deskphone. When the login banner is provided with login banner text and is configured as "enable", the IP Deskphone displays the banner text on the screen when the user logs on.

The banner text is only displayed in the language that is provisioned (changing the IP Deskphone configured language does not change the banner text language). The banner appears only for the primary user of the IP Deskphone. In a multiuser configuration, a secondary user logon does not cause the banner to appear, even if the login banner is configured as enabled.

If the login banner is configured as enabled, the banner screen on the IP Deskphone is displayed after the final step of the logon process.

The following image is an example of the Login Banner screen which displays the provisioned banner text.

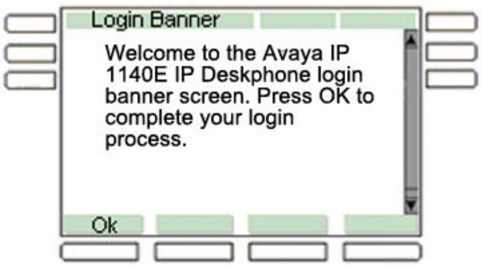


Figure 23: Login Banner

The following table describes the function of the context-sensitive soft key for the Login Banner screen.

Table 22: Context-sensitive soft key for the Login Banner screen

Context-sensitive soft key	Action
Ok	Completes the login process and dismisses the login screen.

The following table describes the function of the Navigation keys for the Login Banner screen.

Table 23: Navigation

Key	Action
Up and down arrows	Allows you to scroll up and down the banner text.
Left and right arrows	No action (the text is word-wrapped automatically).
Enter	No action.

The following table describes the outside actions on content for the Login Banner screen.

Table 24: Outside actions on content

Key or action	Result
Inbox	No action.
Outbox	No action.
Directory (Address book)	No action.
Goodbye	No action.
Expand (IM Box)	No action.
Copy	No action.
Services	Press once, no action. Press twice invokes the Network menu.
Quit	No action.

Table continues…

Key or action	Result
Headset	Brings up the dial prompt (in case the user wants to place an emergency call).
Hold	No action.
Dialpad	No action.
Handsfree	Brings up the dial prompt (in case the user wants to place an emergency call).
Off Hook	Brings up the dial prompt (in case the user wants to place an emergency call).
Mute	No action.
Volume up and volume down	No action.
User-defined feature keys	No action.
Incoming call	Incoming calls get a Do Not Disturb (DND) response while the banner is displayed.

The user must explicitly dismiss the banner screen (like a location list), and the IP Deskphone goes in DND mode until the banner is dismissed. The IP Deskphone cannot make or receive any calls, other than an emergency call, until the banner is dismissed.

If any other pop up messages or prompts, such as a location prompt, occur while the banner is displayed, then the pop up messages or prompts appear below the banner screen, and are viewed by the user only after the user dismisses the login banner.

The following configuration flag is used for enabling or disabling the customized login banner.

LOGIN_BANNER_ENABLE YES/NO (Default: NO)

The banner text is defined in a separate text file that is linked from the original configuration file.

The banner text file is a separate file downloaded by provisioning. The banner text file is specified much like the current dialing plan is specified (file name listed in 11xxeSIP.cfg, under section [LOGIN_BANNER]), and is downloaded when enabled or disabled.

To be accepted, the file must contain at least one byte and must be no larger than 2048 bytes. The encoding of the file must be UTF-8, or compatible with UTF-8, to ensure that all the characters are displayed properly.

Busy Lamp Field

The Busy Lamp Field (BLF) feature is an alternate presence-monitoring mechanism for the IP Deskphone that allows presence functionality on proxies that support BLF.

BLF is an icon state for a corresponding Speed Dial key on an IP Deskphone; the icon state tells you if another extension connected to the same SIP server is busy. If configured, the IP Deskphone subscribes to a resource list available on the server and receives information about other extensions. BLF works through the SIP protocol by making use of **`SUBSCRIBE`** and **`NOTIFY`** messages; the IP Deskphone is the subscriber and the SIP server is the notifier.

How it works

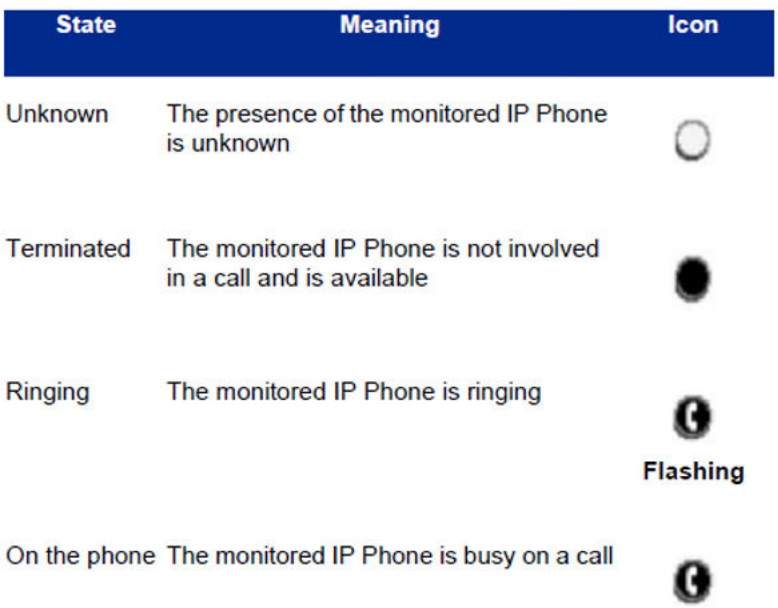
If you configure an IP Deskphone to monitor a list of zero or more extensions, it sends a **SUBSCRIBE SIP** message to the server. A **NOTIFY SIP** message, which includes XML in the message body, is sent to the subscriber to advise the subscriber of the current state of the extension being monitored. Once the status of the monitored extension changes, the subscriber receives a **NOTIFY SIP** message from the server. The subscriber must acknowledge the **NOTIFY SIP** message by responding with a **200 OK SIP** message.

BLF is based on an Event Dialog package. Dialog refers to the SIP relationship that two SIP peers establish. Dialogs can be created by many methods, although RFC 3261 defines only one: the **INVITE** method. In other words, as soon as two SIP peers establish a new call/dialog, modify a call/dialog, or cancel a call/dialog, the monitoring party receives notification about that event. For more information, refer to RFC 4235.

Note:

Dialog Package (BLF) differs from Presence package. Refer to RFC3856 for more information on Presence.

Use the command **BLF_ENABLE** to enable the BLF feature on an IP Deskphone. In order to use BLF, it must be activated, properly provisioned, and connected to the server that supports this feature. It is used whenever a speed dial key is provisioned on the IP Deskphone; an icon assigned to the speed dial key reflects the new status of the monitored peer, which is extracted from a **NOTIFY** message. You can configure speed dial keys for as many parties as you want to monitor; the parties must exist on the configured Resource List Uniform Resource Identifier (URI). Figure 24: Call states and corresponding Presence icons on page 204 shows the various call states and corresponding icons.



State	Meaning	Icon
Unknown	The presence of the monitored IP Phone is unknown	
Terminated	The monitored IP Phone is not involved in a call and is available	
Ringing	The monitored IP Phone is ringing	Flashing
On the phone	The monitored IP Phone is busy on a call	

Figure 24: Call states and corresponding Presence icons

Resource List URI

The SIP-specific event notification mechanism allows the subscriber to request to be notified of changes in the state of a particular resource. Users often subscribe to multiple resources; without an aggregating mechanism, the user would have to generate a **SUBSCRIBE** request for each resource they monitor.

A resource list is identified by a URI, and it represents a list of zero or more URIs (SIP endpoints). Each URI is an identifier for an individual resource to which the user can subscriber. The configuration of URI is done on the server and an IP Deskphone requires only to be configured with the desired Resource List URI; the URI can even be configured automatically if the server supports auto-generation. For more information, refer to RFC 4662.

If **BLF_ENABLE** = **YES** , then use **BLF_RESOURCE_LIST_URI** to configure the Resource List URI. You must use the URI provided by the proxy when you configure the user for BLF.

If **BLF_ ENABLE** = **SCS|SIPX**, the Resource List URI auto generates in the following format:

```
~~rl~C~<username>@<domain></domain></username>
```

BLF call pickup

Important:

BLF Call Pickup is only supported for IP Office. Therefore, **IP_OFFICE_ENABLE** must equal **YES** for Call Pickup to work.

The Call Pickup feature allows a user to pick up a call by pressing the corresponding speed dial key when the indicator for a monitored line flashes. The IP Deskphone must send an **INVITE** with the Replaces header. Target uri, call-id, to-tag and from tag in the Replaces header are taken from the **NOTIFY** message. The Replaces header is specified in RFC 3891.

Use the **MAX_BLFCALLS** parameter to configure this feature. This parameter specifies the maximum number of available BLF(picked up) calls on an IP Deskphone. The actual value of **MAX_BLFCALLS** correlates with the value of **MAX_APPEARANCE**, which specifies the maximum number of available calls of any type. **MAX_BLFCALLS** must always be less than or equal to **MAX_APPEARANCE**. If initial value of the **MAX_BLFCALLS** parameter is greater than the value of **MAX_APPEARANCE**, the value of the **MAX_BLFCALLS** parameter is forcibly reduced.

Universal Serial Bus device support

The Avaya 1100 Series IP Deskphones provide a USB port located on the back of the IP Deskphone to support Universal Serial Bus (USB) devices.

The IP Deskphones support the following USB devices:

- USB memory stick
- USB headsets

For corporate security purposes, you can disable the supported USB devices, individually or all, by disabling the USB port.

Important:

Only one USB headset or one USB memory stick can be connected at a time. Multiple USB headsets or USB memory sticks can not be connected simultaneously. Both narrow band and wideband audio are supported.

Important:

During software upgrade, the IP Deskphone goes into the Do Not Disturb (DND). The IP Deskphone cannot receive any incoming calls, or make outgoing calls, until the software upgrade is complete and the IP Deskphone restarts.

USB port behavior

By default, the Avaya 1100 Series IP Deskphones start with the USB port and all the supported USB devices enabled. You can change the default behavior on all the IP Deskphones by provisioning the USB port lock feature or by manually applying the locks to the IP Deskphone.

System-wide USB port behavior is configured using the Device configuration file. Manual override in the user preference menu, protected by the Administrator password, is available to change individual user settings.

If the USB port is disabled, the USB host controller is not initialized and the USB device is enumerated. The USB menu shows that the USB port is disabled.

If the USB Port is enabled, you can attach any USB 1.1 or 2.2 compliant device to the IP Deskphone; then the IP Deskphone enumerates the USB devices and displays them on the USB screen. If a USB device is not supported by the IP Deskphone, or if a USB device type is locked, the IP Deskphone still enumerates the USB device and displays it on the USB screen. Separate information is provided, in the USB menu, to indicate the USB device types that are locked.

Only USB devices that are unlocked function correctly. Locked USB devices do not work.

Device configuration commands

To configure the USB port behavior using the provisioning server, the following device configuration commands are available:

Note:

The parameters affect the configurations of all the IP Deskphones.

Table 25: USB Port lock device configuration parameters

Commands	Parameters	Remarks
ENABLE_USB_PORT	[YES|NO]	If configured as No, all USB devices are disabled and all other USB device configuration commands are ignored.
USB_MOUSE	[LOCK|UNLOCK]	—
USB_KEYBOARD	[LOCK|UNLOCK]	—
USB_HEADSET	[LOCK|UNLOCK}	—
USB_MEMORY_STICK	[LOCK|UNLOCK]	—

To manually override the USB device setting on a particular IP Deskphone, in the USB Lock menu, use the USB_LOCK_OVERRIDE command.

After you have configured the IP Deskphone to manually override the USB device setting, the USB lock configurations from the device configuration file are ignored and the configurations stored in the IP Deskphone are used. If you later decide to not allow manual override, you have to access the IP Deskphone to reset it individually. The transition from enable USB_LOCK_OVERRIDE to disable USB_LOCK_OVERRIDE triggers an optional restart in order to reread the configurations from the device configuration file.

IP Deskphone information on USB devices

If the Enable USB Port is configured as NO then USB information does not display any USB devices connected in the **System** > **Phone Information** USB Devices screen. The USB information menu displays the information that the USB port is disabled.

The following is an example of the USB Devices information screen when the USB port is disabled.

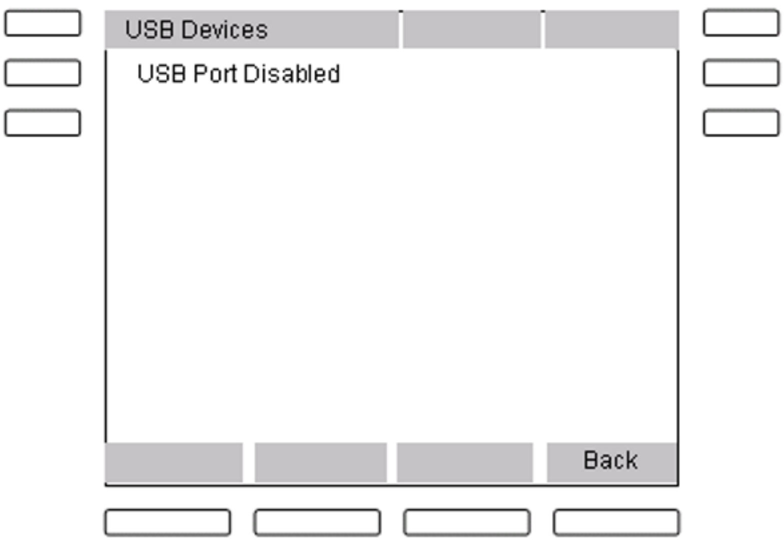


Figure 25: USB Devices information screen — USB Port disabled

If the USB Port is enabled, the USB Devices screen displays information on all USB devices attached, even if the device is locked. USB enumeration is independent of the device driver status. An unsupported device can still be enumerated if it is attached to the IP Deskphone. To ensure that the user is aware of the USB lock status, the USB device information is followed by status information on supported devices. If the USB configurations do not match the USB device status because of reboot requirements, the screen displays a warning that the USB update requires reboot.

An example of the USB Devices information screen with the USB port enabled and selected device locked is shown in the following figure.

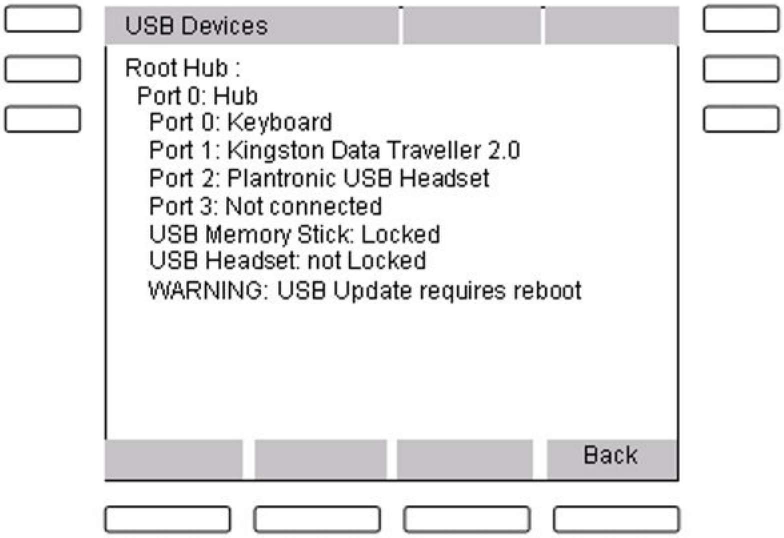


Figure 26: Sample USB Devices information menu

USB lock

Although the USB port allows the IP Deskphone to extend peripheral support without hardware changes, the customer is required to lock the USB port in compliance with the corporate security policy. The lock can be applied on the USB port to disable all USB devices, or it can be applied on individual types of USB devices.

USB Locks preference menu

You can override the system configurations on the IP Deskphone through the USB Locks screen. The USB Locks screen allows you to override the USB lock configurations in the device configuration file to enable or disable the USB port. If the USB Locks Override is enabled and the USB port is not disabled, you can individually lock or unlock the supported USB devices on the IP USB Locks.

To access the USB Locks screen, from the Preference menu, choose **USB Locks**. The protected Administrator password is required.

The following is an example of a USB Locks screen.

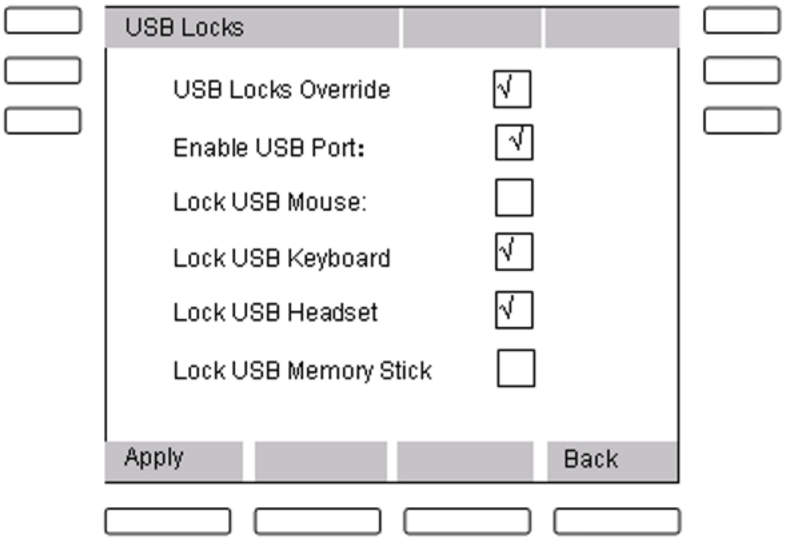


Figure 27: USB Locks screen

The following table describes the options that are listed on the USB Locks screen.

Table 26: USB Locks screen options

USB Locks options	Description
USB Locks Override	• Enables or disables the USB lock configurations from the device configuration file. • If USB Locks Override is not checked, the remaining items on the list appear dimmed and the configurations from the device configuration file are used. • A change, from override to not override, triggers an optional restart request in order to reread the configurations from the configuration file, and starts only the drivers that are enabled or unlocked.
Enable USB Port (only if USB Locks Override is checked)	• Enables or disables the USB port. • If the Enable USB Port is not checked, the remaining items on the list appear dimmed, and the driver is disabled. • A change, from enable to disable, triggers an optional reboot request in order to remove the USB stack.
Lock USB Mouse (only if Enable USB Port is checked)	• The checkbox is used to lock or unlock the USB Mouse • Reboot is not required for change to take effect.

Table continues…

USB Locks options	Description
Lock USB Keyboard (only if Enable USB Port is checked)	• The checkbox is used to lock or unlock the USB Keyboard. • Reboot is not required for change to take effect.
Disable USB Headset (only if Enable USB Port is checked)	• The checkbox is used to lock or unlock the USB Headset. • A change from unlock to lock USB Headset triggers an optional reboot request in order to remove the USB headset driver.
Lock USB Flash Drive (only if Enable USB Port is checked)	• The checkbox is used to lock or unlock the USB Flash Drive. • Reboot is not required for change to take effect.

Important:

Although a locked USB device is not functional, it still appears in the USB menu.

The following table describes the function of the Context-sensitive soft keys for the USB Locks screen.

Table 27: Context-sensitive soft keys for the USB Locks screen

Context-sensitive soft key	Action
Apply	Applies and saves changes; quits the USB Locks screen and returns you to the previous screen. If the changes require reboot, a dialog box appears with a warning that a reboot is required for the change to take effect. The warning dialog box lets you reboot immediately, or delay the reboot for later without updating the status of all the USB driver. The reboot condition is reevaluated each time you access the USB Locks menu, based on the USB Locks configuration. It is possible to undo the changes and remove the reboot requirement. One or more of the following conditions triggers a reboot request: • USB Locks override changed from checked to unchecked • Enable USB Port changed from checked to unchecked • Lock USB Headset changed from checked to unchecked. See Figure 28: Warning screen on page 211.
Back	Discards the changes, dismisses the USB Locks menu and returns you to the previous screen.

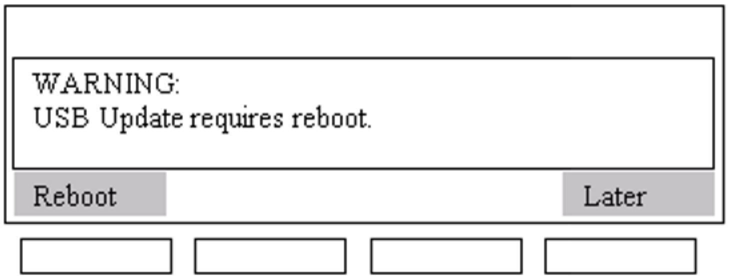


Figure 28: Warning screen

USB flash drive

SIP Software supports a standard USB flash drive for the IP Deskphone.

File system support is restricted to FAT file system with a long file name (Microsoft VFAT). The file system supports a USB memory stick with 8G or less.

USB headsets

USB headsets are supported Avaya IP Deskphone 1100 Series IP Deskphones.

The Avaya IP Deskphone 1100 Series IP Deskphones support Wideband audio on USB headsets.

Note:

Both narrowband and Wideband audio are supported.

Avaya recommends the use of the following headsets:

- GN Netcom GN9350e
- Plantronics CS-50

Hotline service

The Hotline service allows you to provision a SIP Avaya 1100 Series IP Deskphone as a Hotline Phone. From a Hotline Phone, you automatically make a call only to a designated number.

A Hotline Phone is a dedicated IP Deskphone that has only one target. You cannot make a call to any other destinations; even emergency calls, such as E911 are not permitted. A Hotline Phone does not know the Hotline target and relies on the server to replace the To field of all INVITE messages sent from the Hotline Phone with the Hotline target to complete the call.

Important:

You cannot place calls if the server is unavailable during an upgrade.

Making a Hotline call

A call to a Hotline target is automatically placed when an off-hook condition occurs, or when you press digits during idle on-hook, and then lift the handset.

Hotline Service allows only one hotline user to login to the Hotline Phone. The Multiuser Login feature is restricted to one user only.

Hotline service restrictions

Because the Hotline Phone is a dedicated IP Deskphone used only for Hotline service, certain features are restricted on the Hotline Phone.

The following is a list of features, on the IP Deskphone, that are restricted on the Hotline Phone.

- Call Transfer
- Call Forward
- Voice Mail
- Call Park
- Instant Messaging
- MLPP
- E911 call

The display of each feature that is restricted on the Hotline Phone is blocked.

Provisioning

Hotline Service configuration is obtained from the Hotline Service Enable parameter from the service package or the device configuration file. The service package takes precedence over the device configuration file.

Service Package

You can turn Hotline Service, on or off, through the Service Package or the device configuration file. If the Hotline Service Enable parameter from the service package is configured as true, the Hotline Service is enabled (available) from the service package.

Device configuration file

The IP Deskphone uses the configuration parameters for the Hotline Service to indicate if Hotline Service is available and if a hotline call is in progress.

The following table describes the two configuration parameters in the device configuration file for Hotline Service.

Table 28: Hotline Service configuration parameters

Parameter name	Description	Default
HOTLINE_ENABLE	Indicates if Hotline Service is enabled or disabled.	No (indicates that Hotline Service is disabled)
HOTLINE_URL	Used as To field of INVITE message by the SIP IP Deskphone to notify the Proxy Server that this is a call from a Hotline Phone. The HOTLINE_URL is not a real URL of the Hotline target. The IP Deskphone has no idea about the Hotline target. The Proxy server replaces the To field of INVITE request message with a real Hotline target when it receives an INVITE request from the Hotline Phone.	Hotline

Session Timer Service

The Session Timer for the Session Initiation Protocol (SIP) feature (RFC4028) allows the Avaya 1100 Series IP Deskphone to support a keep-alive mechanism for SIP sessions. SIP sessions are periodically refreshed by UPDATE requests (or re-INVITES for the IP Deskphones that do not support UPDATE). The UPDATE requests are sent during an active call to allow endpoints or proxies to determine the status of a SIP session.

The Session Timer Service contains the following elements:

- Session-Expires header
- Min-SE header
- response message (422—Session interval too small)
- tag (timer) for existing headers

The SIP IP Deskphone generates, processes and handles the SIP messages that include the preceding elements.

Session-Expires header

The SIP Session-Expires header delivers the Session-Expires interval and provides information about the entity performing the refreshes. A value of "uac" indicates that the originating endpoint performs the refresh; a value of "uas" indicates that the terminating endpoint performs the refresh. The session interval is the maximum amount of time that occurs between session refresh requests in a dialog box before the session times-out. The minimum for this field is 90 seconds; the recommended value is 1800 seconds (30 minutes).

Min-SE header

The Min-SE header indicates the minimum value for the session expiration in units of delta-seconds. When your make a call, the presence of the Min-SE header informs the terminating endpoint, and proxies, of the minimum value that the originating endpoints accept for the session timer duration in units of delta seconds. When present in a 422 response, the Min-SE header indicates the minimum session value the terminating endpoint accepts. When present in a request or response, the value of the Min-SE header is 90 seconds or more. If the Min-SE header is not present, the default value is 90 seconds. It is a configurable parameter.

Provisioning

The IP Deskphone uses the configuration parameters for the Session Timer Service to indicate if the Session Timer Service is available, and to configure the duration of the session timer.

The following table describes the five configuration parameters in the device configuration file for Session Timer Service.

Table 29: Session Timer Service configuration parameters

Parameter name	Description	Default value
SESSION_TIMER_ENABLE	Indicates if the session timer service is enabled or disabled. If configured as Yes, the Session Timer Service for the IP Deskphone is enabled, and the behavior of the IP Deskphone complies with RFC4028. If configured as No, the Session Timer Service is disabled.	Yes
SESSION_TIMER_DEFAULT_SE	Indicates the default session expiration in seconds. The Session-Expires header, in a request, informs the terminating endpoint and proxies of the Session-Expires interval value that the originating endpoint requires for the session timer duration, in unites of delta seconds.	1800
SESSION_TIMER_MIN_SE	Indicates the minimum session expiration in seconds.	1800
SET_REQ_REFRESHER	Indicates what refresher value is configured in the initial session request. Value 0 indicates that the refresher is omitted; value 1 indicates that the refresher is configured to UAC; value 2 indicates that the refresher is configured to UAS.	0

Table continues…

Parameter name	Description	Default value
SET_RESP_REFRESHER	Indicates what refresher value is configured in the 200 OK response. Value 0 indicates that the refresher is omitted (only valid when SET_REQ_REFRESHER is not equal to 0); value 1 indicates that the refresher is configured to UAS; value 2 indicates that the refresher is configured to UAC.	2

Emergency Services

Important:

Avaya strongly recommends testing the emergency services feature with the entire communications system, including the IP Deskphones during and after the installation of the communications systems. Avaya strongly recommends making arrangements with the Public Safety Answering Point (PSAP) provider to test actual emergency calls.

You can use the Avaya 1100 Series IP Deskphone to make an emergency call to the Public Safety Answering Point (PSAP), from any screen, without a user being logged on. When you connect to the PSAP, the IP Deskphone conveys the caller's location information to the PSAP, if the network supports this feature. If you are not logged on to the IP Deskphone and you pick up the handset or press the handsfree or headset button, the message Emergency calls only appears on the screen of the IP Deskphone.

If you hang up before the connection is established, the IP Deskphone goes back to the initial state. After the connection is established, the call can only be ended by the Public Safety Answering Point (PSAP). If you hang up, the IP Deskphone switches to loudspeaker. If the IP Deskphone is already on the loudspeaker mode, and you press the hang up button, nothing happens. The call is still connected and can only be disconnected by the emergency operator.

Emergency calls originate on the IP Deskphone and are completed by the Call Server. The Call Server communicates with the emergency network or emergency systems for routing, call control, and location information. Although the IP Deskphone allows the user to enter location information, this location information is not used by all Call Servers. Some Call Servers derive the location information based on the number and location databases. Characteristics of emergency calls and limitations of emergency calls using the IP Deskphone are as follows:

- Making calls without logging on is only allowed for emergency calls (according to the defined dialing plan).
- Transmission of the location information depends on support of the proxy and the network.

Location information

If the IP Deskphone turns on or off, the IP Deskphone restarts in the usual way and receives the location information through LLDP-MED or DHCP protocols (from the Layer 2 switch or DHCP server , which must be available and properly configured).

On certain Call Servers that support service packages , a list of locations is sent to the IP Deskphone and the end user is able to select the location during the login process.

When an IP Deskphone registers or makes an emergency call, the IP Deskphone provides the location to the Call Server.

Dialing plan configuration

To allow operator control of disconnect during an emergency call, the IP Deskphone must identify an emergency call as soon as an emergency call is initiated. The IP Deskphone uses an emergency flag in the dialing plan to identify an emergency call. When the dialing plan detects that an emergency number is dialed, it automatically switches to operator controlled disconnect mode when the call is answered. The dialing plan can have multiple emergency numbers.

The following outline describes the format for the dialing plan rules.

1. The first part contains one or more patterns. The patterns are used to match against the dialed number. Multiple patterns are separated by the | character.
2. The second part contains the resulting string used in the dial step.
3. The third part defines the parameters used by the UA to trigger specific dialing actions. The following parameters are defined in the third part and are separated by the | character if both are used.
    - t=xxxx: timer to stop collecting digits or perform automatic dialing out after the user enters the first digit. The xxx is a decimal number for the timer value in msec. The default timer is used if the timer is not specified in the digit map.
    - emergency: if specified, special call features are enabled to handle the call as an emergency call.

The following is an example of an emergency flag in the dialing plan: `911|911#  && sip:user@911.com && t=1000|emergency`

This feature requires configuring the values for additional variables in the configuration file (11xxeSIP.cfg).

The following table describes the configuration values for the emergency dialing plan.

Table 30: E911 Configuration in the IP Deskphone Config file

E911_USERNAME	The emergency user name used for making an emergency call that does not require a logon. You must configure the proxy with the same emergency user name, otherwise, the emergency call fails.
E911_PROXY	Default emergency proxy. This variable must contain the value that matches the value defined by one of the following variables specified in the same configuration file: • SIP_DOMAIN1 • SIP_DOMAIN2 • SIP_DOMAIN3 • SIP_DOMAIN4 • SIP_DOMAIN5 If E911_PROXY does not match the value defined by these five variables, or the variable E911_PROXY is not defined, the value of SIP_DOMAIN1 is used as the emergency proxy.
E911_PASSWORD	The password for emergency username that is used for making an emergency call that does not require login. The proxy must be configured with the same password, otherwise the emergency call fails.
E911_TXLOC	The variable that describes location information that must be sent with the REGISTER SIP message, or with the INVITE SIP message.

Important:

You must add a set of numbers (regular expressions) marked as "emergency" to the IP Deskphone dialing plan. Only these numbers are allowed for emergency calls that do not require logon.

Configuration requirements for making an emergency call when there are no users logged on

1. Configuring the SIP Proxy.
    - The IP Deskphone must have an emergency user in order to make an emergency call without a user logon.
    - The IP Deskphone must have the necessary configurations values for automatic REGISTER of the emergency user (if you choose this implementation method).
    - You must add the emergency user to the proxy.

2. Adding the emergency user to the IP Deskphone configuration file.
   - The IP Deskphone must have E911_USERNAME, E911_PROXY, and E911_PASSWORD configured for making emergency calls.
   - The IP Deskphone must have a specified proxy that contains a user record with the specified user name and password.
   - The IP Deskphone must have these values for automatic REGISTER of the emergency user (if you choose this way of implementation).
   - You must add specified variables to the IP Deskphone configuration file.
3. Adding an emergency number.
   - You must specify an emergency number for emergency calls to:
     - define the numbers that you can use for an emergency call that does not require logging on.
     - trigger emergency functionalities, such as the inability of an emergency call originator to hold or hang up the call after the call is established.
   - You can only dial these numbers if there is no user log on (or the IP Deskphone is blocked).
   - You must add the emergency number to the dialing plan. The emergency flag is mandatory. For more information on the format for dialing plan rules, see Dialing plan configuration on page 216.
4. Configuring the domain list and proxy.
   - You must properly configure the domain list, and the active proxy must be correct, valid, and support current features.
   - You must properly configure the proxy to support current features.
   - The proxy must be able to transmit mixed MIME-types (for successful transferring of the location information).
5. Configuring the proxy with emergency user name and password.
   - You must have configuration access to the proxy to arrange for an emergency user (if this manner of implementation is chosen).
   - The emergency user and password at the proxy side must be identical to the emergency user and password that every IP Deskphone is configured with. Otherwise, you cannot make an emergency call without logging on.

Characteristics of emergency calls

During an active emergency call, the user:

- cannot make outgoing calls.

- is not notified of incoming calls and cannot accept incoming calls. Incoming calls receive a call waiting tone.
- cannot transfer, join, or conference the emergency call, place the emergency call on hold, or park the emergency call.
- cannot auto-retrieve a parked call and auto-retrieval of parked calls is not displayed.
- cannot disconnect the emergency call. Only an emergency center or operator can disconnect the emergency call. If the user attempts to disconnect after the call has been made, the IP Deskphone switches to loudspeaker. If the loudspeaker mode is already on, the connection remains.
- cannot change Audio Quality.
- can reply to IM pop-ups, which are operational during an emergency call.

During an emergency call, the keys function as follows:

- the **Services**, **Inbox**, **Outbox**, **Address Book**, **Mute** , and **Hold** keys are all disabled.
- a right click of the mouse does not show the services menu.
- the increase and decrease volume keys remain functional.
- the feature keys are visible and all except the speed-dial keys are functional.

NAT firewall traversal

The objective of putting devices behind a Network Address Translator (NAT) is to protect the devices from external interruption and to extend the public IP address space. However, the shield to stop unsolicited incoming traffic also has the drawback of breaking a number of IP applications, including SIP.

If a device is behind a NAT, transport addresses obtained are not publicly routable, and therefore, not useful in a number of multimedia applications. The limited lifetime of the NAT port mapping can also cause the SIP signaling to fail. If a port mapping is idle, it can be released by the NAT and reassigned to other applications.

The STUN protocol lets an IP Deskphone discover the presence and type of NATs between the Avaya 1100 Series IP Deskphone and the public Internet. In addition, an IP Deskphone can discover the mapping between the private IP address and port number and the public IP address and port number. Typically, a service provider operates a STUN server in the public Internet, with STUN-enabled IP Deskphones embedded in end-devices, which are possibly behind a NAT.

A STUN server can be located using DNS SRV records using the domain of the service provider as the lookup. STUN typically uses the well-known port number 3478. STUN is a binary encoded protocol with a 20-octet header field and possibly additional attributes. The STUN protocol learns the public IP addresses, and therefore, some security is necessary.

To initiate a STUN lookup, the IP Deskphone sends one or more Binding Request packets using UDP to the STUN server. These packets must be sent from the same IP address that the IP Deskphone uses for the other protocol, because this is the address translation information that the IP Deskphone tries to discover.

The server returns Binding Response packets, which tell the IP Deskphone the public IP address and port number from which it received the Binding Request. The IP Deskphone knows the private IP address and port number it used to send the Binding Request, and therefore, it learns the mapping between the private and public address space being performed by the NAT. If the Binding Response packets indicate the same address and port number as the request, the IP Deskphone knows no NATs are present.

The IP Deskphone supports two methods for NAT traversal of the signaling path:

- SIP_PING
- STUN

The NAT traversal method can be selected manually through the Device Settings menu or configured through the device configuration file. The default NAT traversal method is NONE.

The IP Deskphone can conduct SIP dialogs through a Symmetric NAT using UDP. This allows the IP Deskphone to work from behind and/or in front of a symmetrical NAT with servers and/or clients that support RFC3581. For this feature to work properly, the receiving end device must support RFC3581. This feature is enabled or disabled through the USE_RPORT parameter in the device configuration file.

Note:

RFC3581 does not address NAT traversal for media or voice.

Three-port switch and VLAN functionality

System overview

The Full VLAN support feature can create telephone Voice-VLAN and PC Data-VLAN on the three-port switch of the IP Deskphone manually and automatically (see Figure 29: Voice-VLAN and Data VLAN on page 221).

If both Data and Voice VLANs are enabled on a three-port switch, only the frames with Data and Voice VLAN tagged go to networks. The IP Deskphone receives only the frames with Voice VLAN tagged and sends the frames with Voice VLAN tagged, while PC or Local Networks receive all kinds of frames.

When only voice VLAN is enabled on three-port switch, all kinds of frames go to the Network, the IP Deskphone receives only the frames with Voice VLAN tagged and send all frames with Voice VLAN tagged. PC or Local Networks receive all kinds of frames.

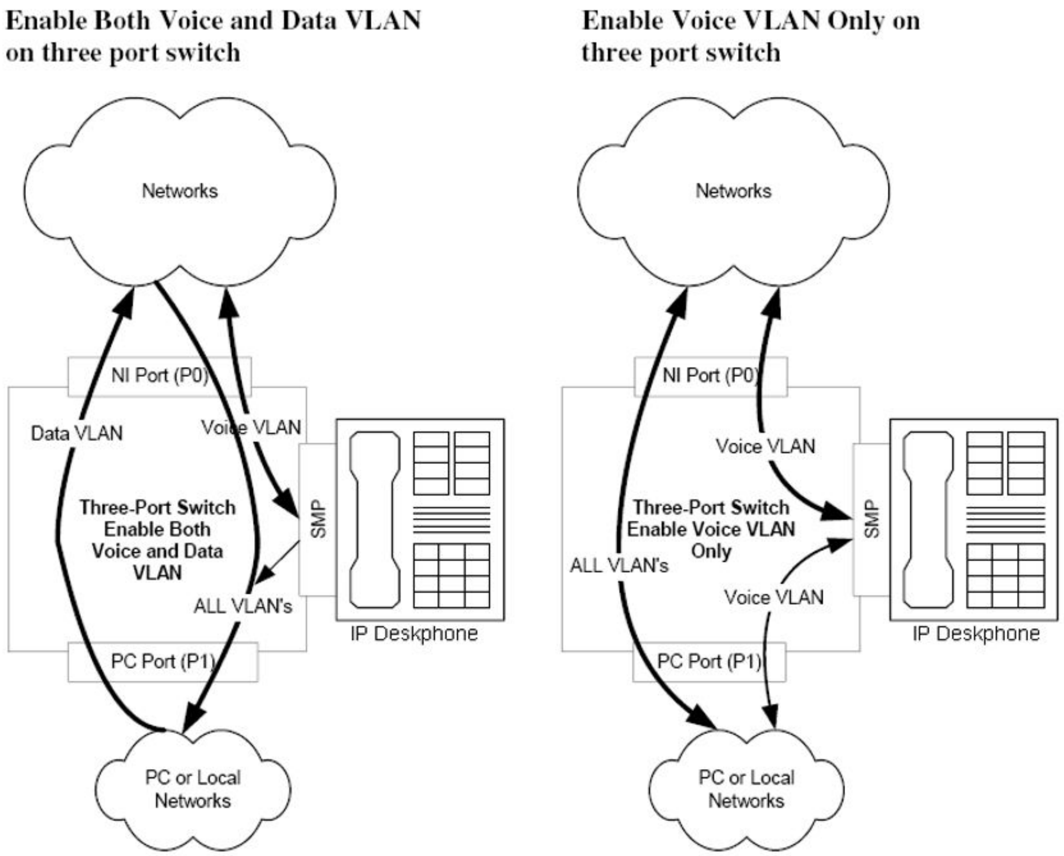


Figure 29: Voice-VLAN and Data VLAN

Table 31: Port functions on the three-port switch when VLAN is enabled

Ports	Voice VLAN enabled	Data VLAN enabled	Both Voice and Data VLAN enabled
Network Port (Port 0)	N/A	N/A	N/A
IP Deskphone Port (SMP)	Receiving the frames with Voice VLAN tagged only. Sending the frames with Voice VLAN tagged.	N/A	Receiving the frames with Voice VLAN tagged only. Sending the frames with Voice VLAN tagged.
PC Port (Port 1)	N/A	Tagging the incoming frame untagged and forwarding it to network port. Replacing the incoming frame tagged with VLAN	Tagging the incoming frame untagged and forwarding it to network port. Replacing the incoming frame tagged with VLAN other than

Table continues…

Ports	Voice VLAN enabled	Data VLAN enabled	Both Voice and Data VLAN enabled
		other than Data-VLAN and forwarding it to network port. Sending all kinds of frames.	Data-VLAN and forwarding it to network port. Sending all kinds of frames.

VLAN configuration can be done either manually or through DHCP. See Provisioning IP Deskphone parameters on page 154 for more detail on configuring VLANs.

802.1x (EAP) Port-based network access control

Extensible Authentication Protocol (EAP) supports multiple authentication methods and represents a technology framework that facilitates the adoption of Authentication, Authorization, and Accounting (AAA) schemes, such as Remote Authentication Dial In User Service (RADIUS). RADIUS is defined in RFC2865.

802.1x defines the following three roles:

1. Supplicant—an IP Deskphone requires access to the network to use network services.
2. Authenticator—the network entry point to which the supplicant physically connects (typically a Layer 2/3 switch). The authenticator acts as the proxy between the supplicant and the authentication server. The authenticator controls access to the network based on the authentication status of the supplicant.
3. Authentication server—performs authentication of the supplicant.

Enable and disable Network-level authentication through the EAP configuration menu.

The RADIUS server is the authentication server and performs the actual authentication of the supplicant. The following EAP methods are supported:

- EAP-MD5 on page 296
- EAP-PEAP on page 297
- EAP-TLS on page 297

The following options are available for the administrator:

- When EAP-MD5 is selected, the administrator is prompted to enter ID1 and Password.
- When EAP-PEAP is selected, the administrator is prompted to enter ID1, ID2, and Password. If the administrator enters only ID1, then ID2 contains same value of ID1.
- When EAP-TLS is selected, the administrator is prompted to enter ID1.
- When Disabled mode is selected, the existing IDs and Passwords are erased.

Authorization

If 802.1x is configured and the IP Deskphone is physically connected to the network, the IP Deskphone (supplicant) initiates 802.1x authentication by contacting the Layer 2/3 switch (authenticator). The IP Deskphone also initiates 802.1x authentication after the Ethernet connection (network interface only) is restored following a network link failure.

However, if the IP Deskphone resets, it assumes the Layer 2 link has remained in service and is authenticated.

The IP Deskphone fails to authorize if the DeviceID and the IP Deskphone passwords do not match the DeviceID and IP Deskphone passwords provisioned on the RADIUS Server. The Layer 2 switch (authenticator) locks out the IP Deskphone and network access is denied. If this happens during reauthorization, all phone services are lost. The connected PC operates as normal.

Device ID

The Device ID is for use with the 802.1x (EAP) protocol. If the 802.1x (EAP) is not used, then there is no prompt to enter the Device ID.

Password

The Password is for use with the 802.1x (EAP) protocol. If the 802.1x (EAP) is not used, there is no prompt to enter the Password.

802.1ab Link Layer Discovery Protocol

802.1ab Link Layer Discovery Protocol (LLDP) is a standard for discovering the physical topology between neighboring devices. 802.1ab LLDP defines a standard method for Ethernet network devices, such as switches, routers, and IP Deskphones to advertise information about themselves to other nodes on the network and to store the information they discover in a Management Information Base (MIB).

802.1ab (LLDP) takes advantage of the VLAN Name and Network Policy TLVs, and provides an automatic configuration of the IP Deskphone network policy parameters. Key parameters, such as VLAN ID, L2 priority, and DSCP values are received from the switch and are automatically configured in the IP Deskphone.

802.1ab Link Layer Discovery Protocol (LLDP) provides the following functionality:

- Periodic transmission of advertisements containing device information, device capabilities, and media specific configuration information to neighbors attached to the same network.
- Reception of LLDP advertisements from its neighbors.

- Implementation of behavioral requirements specified by Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED).
- Storage of received data in local data structures, for example, in MIB modules.

TLVs

The information fields in each MIB are contained in a Link Layer Discovery Protocol Data Unit (LLDPDU) as a sequence of short, variable-length, information elements known as TLVs that each include type, length, and value fields. Each LLDPDU includes several mandatory TLVs plus optional TLVs. Optional TLVs may be inserted in any order.

The IP Deskphone supports both the transmit and receive LLDP mode.

Transmit direction

An LLDPDU transmitted by the IP Deskphone supports the following TLVs:

1. Chassis ID
2. Port ID
3. Time To Live
4. End of LLDPPDU
5. Port Description
6. System Description
7. System Capabilities
8. Port VLAN ID
9. Port And Protocol VLAN ID
10. VLAN Name
11. Protocol Identity
12. MAC/PHY Configuration Status
13. Power Via MDI
14. Link Aggregation
15. Maximum Frame Size
16. LLDP-MED Capabilities
17. Network Policy
18. Extended Power-via MDI
19. Inventory Software Revision
20. Inventory Manufacturer Name
21. Inventory Model Name

Receive direction

The IP Deskphone expects to receive the following TLVs:

1. Chassis ID
2. Port ID
3. Time To Live
4. End of LLDPPDU
5. System Capabilities
6. VLAN Name
7. MAC/PHY Configuration Status
8. LLDP-MED Capabilities
9. Network Policy
10. Location Identification

The IP Deskphone expects to receive the following TLVs:

Table 32: TLV formats

TLV	Fields
Chassis ID	Length = 6 Chassis Subtype = 5 [IP Address] Chassis ID = IP Deskphone IP Address
Port ID	Length = 7 Port Subtype = 3 [MAC Address] Port ID = IP Deskphone MAC address
Time To Live	Length = 2 TTL= 180 [seconds]
End Of LLDPDU	Length = 0
Port Description	Length = 15 Port Description = “Avaya IP Deskphone”
System Description	Length = the length of the system description string, System Description = “Avaya IP Deskphone, xxx, Software: 0604D97” where: xxx = 1120E, 1140E, 1165E Software = software version. “0604D97” is an example only.
System Capabilities	Length = 4 System capabilities = 0x24 [Telephone + Bridge] Enabled capabilities = 0x24

Table continues…

TLV	Fields
	If you disable the PC Ethernet port, the advertised enabled capabilities configured to Telephone only.
Port VLAN ID	PVID = 0 The IP Deskphone does not support port-based VLAN operation.
Port And Protocol VLAN ID	PPVID = 0 Port and Protocol VLAN is not supported and not enabled.
VLAN Name	VLAN name field is configured to “data” and “voice”.
Protocol Identity	1. STP: Protocol identity = the first 8 bytes of an STP PDU starting with the Ethertype field. Length = 8 Protocol Identity = 0x00 0x26 (type/length field of Ethernet packet, size=38) 0x42 0x42 0x03 (LLC header indicating STP) 0x00 0x00 (Protocol Identity field from STP BPDU) 0x00 2. 802.1x:} Length = 3 Protocol identity = 0x888E—(802.1x Ethertype) 0x01—(Version field from 802.1x frame) 3. LLDP: Length = 2 Protocol identity = 0x88CC—(LLDP Ethertype)
MAC/PHY Configuration/Status	Auto-negotiation support/status = Bit 0 = 1 [Auto-negotiation supported] Bit 1 = 1 or 0, depending on the current auto-negotiation status, for example, either enabled or disabled.
	PMD auto-negotiation advertised capability = 0x4000 - 10BASE-T half duplex mode 0x2000 - 10BASE-T full duplex mode 0x0800 - 100BASE-TX half duplex mode 0x0400 - 100BASE-TX full duplex mode 0x0002 - 1000BASE-TX half duplex mode 0x0001 - 1000BASE-TX full duplex mode
	Operational MAU Type = 10 – UTP MAU, 10BT, half duplex mode 11 – UTP MAU, 10BT, full duplex mode 15 - 2-pair Category 5 (CAT5) UTP, 100BT, half duplex mode

Table continues…

TLV	Fields
	16 - 2-pair CAT5 UTP, 100BT, full duplex mode 29 – 4-pair CAT5 UTP, 1000BT, half duplex mode 30 – 4-pair CAT5 UTP, 1000BT, full duplex mode
Power Via MDI	MDI power support = 0: Bit 0 = 0 – Powered Device Bit 1 = 0 – PSE MDI power not supported Bit 2 = 0 – PSE MDI power state disabled Bit 3 = 0 – PSE pair selection can not be controlled
	PSE power pair = 1 Power Class = 3 for 1120E/1140E/1165E IP Deskphones
Link Aggregation	Aggregation status = 0; the link is not capable of being aggregated, and currently is not in aggregation. Aggregated Port ID = 0
Maximum frame size	The MAC/PHY supports an extension of the basic MAC frame format for Tagged MAC frames. The maximum frame size is configured to 1522.
LLDP-MED System Capabilities	Bit 0 = 1—LLDP-MED Capabilities–supported Bit 1 = 1—Network Policy–supported Bit 2 = 1—Location Identification–supported Bit 3 = 0—Extended Power using MDI-PSE–not supported Bit 4 = 1—Extended Power using MDI-PD–supported Bit 5 = 1—Inventory–supported The Class Type field can be configured to 3 -Telephone
Network Policy Discovery	Application Type-1—voice Unknown Policy Flag (U)—1 only if the policy is unknown Tagged Flag (T)—configure accordingly Reserved (X)-0 VLAN ID—configure accordingly L2 Priority—configure accordingly DSCP Value—configure accordingly
Location Identification Discovery	Coordinate-based LCI–16 bytes Civic Address LCI I–variable length This format can have more than one address element and one address element can range from a minimum of 7 to 256 bytes. ECS ELIN I–variable between 10 and 25 bytes

Table continues…

TLV	Fields
	Although location is received, it is not available to end user in this release of the SIP Software.
Extended Power-via MDI Discovery	Power Type = 01–PD Device Power Source = 00–Unknown. There is no hardware support for determining the power source. Power Priority = 0010–High Power Value = Maximum power required as shown below:
	1120E NTYS03 = 8 1140E NTYS05 = 8 1165E NTY507
Software Revision	Configure to the software version being used, for example, 0604D97.
Manufacturer Name	“Avaya-xy”, where: xy is a 2-digit manufacturer code as shown below:
	1120: Code 01 1140: Code 01 1165:
Model Name	Contains a string, which specifies the IP Deskphone model, for example, “IP Deskphone xxx”, where, xxx is one of the following values: 1120E, 1140E, 1165E.

PC Client Softphone interworking

The interworking feature allows the user to access the functionality of the SIP 1100 Series IP Deskphone using a softphone client on their PC. On an incoming call, both the IP Deskphone and the PC Client Softphone ring. When the user answers the IP Deskphone, the softphone remains available for Instant Messages, video and other multimedia features

The IP Deskphone, PC Client softphone, and the Call Server are all necessary to support interworking and the Click-to-Answer functionality.

The interworking feature enables the IP Deskphone to automatically answer an incoming call for the purpose of Click-to-Answer. To avoid any security risk, the user must pre-grant authorization to another user, or user groups, to allow them to make requests for the IP Deskphone to automatically answer their calls.

By using Click-to-Answer, the user can answer a call on their PC Client Softphone, causing the server to send an auto-answer request to the IP Deskphone. (When a user logs in, the IP Deskphone sends a special identifier so that only that specific IP Deskphone receives the request even though the user is logged in on multiple IP Deskphones.) The call is answered without user interaction, but the microphone is muted to prevent the device from being used as a listening device by a malicious user. When a call is answered, the user hears a ring-splash notification and can un-mute the microphone to allow bidirectional media.

Pre-granting authorization for the Answer-Mode

The user must specify which users or groups of users are authorized to request auto-answer. The user can grant authorization through the Feature Options menu if the interworking feature is enabled in the user's IP Deskphone device configuration.

The user can enable and disable one or more of the following groups:

- Allow Public—Authorizes anyone on the internet.
- Allow Friends List—Authorizes everyone on the user's Friends List.
- Allow Directory—Authorizes everyone in the user's Personal Directory.
- Allow Addresses—Acts as a white-list of domain names and SIP addresses that have authorized users.

Answer-Mode Settings screen

The Answer-Mode Settings screen is used to pre-grant authorization to request an automatic answer to potential callers or groups of callers.

The Answer-Mode Settings screen has the following two independent configurations:

- Allow Mode: [Current Setting]
- Allow Addresses

For the **Allow Mode** option, the current setting can be one of the following choices:

- Disabled
- Friends
- Directory—includes all Friends
- Public—includes all users

For the **Allow Addresses** option, the user can edit a listing by adding domain names or SIP addresses up to a maximum defined in the device configuration.

To access the Answer-Mode Settings screen, from the **Preference** menu, choose **Feature Option** and **Answer-Mode Settings**.

The following screen appears.

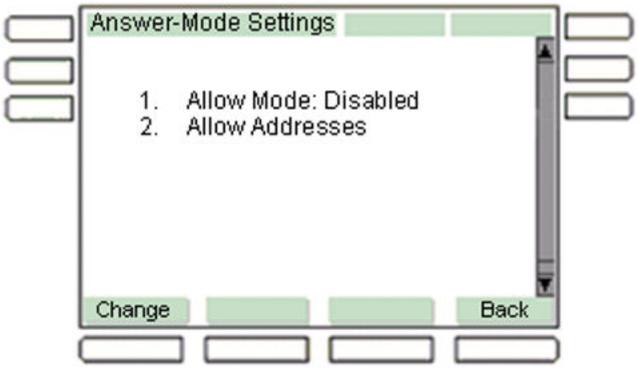


Figure 30: Answer-Mode Settings screen

Allow-Mode Settings screen

The Allow-Mode Settings screen allows you to disable the feature, and to allow automatic requests for Friends, Directory, or Public users.

To access the Allow-Mode Settings screen, on the **Preference** menu, choose **Feature Option**, **Answer-Mode Settings**, and **Allow Mode**.

The following screen appears.

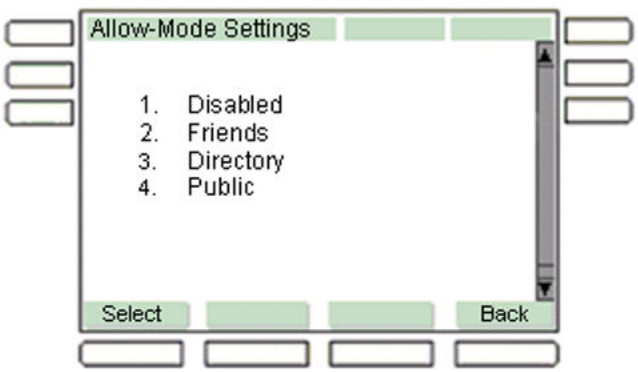


Figure 31: Allow-Mode Settings screen

Allow Addresses screen

The Allow Addresses screen is used to pre-grant authorization to request an automatic answer to a list of user-entered domains and SIP addresses.

If the user selects the **Allow Addresses** option in the Answer-Mode Settings screen, the user is presented with an interface for entering a list of strings. For the purpose of Click-to-Answer, only the current user is needed in the list because the requests originates from the user's PC Client Softphone.

For the **Allow Addresses** option, the user can edit a list of domain names or SIP addresses. The items in the list can be in any of the following formats:

- Single SIP user address

  For example:

`sipuser@sipdomain.com`

- SIP domain

  For example:

  `sipdomain.com` (all users from `sipdomain.com`

- IPv4 address of a SIP domain

  For example:

  `172.25.20.20`

- IPv6 address of a SIP domain

  For example:

  `2001:db8::57ab`

The user can add as many entries as the device configuration allows. If the **Add** soft key is disabled, then the user has reached the maximum number or entries. The user can also edit and delete entries.

To access the Allow Addresses screen, on the **Preference** menu, choose **Feature Options**, **Answer-Mode Settings**, and **Allow Addresses**.

If there are no domains in the list, the following screen appears.

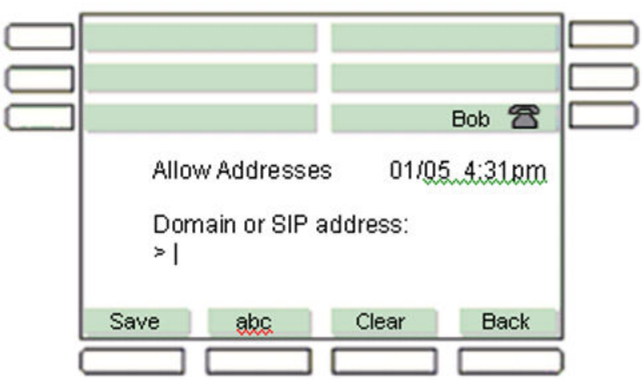


Figure 32: Allow Addresses screen — first entry

The following screen is an example of the Allow Address screen if one (or more) domain or SIP address is in the system.

Figure 33: Allow Addresses screen with domains and SIP addresses

Automatically answering a call

With the interworking feature enabled, the IP Deskphone can answer automatically, manually, or reject an incoming auto-answer request. If the request is valid and the user is authorized to make the request (see Pre-granting authorization for the Answer-Mode on page 229), the call is answered automatically.

A "ring splash", or short ring tone, indicates to the user that the call was automatically answered. The subject is "Auto-Answered", and the microphone is muted (the user can deactivate the mute status by pressing the **Mute** key on the IP Deskphone).

The following image is an example of a notification indicating an auto-answered call.

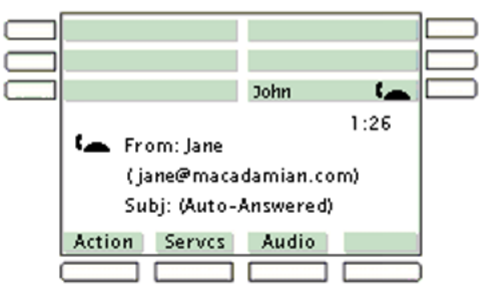


Figure 34: Example of a Notification screen indicating an Auto-Answered call

When a call is auto-answered and the handset is on the hook, the handsfree key is activated.

If there is an active call when an auto-answer request is received, the active call is placed on hold and the incoming call is answered.

If a user who is not pre-granted authorization requests a call to be automatically answered on the IP Deskphone, the call is not automatically answered and is treated as a normal call; the IP Deskphone rings and the user answers it manually.

Configuring the PC Client Softphone

Enabling the interworking feature in the IP Deskphone device configuration file allows the user to pre-grant authorization to other users and to configure the IP Deskphone to auto-answer.

Multi-Level Precedence and Preemption

The Multi-Level Precedence and Preemption (MLPP) service provides the following features:

- Precedence
- Preemption
- Call Origination Busy
- Re-authorization
- Speakerphone exclusive to 911 Emergency

The MLPP service feature is supported only on SIP 3.1 and later software. Users receive a service package with MLPP enabled if the service is configured for MLPP on the ARTS-Avaya Aura® Application Server 5300 server. For information on configuring the MLPP service, see *Avaya Aura® Application Server 5300 Using the Provisioning Client* (NN42040-112).

To enable MLPP, DOD_ENABLE must be configured as YES in the device configuration file.

Precedence

Precedence enables an IP Deskphone user to specify the precedence level of each call that is placed. During call processing, this precedence level is used to assure preferential call completion of higher precedence calls within the same MLPP service domain, even if that means preempting lower precedence calls.

The precedence levels are:

- Routine
- Priority
- Immediate
- Flash
- Flash-Override
- Flash-Override-Override
- Emergency

.A user can initiate a call only with a precedence level equal to or below the authorized precedence level that has been configured for that user. All calls automatically default to Routine, unless a higher precedence is chosen.

Once the precedence level for a call has been set, the precedence level for that call cannot be changed.

Precedence calls cannot be placed to clients that are using SIP software earlier than SIP 3.1.

Precedence level for a call is set either at the IP Deskphone used by the user or through the World Wide Numbering Plan at the Local Session Controller (LSC) Assured Real-Time Services-Avaya Aura® Application Server 5300.

Changing call precedence:

A user must enter a user password before initiating or transferring a call with a precedence level higher than Routine. The user is able to change the default precedence level using the Precedence menu on the IP Deskphone: **Options > Select Precedence**. The menu is available either when dialing or transferring a call.

This feature is also available when dialing from the Address Book, using Speed Dial, or using Redial. There is no limit to the number of password retries.

The ENABLE_SERVICE_PACKAGE parameter must be configured as YES and MLPP must be configured for the user.

Domains

There are three official MLPP domain names (MLPP_NETWORK_DOMAIN): DSN, DRSN and ETS. Each has a pre-defined list of priorities.

Domain name	Priorities
DSN	• Routine • Priority • Immediate • Flash • Flash-Override
DRSN	• Routine • Priority • Immediate • Flash • Flash-Override • Flash-Override-Override • Emergency
ETS	• Emergency • Emergency

The default domain is DSN.

To configure the call precedence level properly, the precedence value configured should match one of the precedence levels available for the MLPP_NETWORK_DOMAIN parameter.

If the MLPP_NETWORK_DOMAIN value does not match any of the values listed in the preceding table, then the list of precedence levels specified for the DSN Network Domain is applied.

Preemption

Higher precedence calls preempt calls lower in precedence when a user has no free call appearances.

If an IP Deskphone reaches the maximum call appearance limit and a higher precedence call is received, then one of the existing calls is preempted in order to present the higher precedence incoming call. An incoming call with a precedence level less than or equal to the already-received call precedence levels is not presented.

IM sessions cannot be preempted because they do not count as a call appearance.

Warning:

Emergency 911 calls can be preempted when there are no available call appearances and there is an incoming above-Routine precedence call.

Order of call preemption:

The following is the order of call preemption:

1. The lowest precedence call
2. If there are multiple calls on the same precedence level, then the following order is used
    a. Any outgoing call that is unanswered
    b. the oldest incoming call that is unanswered
    c. the oldest held call

Call Origination Busy

When Call Origination Busy is enabled, incoming calls are prevented from disturbing the IP Deskphone user when in the process of making an outbound call. When the IP Deskphone is on-hook or off-hook and the first digit or character is entered, then any call that comes in during the entry sequence is not presented. An incoming call that was not presented is then presented when:

- the outbound call is cancelled by pressing Goodbye and the IP Deskphone goes back to the idle state.
- the receiver is placed on-hook and the IP Deskphone goes back to the idle state.
- an outbound call is placed and that outbound call rings.
- an outbound call is placed and receives a busy signal.

Re-authorization

When a user is logged in to an IP Deskphone, and the administrator changes the user password, any attempt by the user to place a call or network request is responded to with an error message.

When the Re-authorization feature is enabled, and a user password is changed by the administrator, the user can, while attempting to make a new call, enter the new password when prompted without having to log out of the IP Deskphone.

If the new password is entered correctly, the call is placed and the password is updated on the IP Deskphone. If an incorrect password is entered, then an error message is displayed, the user hears a busy tone, and the IP Deskphone returns to the idle state.

Speakerphone Exclusive to 911 Emergency

If this feature is enabled, speakerphone is allowed only for making 911 Emergency calls. The speakerphone restriction is applicable to both the Handsfree key and line keys.

As well, when this feature is enabled:

- the Answer soft key is not displayed for an incoming call
- the user cannot answer a call by pressing the Handsfree key or line key, except for calls from the Emergency 911 operator
- the user cannot go handsfree by pressing the Handsfree key

To answer any call except from Emergency 911, the user must go off-hook.

MLPP tones

Unique tones are played when MLPP is enabled.

Precedence Ringback Tone:

A precedence ringback tone is played when the calling party makes a precedence call. This tone is only played after the call has been confirmed by the server.

Precedence alerting tone:

A precedence alerting tone is played to alert the called party that a precedence call is arriving. This tone is delivered through the speaker. The precedence alerting tone is played if there is no active call or a if call is on hold.

Precedence Call Waiting tone:

When a call with a precedence level higher than Routine is received, and the user is busy with another call, the precedence Call Waiting tone is played instead of the normal Call Waiting tone. This tone is delivered through the Handsfree speaker.

Preemption tone:

When a call is preempted, the preemption tone is played. This tone is delivered through the Handsfree speaker.

Feature interactions

The following table describes IP Deskphone feature interaction with MLPP.

Feature	Interaction with MLPP
Call Park	Not available when MLPP is enabled.
Call Forward	Call Forward is the responsibility of the Call Server. Call forwarding is disabled locally on the IP Deskphone if **DoD_Enable** is turned on in the device configuration file.
Call Transfer — Direct	Available, but precedence of the call is maintained.

Table continues…

Feature	Interaction with MLPP
Call Transfer — Consultative	Available. A consultation call can have its own precedence level. The transferred call uses the greater precedence level of the initial call and the consultative call.
Conference call (Ad-hoc conference)	Available. The precedence level of the conference is the highest precedence level of all the joined calls.
Call Waiting Disabled	Not available when MLPP is enabled.
Dialing plan	Available with MLPP, with support for World Wide Numbering available through the Call Server.
Do Not Disturb	Incoming call with a Routine precedence level is rejected when Do Not Disturb is enabled on the IP Deskphone. Incoming call with a precedence level higher than Routine is presented even when Do Not Disturb is enabled on the IP Deskphone.
Multiuser	When MLPP is enabled, only one user can be logged on to the IP Deskphone. If an MLPP user is logged on to the IP Deskphone, other user logons are blocked. If a non-MLPP user is logged on and a MLPP user attempts to log on, then when the IP Deskphone detects the new user is an MLPP user, the MLPP user is automatically logged off. The MLPP user cannot log on until the other user is logged off.
Speakerphone	Available only for 911 calls when the Speakerphone Exclusive to 911 Emergency feature is enabled.

DSCP and MLPP:

The DSCP feature enables the IP Deskphone to classify outgoing traffic by marking each outgoing packet with the proper DSCP value. The User signaling packet and OA&M management packet are marked according to preconfigured DSCP parameters in the device configuration file. When the MLPP feature is enabled, the media packet is marked to a DSCP value converted from the precedence level of each call.

MLPP configuration

MLPP is enabled through a service package on the ARTS-Avaya Aura® Application Server 5300 server.

To enable MLPP on the IP Deskphone, DOD_ENABLE must be configured as YES in the device configuration file

MLPP, Call Origination Busy, and Speakerphone Exclusive to 911 Emergency configuration details, and the network domain and precedence domains to which the user belongs are retrieved from the device configuration file 11xxDeviceConfig.dat. MLPP is disabled until the configuration data has been successfully retrieved.

MLPP onfiguration data for the device configuration file 11xxDeviceConfig.dat is presented in the following table.

Parameter	Description	Default
DOD_ENABLE [YES | NO]	Identifies whether it is DoD ARTS network.	NO
MLPP_NETWORK_DOMAIN [<name>]	The network domain of the user to be added to the INVITE message of outgoing calls.	DSN
MLPP_PRECEDENCE_DOMAIN [x]	The local precedence domain of the user to be added to the INVITE message of outgoing calls.	000000
MAX_APPEARANCE [x]	The maximum number of call appearances a single user can have.	10
CALL_WAITING_TONE [0|1]	Configures the call waiting tone. 0 – single buzz tone 1 – periodic two-beep tone.	0
DISABLE_SPKRPHN [YES | NO]	Disables the speakerphone for all non-911 calls.	NO
CALL_ORIGIN_BUSY [YES |NO]	User is not interrupted (presented with an incoming call) when entering address of outbound call. YES– user is not presented with an incoming call NO – user is presented with an incoming call.	NO

SIP Domain DNS Lookup feature

The DNS Lookup feature enables the IP Deskphone to discover IP addresses for a specified SIP domain using DNS.

There are two ways the DNS Lookup feature can provide SIP domain IP addresses to the IP Deskphone:

1. using DNS SRV records (refer to RFC2782)
2. using DNS A/AAAA records (IPv4/IPv6 address records)

How DNS lookup works

One or two IP addresses can be configured for a particular SIP domain - primary and secondary IP addresses:

- SERVER_IP[x]_1
- SERVER_IP[x]_2

where x = the domain number from 1 to 5.

If the IP Deskphone attempts to log on using these configured addresses and fails to do so, the IP Deskphone then tries to discover the IP addresses using DNS. If there is no primary or secondary SIP domain IP address configured, then the IP Deskphone uses DNS to determine the IP address. If only SERVER_IP[x]_2 is configured (SERVER_IP[x]_1 is 0.0.0.0), then DNS Lookup is used first; if DNS Lookup fails, only then is the secondary IP address tried.

The DNS Lookup feature tries to obtain SIP domain IP addresses through DNS SRV records, using the domain name as a parameter for UDP, TCP, and TLS. Multiple SRV records can be configured for each domain and for each transport protocol (UDP, TCP and TLS). The hostname is returned instead of the IP address. The hostname must point to an address record (A or AAAA record).

SRV record example:

```
_sip._tcp.example.com. 86400 IN SRV 0 5 5060 sipserver.example.com
```

where:

- sip = the desired service
- tcp = the transport protocol
- example.com = the configured domain name
- 5060 = the port to be used
- sipserver.example.com = the SIP proxy to be used (hostname is replaced by the IP address using A/AAAA records)

The DNS Lookup feature then tries to find the IP address of the SIP domain in A/AAAA records on the DNS Server. Only the IP address is returned; therefore, default ports are used — 5060 for UDP/TCP and 5061 for TLS.

Important:

If the Fail Back to Primary feature is enabled, then DNS lookup is not used. In this case, you must configure both primary and secondary IP addresses for a domain.

Caution:

If DNS servers are not properly configured or do not respond, DNS Lookup can take a long time until all necessary requests are sent and corresponding timers expire.

Server Profiles

A System Configuration file allows the administrator to specify a list of domains to which the IP Deskphone can connect. The administrator can specify up to five different SIP domains. Each SIP domain supports 2 SIP servers: the Primary (S1) and the Secondary (S2). The System Configuration file contains the SIP server-specific configuration parameters that are applied to any SIP server specified in the list of SIP domains.

The Server Profiles option supports two different sets of configuration parameters: one specific to the Primary SIP server and one specific to the Secondary SIP server. Each server can be configured separately by updating configuration parameters contained in the System Configuration file with values taken from the Server Profile configuration file. Server Profile parameters are always applied on top of the System Configuration file.

The Server Profile file format is similar to the System Configuration file format, excluding the following configuration parameters:

Table 33: Parameters not included in Server Profile configuration file

SIP_DOMAIN1	SERVER_TCP_PORT2_2	CONFERENCE_URI1
SIP_DOMAIN2	SERVER_TLS_PORT2_2	ADHOC_ENABLED1
SIP_DOMAIN3	SERVER_PORT3_1	MAX_ADHOC_PORTS1
SIP_DOMAIN4	SERVER_TCP_PORT3_1	CONFERENCE_URI2
SIP_DOMAIN5	SERVER_TLS_PORT3_1	ADHOC_ENABLED2
SERVER_IP1_1	SERVER_PORT3_2	MAX_ADHOC_PORTS2
SERVER_IP1_2	SERVER_TCP_PORT3_2	CONFERENCE_URI3
SERVER_IP2_1	SERVER_TLS_PORT3_2	ADHOC_ENABLED3
SERVER_IP2_2	SERVER_PORT4_1	MAX_ADHOC_PORTS3
SERVER_IP3_1	SERVER_TCP_PORT4_1	CONFERENCE_URI4
SERVER_IP3_2	SERVER_TLS_PORT4_1	ADHOC_ENABLED4
SERVER_IP4_1	SERVER_PORT4_2	MAX_ADHOC_PORTS4
SERVER_IP4_2	SERVER_TCP_PORT4_2	CONFERENCE_URI5
SERVER_IP5_1	SERVER_TLS_PORT4_2	ADHOC_ENABLED5
SERVER_IP5_2	SERVER_PORT5_1	MAX_ADHOC_PORTS5
SERVER_PORT1_1	SERVER_TCP_PORT5_1	DNS_DOMAIN
SERVER_TCP_PORT1_1	SERVER_TLS_PORT5_1	DHCP_ENABLE
SERVER_TLS_PORT1_1	SERVER_PORT5_2	ENABLE_USB_PORT
SERVER_PORT1_2	SERVER_TCP_PORT5_2	USB_HEADSET
SERVER_TCP_PORT1_2	SERVER_TLS_PORT5_2	ENABLE_BT
SERVER_TLS_PORT1_2	EAP	PCPORT_ENABLE
SERVER_PORT2_1	EAPID1	
SERVER_TCP_PORT2_1	EAPID2	
SERVER_TLS_PORT2_1	EAPPWD	
SERVER_PORT2_2	LLDP_ENABLE	
AUTOLOGIN_ENABLE	AUTOLOGIN_ID_KEYxx	
AUTOLOGIN_PASSWD_KEYxx	AUTOLOGIN_AUTHID_KEYxx	

All Server Profile files are uploaded to the IP Deskphone through the standard upgrade mechanism. When switching from one server to another server, the IP Deskphone applies the configuration parameters for the appropriate server.

The Server Profile option is implemented using the following command parameters:

- **PRIMARY_SERVER_PROFILE <filename>**
- **SECONDARY_SERVER_PROFILE <filename>**

The commands are processed as follows:

1. If the x_SERVER_PROFILE command is specified and contains the x Server Profile <filename>, the Server Profile file is downloaded to the IP Deskphone during the standard upgrade mechanism after downloading the System Configuration file.

   If the Server Profile file is specified but cannot be downloaded, the IP Deskphone uses the old Server Profile file, if it exists in the Flash File System (FFS). If there is no old Server Profile file, the IP Deskphone applies the parameters from the System Configuration file by default.

   For example: **PRIMARY_SERVER_PROFILE profile01.dat** — applies values from the **profile01.dat** file for the Primary server

2. If the x_SERVER_PROFILE command is specified, but the parameter is absent, the IP Deskphone applies the parameters from the System Configuration file by default for this server. The old Server Profile file is removed from the FFS.

   For example: PRIMARY_SERVER_PROFILE <blank> — uses configuration parameters taken from the System Configuration file and removes the old Server Profile file designated for the Primary Server

3. If the „x_SERVER_PROFILE' command is not specified or is skipped, the IP Deskphone applies the configuration values obtained from the old Server Profile file, if it exists. Otherwise, the configuration values are taken from the System Configuration file by default.

Note:

If the IP Deskphone is reset to factory default, all profiles are removed.

The Primary and Secondary Server Profile file names are displayed in the Server Settings menu of the IP Deskphone.

Limitations:

Only one server profile can be active at time; this means that in Multi-User mode, the logic is applied for only the Primary User.

IP Deskphone soft reboot

When a different server profile is applied, changes to certain parameters can cause the IP Deskphone to perform a soft reboot.

Changes to the following parameters initiate a soft reboot.

FIPS_MODE	ENABLE_UPDATE	ENABLE_USB_PORT
SFTP_WRITE_PATTERNS	SESSION_TIMER_ENABLE	USB_HEADSET
SFTP_READ_PATTERNS	SESSION_TIMER_DEFAULT_SE	ENABLE_BT

Table continues…

MLPP_NETWORK_DOMAIN	SESSION_TIMER_MIN_SE	PCPORT_ENABLE
MLPP_PRECEDENCE_DOMAIN	SET_REQ_REFRESHER	LLDP_ENABLE
SNTP_ENABLE	SET_RESP_REFRESHER	EAP
IPV6_ENABLE	DOD_ENABLE	EAPID1
IPV6_STATELESS	SLOW_START_200OK	EAPID2
SIP_TCP_PORT	MAX_APPEARANCE	EAPPWD
SIP_TLS_PORT	USE_PUBLISH_FOR_PRESENCE	

Managing Server Profile files

To download a new Server Profile file, the Server Profile parameters must first be configured in the System Configuration file and provisioned in the Device Configuration file. The IP Deskphone downloads the new Server Profile file on startup, or the download can be initiated through pressing the **Services** key on the IP Deskphone, and selecting **Check for Updates > Upgrade [DEVICE_CONFIG]** from the menu

Information about profiles is presented in the IP Deskphone File Manager. If a Server Profile file is downloaded on the IP Deskphone, the file name (profile1.dat or profile2.dat) is displayed in the System folder of the File Manager.

To delete a Server Profile on the IP Deskphone, press the **Delete** soft key; the profile is completely removed from flash and main memory. When a server profile is deleted, if parameters in the server profile have corresponding parameters in the System Configuration file, then those System Configuration file parameters are implemented after the server profile parameters are deleted.

The contents of each file can be viewed by using the **prtcfg** command in the PDT shell or by using the **printProfConfig <n>** command in the vxshell where <n> is one of the following values:

- 0 — root System Configuration file
- 1 — first profile
- 2 — second profile
- 3 — all profiles
- any other value — all profiles

Auto Login parameters in server profiles

In SIP 4.4 and later, a user can now have a different auto-login for each server.

If the IP Deskphone configuration parameter AUTOLOGIN_ENABLE is configured as 2 or USE_AUTOLOGIN_ID, then the UserID, AuthID, and Passwd values are extracted from the AUTOLOGIN[_ID_KEY|_AUTHID_KEY|_PASSWD_KEY] configuration parameters.

Server profiles support all configurations of the AUTOLOGIN_ENABLE parameter.

If the AUTOLOGIN_ENABLE parameter in a profile is configured as 0 (or NO) or 1 (or YES), then the configuration file behaves as if there was no profile.

If the AUTOLOGIN_ENABLE parameter in the profile is configured as 2 (or USE_AUTOLOGIN_ID), the IP Deskphone performs a soft reset. After the soft reset, users specified by the AUTOLOGIN[_ID_KEY|_AUTHID_KEY|_PASSWD_KEY] configuration parameters are logged in.

If the profile does not contain the AUTOLOGIN_ENABLE parameter, the parameter from the System Configuration file is used.

Note:

Auto login user names and passwords are not printed using the **`prtcfg`** command as they are not stored in the system configuration file and are secure parameters which should not be displayed.

Example of Auto-Login parameters in config file

The following example shows the AUTOLOGIN parameters as they might be used in phone's config file. In this example, the PROMPT_AUTHNAME_ENABLE is YES, so the AUTOLOGIN_AUTHID_KEYnn parameter is included for each login.

```
AUTOLOGIN_ENABLE USE_AUTOLOGIN_ID
PROMPT_AUTHNAME_ENABLE YES
# DN Key 1
AUTOLOGIN_ID_KEY01 7903@mydomain.com
AUTOLOGIN_AUTHID_KEY01 steven
AUTOLOGIN_PASSWD_KEY01 7654
# DN Key 2
AUTOLOGIN_ID_KEY02 7904@mydomain.com
AUTOLOGIN_AUTHID_KEY02 steven
AUTOLOGIN_PASSWD_KEY02 7654
```

Chapter 12: IP Deskphone restrictions

Service package restrictions

A limited number of Call Servers support the service package. The service package is a means of providing configuration settings to the IP Deskphone.

Individual features and feature restrictions are sent to the IP Deskphone as a part of the service package every time a particular user logs on to the IP Deskphone. If the Call Server does not support service packages, or if the Call Server restricts some of the features in the service package, functionality of some features is restricted.

If functionality is restricted, the associated buttons and context-sensitive soft keys are not accessible or do not respond.

Chapter 13: Security

This chapter describes the following security features:

- SIP over TLS
- Connection persistence
- SRTP
- SFTP
- SSH
- Last successful or unsuccessful logon
- Enhanced administrative password security
- Debug port security

SIP over TLS

To avoid security problems such as message integrity attacks, SIP over TLS uses Transport Layer Security (TLS) to provide secure communication between the Avaya 1100 Series IP Deskphone and the SIP proxy.

Transport Layer Security (TLS) protects SIP signaling traffic. It sits on top of the Transmission Control Protocol (TCP), the preferred default protocol for SIP traffic. You can use TLS with a user name and password to provide a means of server-only authentication. IP Deskphone-specific Public Key certificates can provide even stronger mutual-authentication of both the server and the IP Deskphone.

Using SIP over TLS protects SIP messages on a hop-by-hop basis. To achieve complete end-to-end security through the use of TLS, each element involved in the system must also be capable of securing SIP traffic using TLS.

Connection persistence

Connection persistence allows the IP Deskphone to establish a connection and monitor the connection for failure by using "keep-alive requests.

The IP Deskphone establishes connection with the proxy using the commonly accepted ports. Periodically, based on a configured timer value, the IP Deskphone issues a request to the server to verify that the connection with the server at the TCP level is still active. When the IP Deskphone discovers that the keep-alive packet has not been answered, it attempts to reestablish a connection with the proxy. If this is successful, the IP Deskphone reregisters with the proxy (and sends a new subscription requests where appropriate). If it is not possible to reestablish the connection, the IP Deskphone falls back into a state where connection attempts are tried periodically based on random, but increasing time periods, in order to give the server adequate time to recover.

SSH and secure file transfer

The Secure Shell Handler (SSH) is a widely-used protocol for providing secure logon access to run commands remotely. To establish a connection, you must access the SSH-capable client, and know the user name and password that is configured on the IP Deskphone through the use of the provisioning system.

Secure File Transfer Protocol (SFTP) lets the administrator securely log on to the IP Deskphone (using the common user name and password shared with SSH/PDT). After you logon, the IP Deskphone displays a list of files on the flash file that you can transfer.

SSH and SFTP

The following table provides a list of SSH and SFTP configuration parameters.

Parameter	Description	Default value	Boundaries
Enable SSH	Enables the SSH server on the IP Deskphone for secure shell access.	Not checked (off)	Not checked (off) Checked (on)
Enable SFTP	Enables the SFTP server on the IP Deskphone for secure FTP access. SSH must be enabled for SFTP to be enabled	Not checked (off) (appears dimmed until SSH is enabled)	Not checked (off) Checked (on)
User ID	The User ID that must be entered when connecting to the IP	None	Non-null string Maximum: 11 characters

Table continues…

Parameter	Description	Default value	Boundaries
	Deskphone SSH or SFTP.		
Password	The password that must be entered when connecting to the IP Deskphone through SSH, SFTP.	None	Non-null string Maximum: 11 characters

UI Properties for Device Settings SSH and SFTP parameters are as follows:

- The User ID field is empty and the Password field displays "****" when both SSH and SFTP are disabled and applied.
- The user can enable SSH or SFTP.
- The user must provide a valid user ID and password when the User ID field is empty, and an application (SSH or SFTP) is selected. If a valid user ID and valid password are not provided, and the user presses the **Apply** context-sensitive soft key, one of the following error message appears:
  - `Enter [4..11] chars` – appears if a valid user ID is not provided.
  - `Enter [4..11] chars` – appears if a valid password is not provided.
  - `Enter [4..11] charsEnter [4..11] chars` – appear if both a valid user ID and a valid password are not provided.

TCP/TLS operation overview

TCP is the alternative protocol the IP Deskphone uses when sending and receiving SIP requests. Avaya recommends TCP for Avaya SIP-enabled entities.

When a server initiates a TCP or TLS connection to the IP Deskphone, the connection only lasts as long as the server chooses to keep the connection open; a persistent connection is not maintained by the IP Deskphone.

How the IP Deskphone uses TCP

TCP is a connection-based protocol, which means the IP Deskphone must first establish a connection with a target. This is done using a three-way handshake. After the handshake process is complete and a connection is made, the IP Deskphone can send data over the TCP connection. The data, which makes up a SIP request, can now be sent and received by either side of the communication.

How the IP Deskphone uses TLS

Transport Level Security (TLS) is a protocol for establishing a secure connection between two end-points. After a connection is established using TCP, TLS negotiates the cryptographic parameters used to secure the traffic that is sent over that connection. TLS, Public Key Cryptography, and X. 509 certificates provide either mutual or server authentication.

- Mutual authentication occurs when both the client and the server have public key certificates assigned, that are used during the TLS handshake, to validate the identity of both communicating parties. Both the server and the end point device certificates are "signed" by well-known trusted certificate authorities.
- Server authentication occurs when a server has a certificate signed by a certificate authority. The certificate is only used for the client to validate the identity of the server it is connected to. After the TLS connection is established, the server can identify the IP Deskphone through a user name and password.

How TLS impacts SIP

TLS impacts SIP in the following ways:

- URIs – contain transport parameters used to indicate the preferred method of contact. For example,

  `Contact: Bob<sip:bob@company.com;transport=tls>`

  Important:

  A transport parameter of TLS indicates that the server or client prefers TLS to be used for communication.

  SIP Software Release 4.0 and later adds transport=tls to the contact header when using TCP or TLS.
- VIA header – contains the transport protocol used to send a request. For example, Via: SIP4.1/TLS `bob.company.com;....;alias`

  The IP Deskphone attempts to downgrade the allowed protocols if connection attempts are made and fail. In order to avoid the IP Deskphone using an unsecure protocol, only TLS is enabled.

  The order of preference for protocols is always: TLS, TCP, and UDP.

  You must enable the SIP TLS Listening port for incoming TLS connections to be made.

Certificate requirements

For the IP Deskphone to validate that the server certificate provided by the TLS-enabled proxy matches the connected address, the certificate must contain the IP Addresses of the IP Deskphone.

The server certificate has a Subject Alternative Name field, which contains the IPv4 and IPv6 IP addresses that correspond with the proxy. For example:

```
subjectAltName=IP:192.168.100.100subjectAltName=IP:
2001:0db8:0000:0000:0000:0000:1428:5 7ab
```

Important:

The IP Deskphone must have a device certificate loaded. If the device certificate is not loaded, the IP Deskphone fails to establish a TLS connection with the system.

IP Deskphone configuration

The following table lists the various security parameters for the IP Deskphone.

Table 34: Provisioning parameters summary

Parameter	Purpose	Default	Allowed
SERVER_TCP_PORT1_1 1 SERVER_TCP_PORT1_2 SERVER_TCP_PORT2_1 SERVER_TCP_PORT2_2 SERVER_TCP_PORT3_1 SERVER_TCP_PORT3_2 SERVER_TCP_PORT4_1 SERVER_TCP_PORT4_2	Configures the TCP and TLS ports used when connecting to the SIP domain.	TCP: 5060 TLS: 5061	Integer

Table continues…

Parameter	Purpose	Default	Allowed
SERVER_TCP_PORT5_1 SERVER_TCP_PORT5_2 SERVER_TLS_PORT1_1 SERVER_TLS_PORT1_2 SERVER_TLS_PORT2_1 SERVER_TLS_PORT2_2 SERVER_TLS_PORT3_1 SERVER_TLS_PORT3_2 SERVER_TLS_PORT4_1 SERVER_TLS_PORT4_2 SERVER_TLS_PORT5_1 SERVER_TLS_PORT5_2			
SIP_UDP_PORT SIP_TCP_PORT SIP_TLS_PORT	Configures the local SIP listening ports. After you change the listening ports parameters through the Check For Updates functionality, you must restart the IP Deskphone to apply the modified values.	UDP: 5060 TCP: 5060 TLS: 5061	Integer
CONN_KEEP_ALIVE	Configuration values that affect connection persistence.	30	Min: 15 Max: 1800
REGISTER_RETRY_TIME		30	Min: 30 Max: 1800
REGISTER_RETRY_MAX TIME		1800	Min: 600 Max: 1800

Table continues…

Parameter	Purpose	Default	Allowed
KEEPALIVE_RETRIES		3	Min: 0 Max: 10 See Managing connection persistence on page 258.
SRTP_ENABLED SRTP_MODE	SRTP configuration values.	No BE-2MLines	BE-2MLines BE-Cap Neg SecureOnly
SRTP_CIPHER_1 SRTP_CIPHER_2	Allows configuration of the preferred order for SRTP cipher offers.	AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32	AES_CM_128_HMAC_SHA1_32 AES_CM_128_HMAC_SHA1_80 None
LOGIN_NOTIFY	Configures whether or not the login banner appears after a successful logon.	Off	Off Success Failure Both
LOGIN_NOTIFY_TIME	Configures whether or not the time at which the login success or failure occurred appears.	Not checked	Not checked (off) Checked (on)
SSH	Configuration of the SSH server on the IP Deskphone. The parameter must remain consistent with the current UNIStim design.	NO	YES NO
SFTP	Configuration of the SFTP server on the IP Deskphone. The parameter must be added, but can remain consistent with SSH.	NO	YES NO
SFTP_READ_PATTERNS	File extensions allowed to read (get) from the SIP client.	.cfg,.dat	"," separated values. See Note 1. After a change is detected in this parameter, the system resets.
SFTP_WRITE_PATTERNS	File extensions allowed to write (put) from SIP client.	.cfg,.dat	"," separated values. See Note 1 and Note 2.

Table continues…

Parameter	Purpose	Default	Allowed
			After a change is detected in this parameter, the system resets.
SSHID	Configuration of the SSH and SFTP user ID.	None	See Note 3.
SSHPWD	Configuration of the SSH and SFTP password.	None	See Note 3.
HASHED_ADMIN_PASS W ORD	Indicates whether the Admin Password is hashed or not.	NO	YES NO
ENALBE_LOCAL_ADMI N_ UI	Configures the availability of the local administration UI on the IP Deskphone.	YES	YES NO
HASH_ALGORITHM	Hash algorithm.	SHA1	SHA1 MD5
MKI_ENABLE	Use Master Key Identifier (MKI) or not.	NO	YES NO
ALLOW_EMERGENCY_ PRIORITY_HEADER	Indicates if "Priority: emergency" header must be added to emergency outgoing calls or not.	NO	YES NO
CALLINFO_IMAGE_ENA BLE	Specify whether to obtain image from "Call-Info" url or not.	NO	YES NO
SECURE_UI_ENABLE	Configures the availability of other sensitive data that you want to hide from the normal end user, such as the IP address, the MAC address on the IP Deskphone information screen, and the FE IP Address and Port on the audio quality details screen.	NO	YES NO
ADMIN_PASSWORD_E XPIRY	The date that the configured ADMIN_PWD is no	Empty	Timestamp

Table continues…

Parameter	Purpose	Default	Allowed
	longer valid, and a new password must be downloaded from the provisioning server.		

Note:

Note 1: The SFTP file read and write pattern entries must be strictly followed.

The following are examples of valid and invalid formats of SRTP read and write patterns.

Example of valid formats:

SFTP_READ_PATTERNS: cfg,.rel,.re2,.re3,.dat SFTP_WRITE_PATTERNS: cfg,.txt,.wr1,.wr2

Example of an invalid format:

.cfg, .txt

For the SFTP file read and write pattern entries to be valid, there must be no space between the extensions.

Note:

Note 2: SFTP writes can only be made to the sftpWr folder. You are only allowed to write a file that is 10%, or less, of the available space on the folder.

If a file size greater than 10% is written, a write failure occurs, and the system logs the following event:

```
1042[Minor][TUE JAN 02 19:08:18 2007][353][i:/fw/build/../util/sshapp/
sftpS erver.c:691] - File (./sftpWr/lf.wrl) too large to write.
```

Note:

Note 3: If logon failures occur for SSH and SFTP applications, the system logs the following event:

```
1040[Minor][TUE JAN 02 20:12:14 2007][4189][i:/fw/build/../sshapp/
sshServer .c:616] - SSH Authentication Failed.
```

Manually configure the IP Deskphone for UDP and TCP

After you enable the administration user interface, you can manually change network settings on the IP Deskphone. You can manually configure the IP Deskphone through the Server Settings menu.

Note:

To meet security requirements, the local administration user interface of the IP Deskphone can be disabled for deployed IP Deskphones. If this is the case then you must manually configure the parameters during initial IP Deskphone configuration or through the provisioning server.

Note:

Disabling the local administration user interface drastically reduces the ability to view or edit the configuration of the IP Deskphone, and almost completely removes the ability to diagnose any communication or configuration errors in the field. However, disabling the local administration user interface increases the security of the IP Deskphone because the user is not able to view the configurations or make changes.

Configuring the domain protocol

1. Press the **Globe** key twice.
2. Using the Navigation key cluster, select **Server Settings**..
3. Select a domain.
4. Enter the admin password (if the UI and password are enabled).
5. Use the Navigation key cluster to scroll through the Domain List screen and select the required configured SIP domain.
6. Press the **Edit** context-sensitive soft key.

Table 35: Listening port parameters

Parameter name	Description	Default value	Boundaries
SIP UDP Port	The listening port on the IP Deskphone for incoming UDP requests.	5060	Min: 1024 Max: 65535 Disabled: 0 (must be non-zero for a TLS-only option)
SIP TCP Port	The listening port on the IP Deskphone for incoming TCP requests.	5060	Min: 1024 Max: 65535 Disabled: 0 (must be non-zero for a TLS-only option)
SIP TLS Port	The listening port on the IP Deskphone for incoming TLS requests.	0	Min: 1024 Max: 65535 Disabled: 0 (must be non-zero for a TLS-only option)

Note:

The configuration of the IP Deskphone for various protocols must be completed for outgoing and incoming connections. For a complete TLS-only option, the outgoing server UDP and TCP protocols must be configured as a non-zero value, and the incoming UDP and TCP listening ports must be configured as a non-zero value.

Using the TLS to connect to the SIP proxy

The IP Deskphone can establish a connection with the proxy after the appropriate configurations are made for the TLS. After the IP Deskphone registers with the SIP Proxy, the user can detect if a secure connection is established by the presence of a security icon (padlock) on the idle screen.

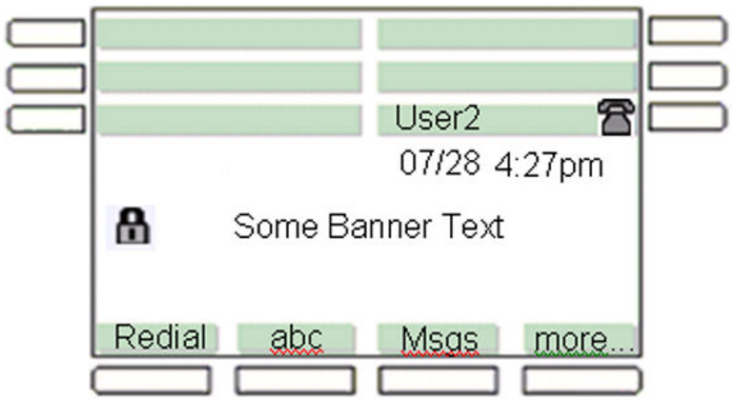


Figure 35: Security icon enabled

Note:

Connecting to the server requires that the IP Deskphone uses, at a minimum, TLS_RSA_WITH_AES_128_CBC_SHA, and as an objective, TLS_RSA_WITH_AES_256_CBC_SHA. Because this is a server-specific configuration, the IP Deskphone must be prepared to handle both. There is no difference in screen indication, regardless of the type of cipher used.

The following table describes the configurations that affect the presence of the security icon on the idle screen of the IP Deskphone.

Configuration	Result	Idle Screen Security Icon Display
Default: UDP + TCP	SIP is unsecured.	No
UDP only	SIP is unsecured.	No
TCP only	SIP is unsecured.	No
TLS only	Connection is only established if SIP is secure.	Yes
UDP + TLS: unsupported	Unsupported.	Unsupported
TCP + TLS	Connection is established with either TCP or TLS.	Yes – only if TLS connection is used No – if fall back to TCP occurs
UDP + TCP + TLS	Connection is established using TCP or TLS, potentially falling back to using only UDP.	Yes – only if TLS connection is established

Table continues…

Configuration	Result	Idle Screen Security Icon Display
		No – if fall back to TCP or UDP occurs
None : unsupported	Unsupported	Unsupported

Unsupported configurations cannot be saved. If the configurations are unsupported, the IP Deskphone displays an error message.

The following is an example of an error message for unsupported configurations:

```
Unsupported: UDP + TLS
```

```
Unsupported: No protocols enabled.
```

Registration behavior based on configuration settings

The following table describes the behavior of the IP Deskphone when the IP Deskphone is configured to communicate with a server using specific protocols.

Table 36: Registration results based on configuration

Configuration	Description	Expected result	Possible results
IP Deskphone: UDP + TCP Server: UDP + TCP + TLS	The IP Deskphone allows protocols enabled for communication with the server.	The IP Deskphone establishes a connection to the server using TCP.	If the server does not accept incoming requests on TCP, it takes approximately thirty seconds for the initial connection attempt to fail, and then the IP Deskphone attempts to contact the server using UDP. If this connection also fails, the IP Deskphone waits a configured period of time before attempting to reconnect.
IP Deskphone: UDP Server: UDP + TCP + TLS	The IP Deskphone only has UDP enabled for sending requests to the server.	The IP Deskphone registers using UDP as the protocol.	If the IP Deskphone is unable to contact the server, it waits a configured period of time before attempting to reconnect.
IP Deskphone: TCP only Server: UDP	The IP Deskphone only has TCP enabled for sending requests to the server.	The IP Deskphone registers using TCP as the protocol.	If the IP Deskphone is unable to contact the server, it waits a configured period of time before attempting to reconnect.

Table continues…

Configuration	Description	Expected result	Possible results
+ TCP + TLS			
IP Deskphone: TLS only Server: UDP + TCP + TLS	The IP Deskphone only has TLS configured for sending requests to the server. The IP Deskphone must have a device certificate installed if the server is configured for mutual authentication.	The IP Deskphone registers using SIP over TLS. If a device certificate is provisioned, and the server is configured for mutual authentication, then the IP Deskphone provides a certificate during the TLS handshake. Otherwise, server-only authentication is used.	If the IP Deskphone is unable to contact the server, it waits a configured period of time before attempting to reconnect.
UDP + TLS: unsupported	Unsupported	Unsupported	Unsupported
IP Deskphone: TCP + TLS Server: UDP + TCP + TLS	The IP Deskphone attempts to contact the server using TLS first, because TLS has higher priority than TCP.	The IP Deskphone registers the same as if it was configured for TLS only.	If the IP Deskphone is unable to connect to the server using TLS, it attempts to connect using TCP. If attempts to connect using TLS and TCP fail, the IP Deskphone waits a configured period of time before attempting to reconnect.
IP Deskphone: UDP + TCP + TLS Server: UDP + TCP + TLS	The IP Deskphone attempts to contact the server using TLS first, because TLS has higher priority than TCP and UDP.	The IP Deskphone registers the same as if it was configured for TLS only.	If the IP Deskphone is unable to connect to the server using TLS, it attempts to connect using TCP. If attempts to connect using TLS and TCP fail, the IP Deskphone attempts to connect using UDP. If attempts using TLS, TCP, and UDP fail, the IP Deskphone waits a configured period of time before attempting to reconnect.
None: unsupported	Unsupported	Unsupported	Unsupported

Note:

The server must be configured with the appropriate protocols enabled for the success condition to be realized. Failure results are possible if the server configuration is changed to disallow protocols.

Managing connection persistence

The IP Deskphone attempts to establish and maintain a persistent connection with the proxy when TCP and TLS are active protocols. After this connection is established, the IP Deskphone sends all outgoing connections over this persistent connection.

SIP IP Deskphones and servers, which use UDP to communicate, listen for incoming connections on known ports, and originate each request on a randomly selected UDP port. Even if TCP is used, new requests can potentially be sent using a new source port unless the connection between the IP Deskphone and proxy is kept active.

Connection persistence does the following:

- Keeps a connection established between a client and the outgoing proxy.
- Reuses the open connection for future incoming and outgoing requests.

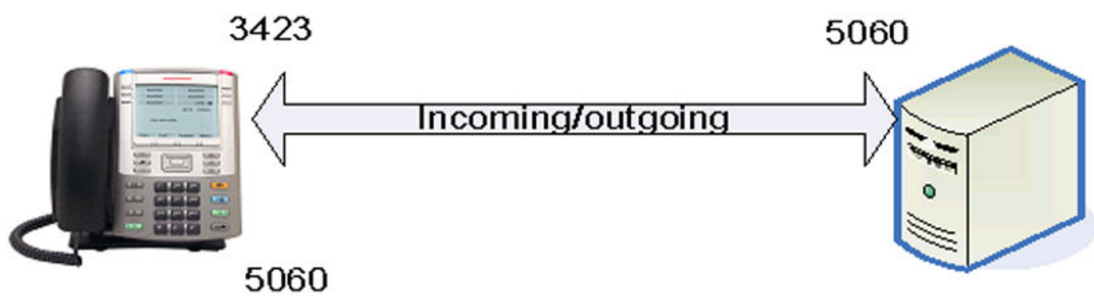


Figure 36: Incoming/Outgoing with connection reuse

When using UDP, an IP Deskphone behind a firewall must periodically send a request to the server to maintain an open pinhole in the firewall so that the server can contact the IP Deskphone when sending requests.

When using TCP/TLS and connection persistence, it is not necessary to send a SIP_PING to the server in order to keep a pinhole alive, and the keep-alive mechanism is reduced to a method which involves significantly less overhead.

The following figure demonstrates how critical it is that the server can communicate directly with the IP Deskphone through the use of the established TCP connection because it has no way of getting through the firewall in order to contact port 5060 on the IP Deskphone.

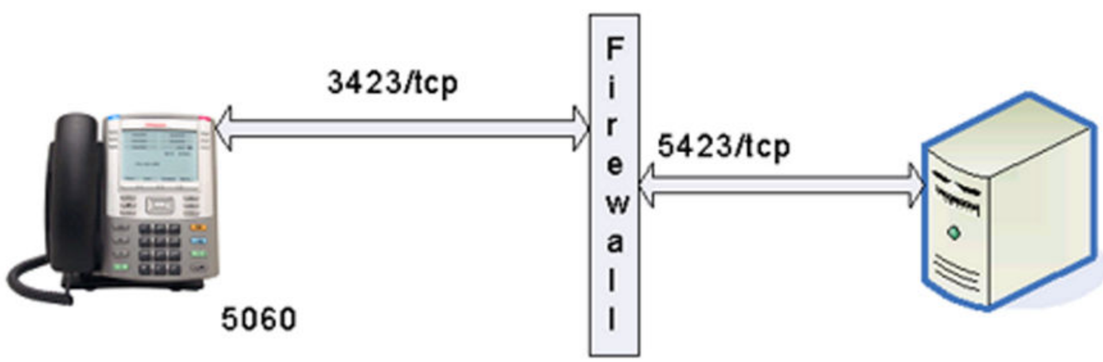


Figure 37: Connection reuse and a firewall

Table 37: Connection timers definitions and allowed values

Parameter name	Description	Default value	Boundaries
OS Keep-alive only	Selecting this value causes the OS TCP Keep-alive functions to be used instead of the CRLF ping/pong mechanism. Some system deployments may prefer the lighter weight TCP keep-alive	Not checked	Checked
Keep-alive	This is a value, measured in seconds, that the IP Deskphone uses when a connection to the server is established using TCP or TLS. The IP Deskphone periodically sends a packet to the server, which contains a pair of CRLF, to ensure the server is responding.	30	Min: 5 Max: 1800
Register Retry	When a connection failure occurs, this value in seconds is how long the IP Deskphone waits before attempting to reregister with the proxy.	30	Min: 30 Max: 1800
Register Max Retry	After a failure to reconnect with the proxy, the IP Deskphone increases the amount of time that it waits for the next registration retry attempt. This value, measured in seconds, is the maximum value that the IP Deskphone waits in between retry attempts	1800	Min: 600 Max: 1800

SRTP

Secure Real-time Transport Protocol (SRTP) encrypts the Real-time Transport Protocol (RTP) traffic between two end-points to achieve full security for the media path.

Security Descriptions for the Session Description Protocol (SDESC) (RFC4586) defines a mechanism to transmit the necessary cryptographic parameters between two end-points. SRTP is initiated when Secure Real-time Transport Control Protocol (SRTCP) allows both sides of a conversation to agree on the keys you can use to encrypt or decrypt the messages that are transmitted.

Media security — SRTP

Secure RTP (SRTP) encrypts the media path between two end-points. After both end-points agree on the necessary parameters to encrypt and decrypt audio packets, the voice path between them is established.

SRTP is configured on the IP Deskphone to provide multiple levels of protection.

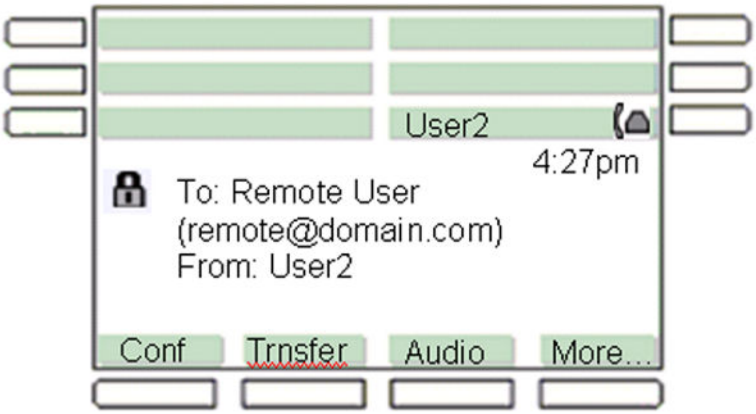
The following table highlights the two cipher suites that are used and their related parameters.

Table 38: SRTP properties

Parameter	AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_32
Master key length	128 bits	128 bits
Master salt length	112 bits	112 bits
SRTP lifetime	2^48 packets	2^48 packets
SRTCP lifetime	2^31 packets	2^31 packets
Cipher	AES Counter Mode	AES Counter Mode
Encryption key	128 bits	128 bits
MAC	HMAC-SHA1	HMAC-SHA1
SRTP auth. tag	80 bits	32 bits
SRTCP auth. tag	80 bits	80 bits
SRTP auth. key len.	160 bits	160 bits
SRTCP auth. key len.	160 bits	160 bits

Call security is identified by the presence of the security icon present during an active call, as shown in the following example.

The presence of the security icon is the only visible indication that the media path is encrypted. The presence of this icon depends on whether the IP Deskphone has been configured to support SRTP or not and is visible when the IP Deskphone is not in the idle screen.



Available SRTP configurations are provided in the following table.

Table 39: Configuration effects on media security display

Configuration	Result	Media Security Icon Display (during active call)
Default: UDP + TCP, no SRTP	SIP is unsecured; media is unsecured.	No
UDP + TCP. Best-Effort SRTP	SIP is unsecured; media is encrypted, but due to transmission of crypto parameters in clear text, the media cannot be considered secure.	No
UDP + TCP, SRTP-Only	SIP is unsecured; media is encrypted, but due to transmission of crypto parameters in clear text, the media cannot be considered secure.	No
TLS, no SRTP	SIP is secured; media is unencrypted.	No
TLS, Best-effort	SIP is unsecured; media is encrypted only if both end-points agree on use of SRTP.	Yes/No, depending on negotiation
TLS, SRTP Only	SIP is secured, media is encrypted. If both end-points do not agree on the use of SRTP, the connection fails.	Yes

The security icon indicates the security status of a call, and is useful for best-effort environments where there is a possibility of an unsecured call or where TLS is not used to communicate with the proxy.

Note:

The FAST_EARLY_MEDIA_ENABLE option must be set to NO to support SRTP.

Last successful or unsuccessful logon

You can configure the IP Deskphone to provide the user with logon feedback regarding the last successful logon or the last unsuccessful logon, and provide the local time at which logon feedback was logged (assuming that the IP Deskphone has the correct time configured). The time is correct when the IP Deskphone successfully retrieves the correct time during a successful logon process, or through the use of SNTP.

The display of a logon success and failure notification is local only to the IP Deskphone being used, and displays the last time that a user successfully logged on to the IP Deskphone or failed to log on to the IP Deskphone.

The figures shown below provide examples of the IP Deskphone display screen based on the configuration of the IP Deskphone and whether Login Notify is enabled or not.

The following notification appears on the display screen when the user login ID or password is incorrect and log in fails.

Note:

The server recognizes account login failure thresholds. After a configurable number of failures, the server temporarily disallows login attempts for an account. The IP Deskphone does not display any indication of this lockout.

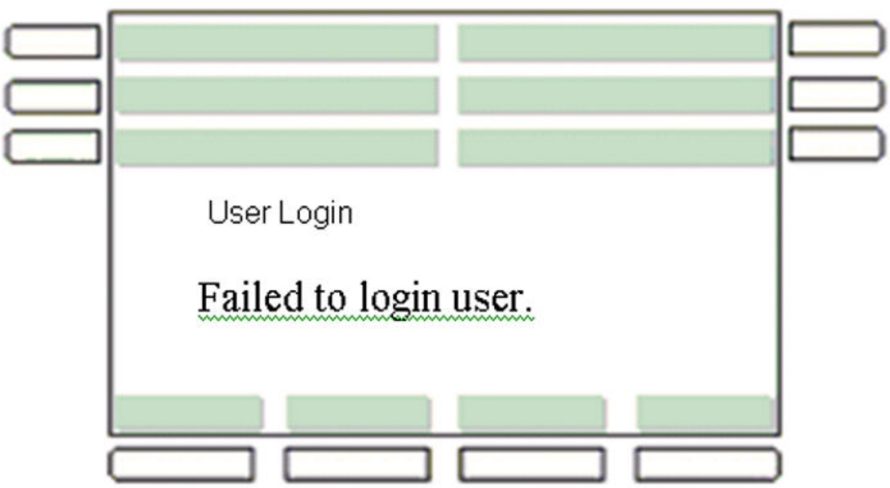


Figure 38: New login failure notification

The following notification appears on the display screen when the user successfully logs on.

Figure 39: Basic login notification

The following notification appears on the display screen when the user successfully logs on when Login Notify with Time is enabled.

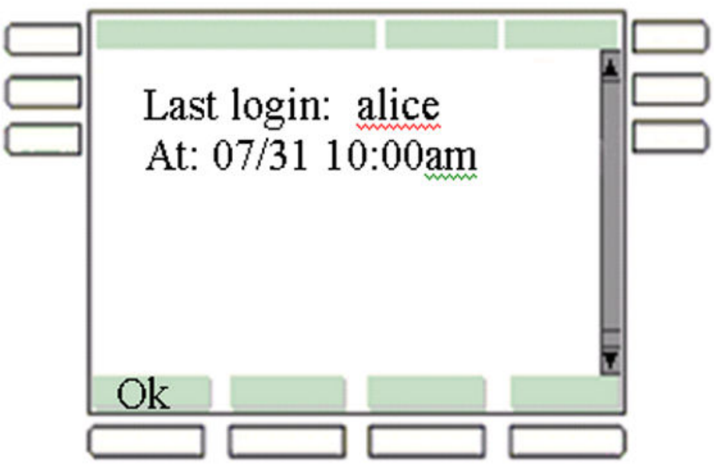


Figure 40: Basic login and time notification

The following notification appears on the display screen to notify the user of the last unsuccessful log on attempt made.

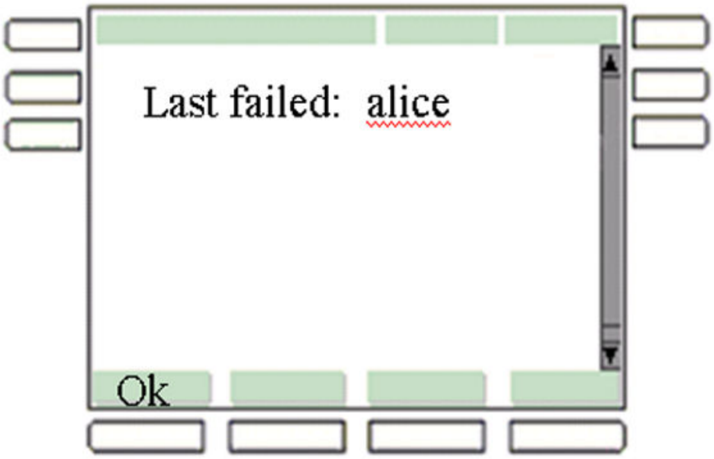


Figure 41: Login failure notification

The following notification appears on the display screen to notify the user of the date and time of the last unsuccessful log on attempt made.

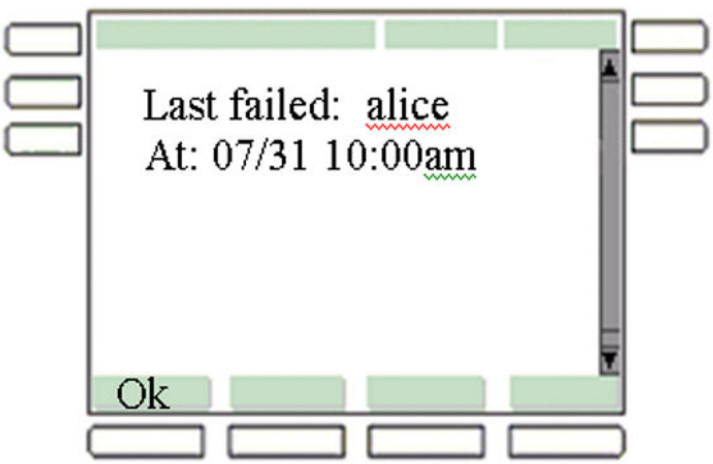


Figure 42: Login failure with time notification

The following notification appears on the display screen to notify the user of the last successful and unsuccessful log on attempts made.

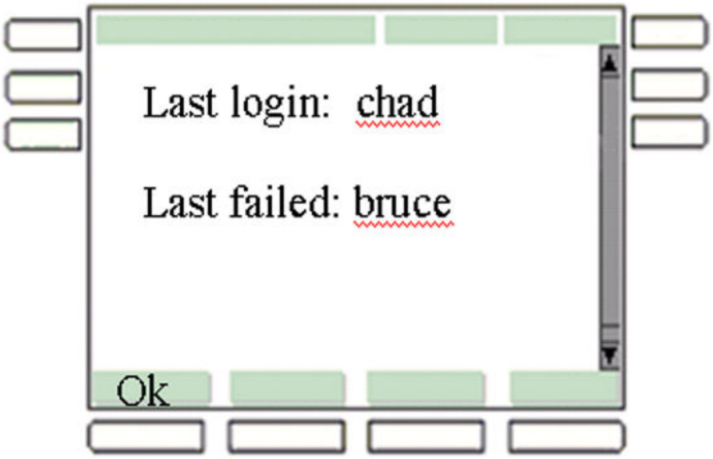


Figure 43: Login and login failure notification

The following notification appears on the display screen to notify the user of the date and time of the last successful and unsuccessful log on attempts made.

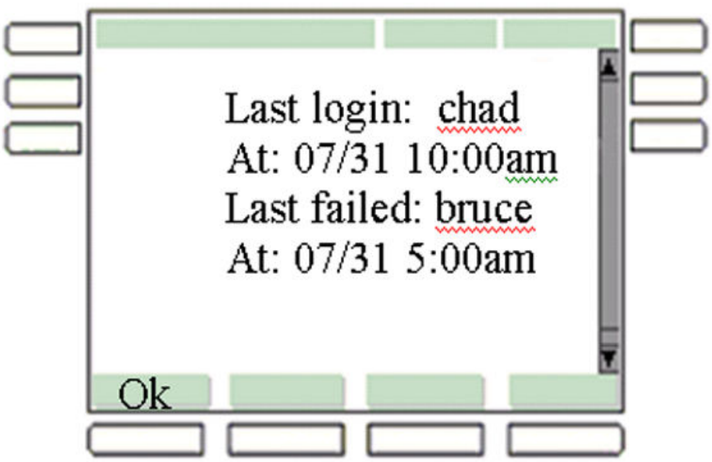


Figure 44: Login and login failure with time notification

Enhanced administrative password security

The provisioning server can provide additional security associated with the administrative password. The provisioning server provides the password to the IP Deskphone in the form of an SHA1 or MD5 hash instead of the plain text password. This removes the need to store the password on the IP Deskphone by using the existing ADMIN_PASSWORD provisioning parameter.

The provisioning server can also enforce a password expiry using the provisioning flag, ADMIN_PASSWORD_EXPIRY. This flag contains a date after which the admin password stored on the IP Deskphone is not accepted. After this time, the administrative password must be changed in the administrative server. Password expiry can only be enforced if the date and time are retrieved by the IP Deskphone through SIP, SOAP, or SNTP.

Important:

IP Deskphone licensing information is located in the *Keycode Retrieval System (KRS) User Guide*. You must register for access to KRS.

File Manager interface

A File Manager interface allows a user to use a USB drive to copy files from the flash file system of the IP Deskphone. The ability to modify or restrict the file types that can be copied are available through device configuration flags. An administrator can restrict the user from copying or deleting file types based on the device configuration flags that are configured.

Password protected screensaver

A user-defined password can enable a password protected screensaver on the IP Deskphone. A user-defined password is not secure because the user-defined password does not have any special rules for complexity. If a user-defined password introduces a security risk on the IP Deskphone, the administrator can disable the user-defined password function by changing the configuration file flag; the users can no longer use passwords that they configured for the screensaver.

Note:

The user-defined passwords for the IP Deskphone screensaver is disabled by default.

Debug port security

The debug port (Accessory Expansion Module (AEM) port) is disabled by default to prevent unauthorized access and intervention in IP Deskphone operation when a dongle is used.

Enabling the debug port requires access to the **Advanced Diag Tools** menu, which is always protected by the admin password, and enabling the **Debug port** option.

The default value of the **Debug port** option is **disabled**. Resetting the IP Deskphone to the factory defaults resets this parameter as well.

The **Debug port** option can be manually changed on a per-phone basis. The change survives an IP Deskphone reboot.

The **Debug port** option cannot be changed while the vxshell is active on the IP Deskphone (that is, vxshell is accessed through the PDT). If an attempt is made to change the option while the vxshell is active, the error message `Cannot change Debug port` is displayed on the phone screen. There is no way to change the **Debug port** option through provisioning or configuration files

When the **Debug port** option is disabled, and a dongle is connected to the IP Deskphone, the dongle is disabled from the very start of VxWorks and neither input nor output debug information is available. If an Expansion Module is connected to the AEM port, it is recognized and is fully functional (EXP_MODULE_ENABLE parameter must be set to YES).

When the **Debug port** option is enabled, the debug port of the IP Deskphone can be used for connecting a debug dongle. If a Expansion Module is connected to the AEM port, it is not recognized and does not function

In SIP 4.4 and later, the “magic key” sequence to switch between dongle mode and Expansion Module mode ([MUTE]-[UP]-[DOWN]-[UP]-[DOWN]-[UP]-[2] for dongle mode and [MUTE]-[UP]-[DOWN]-[UP]-[DOWN]-[UP]-[1] for Expansion Module mode) is not supported.

Chapter 14: Audio codecs

The optional audio codecs feature allows you to select the audio compression or decompression algorithm (codec) used on the IP Deskphone. You provision codecs using the Device Configuration file, and then the user can select from the provisioned codecs using the Audio menu on the IP Deskphone. This feature supports wideband audio performance, where wideband is defined as the frequency range between 150 and 6800 Hz.

When the user selects an audio codec, that codec is used for both incoming and outgoing calls.

The following table lists the audio codecs supported by IP Deskphone.

Table 40: Audio codecs supported by IP Deskphone

Codecs	Description
G.722 (1100 series only)	This codec is a wideband audio codec.
G.723.1	This codec is a compressed, non-wideband audio codec. It provides high-quality audio with less network connection requirements. This codec is ideal for bandwidth-conscious environments that do not support higher quality encoding. Expanded support of the existing G.729a codec with Annex allows for two byte Silence Insertion Descriptor (SID) frame for CNG.
G.711 a-law	PCMA
G.711 mu-law	PCMU
G.729	Expanded supported of the existing G.729a codec with AnnexB (G.729b) allows for Comfort Noise Generation (CNG).

In the case of an upgrade from a UNIStim IP Deskphone or an earlier version of the SIP firmware, Avaya recommends that you specify the preferred codec in the Device Configuration file; otherwise the default value is used.

The G.711 codec (PCMU and PCMA) is always used to place the codec list for emergency 911 calls. The G.711 codec is always used to receive incoming calls from the emergency operator. If the administrator disables this codec, the SIP phone can make outgoing non-emergency calls.

You can configure a maximum of 15 codecs. You can enable or disable the use of specific codecs for incoming and outgoing calls, though incoming and outgoing calls are not specifically independent.

The following table contains static payload types and other parameters for the supported codecs, including the default ptime value for each codec. The phone may use a different value, ranging from the default to 50 msec, if the caller (a third party caller) requests it by adding the corresponding ptime attribute to the SDP. The 1100 SIP IP Deskphone does not include ptime in its SDP message. Note that 10 msec ptime is not supported.

Table 41: Static payload types and other parameters for the supported codecs for the IP Deskphone

Codec	Payload type	SDP encoding name	Clock rate (HZ)	Bit rate (Kbps)	Default ptime (msec)	Channels
G.711 a-law	8	PCMA	8000		20	1
G.711 u-law	0	PCMU	8000		20	1
G.729A + 40ms ptime	18	G729	8000		20	1
G.729B	18		8000	8	20	1
G.722 (1100 series only)	9	G722	8000	64	20	1
G.723.1	4	G723	8000	5.3 6.3	30	1
G.723.1A	4		8000	5.3 6.3	30	1

The annexes selection for G.729 and G.723.1 are not available to the user and the administrator is responsible for enabling or disabling annexes using the Device Configuration parameters.

Codec preference through the Device Configuration file

Use the Device Configuration file to specify a list of codecs, and the preferred order in which they are used for incoming and outgoing calls. You can add a text descriptor to the technical name of the audio codec; these descriptors appear on the user interface of the IP Deskphone.

You can specify, by name, the exact codecs to offer in the Device Configuration file. This grants the administrator full control over the audio settings used for inbound and outbound calls. The following table is a sample of Device Configuration file entries for audio codec configuration.

Table 42: Sample Device Configuration file entries

```
AUDIO_CODEC1 PCMA standard a-law
AUDIO_CODEC2 PCMU standard u-law
AUDIO_CODEC3 G729 729 codec
AUDIO_CODEC4 G722 wideband codec
AUDIO_CODEC7 G723 high-compression codec
```

The IP Deskphone displays the codecs listed in the exact order that they are listed in the Device Configuration file.

The list of codecs specified in the Device Configuration file determines the list of codecs that are available for selection on the IP Deskphone.

Two fields in the device configuration file, G729_ENABLE_ANNEXB and G723_ENABLE_ANNEXA are used to enable or disable AnnexB and AnnexA support by G.729 and G.723 codecs, respectively. These flags can have the following values: YES, NO (No is the default value).

Important:

If codecs are not specified, the default list used by the current version of the IP Deskphone is PCMU, PCMA, G.729.

To stop the IP Deskphone from using a specific codec, you must change its entry in the Device Configuration file to a different codec, and then clear the value of the original specific codec, which disables the codec entry. If you remove all codecs from the allowed list, the IP Deskphone resets to the default list of codecs.

Important:

To reset the phone to the default list of codecs, it is necessary to remove the values against each AUDIO_CODECx item in the Device Configuration file.

For example:

```
AUDIO_CODEC1 PCMA standard a-law
AUDIO_CODEC2 PCMU standard u-law
AUDIO_CODEC3 G729 729 codec
AUDIO_CODEC4 G722 wideband codec
AUDIO_CODEC5 G723 high-compression codec
```

would become

```
AUDIO_CODEC1
AUDIO_CODEC2
AUDIO_CODEC3
AUDIO_CODEC4
AUDIO_CODEC5
```

If the ordered list of codecs is small and no matching codec is found during negotiations, the call drops, as the audio stream cannot be established. For backward compatibility with SIP Firmware Release 1.X, the Device Configuration file supports the **DEF_AUDIO_QUALITY** parameter as long as no codec is allowed using the parameter AUDIO_CODECN, in which case the DEF_AUDIO_QUALITY parameter is ignored and has no effect.

Specifying the DEF_AUDIO_QUALITY as High or Medium has the same effect as omitting the parameter altogether and without specifying codec through the parameters.

If set to Low, then the list of default codecs is reversed before being sent in the SDP negotiations. When you do not provide a text description in the Device Configuration file, the application uses the default text description from the language file.

The **AUDIO_CODECN** parameters specifies the order of preference for audio codecs. If there are no valid entries provided, then the parameter uses the default list of codecs. If you enter a codec that is not recognized by the IP Deskphone, then the parameter considers the codec as a blank entry. To remove a codec from the list, you must first blank the entry, or change it to an invalid codec name in the Device Configuration file.

Codec preference selection on the IP Deskphone

The Audio Quality Settings screen on the IP Deskphone allows the user to select an exact codec by name. This grants the user full control over the audio settings used for inbound and outbound calls.

The list of codecs is populated with the names of the codecs provided during Device Configuration. If a text descriptor is provided for a codec in the Device Configuration file, it appears after the codec name. The Audio Codec Ordering screen allows the user to modify the order of preference of the codecs. To change the list of available codecs, you must perform an update through Device Configuration. The IP Deskphone creates the ordered list from the list of codecs in the Device Configuration file. The user can reorder the list using the Preferences menu. On subsequent Device Configuration updates, at start time, or other updates, the ordered codec list of the user is synchronized with the list in the Device Configuration file. This synchronization makes both lists equal. If the user creates an order that is different from the one in the Device Configuration file, the IP Deskphone appends it to the end of the list.

Codecs preferences on the IP Deskphone

The user cannot modify the text descriptors through the IP Deskphone; the text descriptors can only be read by the user. After the system loads the Device Configuration file, the user preference selections are synchronized with the system codecs specified in the Device Configuration file. This ensures that the codecs available to the user are always set according to user preferences.

If the user modifies the order through the IP Deskphone, then the user-defined order is saved for the codecs that are defined as system codecs in the Device Configuration file. Codecs are appended at the end of the list in their relative order from the Device Configuration file. Until the user modifies the order of the codecs, the list of ordered codecs reflects the order specified in the Device Configuration file.

The following table shows examples of the list of codecs provided by Device Configuration, user configuration, and resulting list of codecs that the system uses for presentation and codec negotiation purposes.

Table 43: Examples of the ordered lists of Codecs

Supported by IP Deskphone	Ordered list of codecs provided by Device Configuration	Ordered list of codecs provided by user configuration	Ordered list of codecs used by the SIP IP Deskphone
	A, B, C, D, E	N/A	A, B, C, D, E
	A, B, C, D, E	E, D, C, B, A	E, D, C, B, A
A, B, C, D, E, F, G	A, B, C, D, E	A, D, E	A, D, E, B, C
	A, C, D, E	A, B, C, D, E	A, C, D, E
	A, C, D, E	A, B, C, E	A, C, E, D

Note:

The user-defined order of the codecs can be specified/changed by means of the Custom keys file through the section **[audiocodecs]**. See Custom keys file on page 195. When the IP Deskphone downloads the Custom keys file, the IP Deskphone performs the following actions:

- The IP Deskphone parses the section **[audiocodecs]** from the Custom keys file. If the codec specified within the file exists in the list of codecs in the Device Configuration file, then the codec is added to the list of the supported codecs. Otherwise, the codec is rejected.
- The IP Deskphone adds the last codecs, presented in the Device Configuration file, to the list of supported codecs.

Chapter 15: Certificate-based authentication

Certificate-based authentication

Certificate-based authentication allows the administrator to ensure that the IP Deskphone is authorized to access the enterprise LAN environment and to connect securely to:

- SIP proxy using TLS
- Provisioning servers using HTTPS
- EAP service using EAP-PEAP, EAP-TLS

Certificates bind an identity to a pair of electronic keys that are used to encrypt and sign digital information, and make it possible to verify someone's claim that they have the right to use a given key. Certificates provide a complete security solution, assuring the identity of all parties involved in a transaction. Certificates are issued by a Certification Authority (CA) and are signed with the CA's private key.

A certificate contains the following information:

- Owner's public key
- Owner's name
- Expiration date of the public key
- Name of the issuer (the CA that issued the certificate)
- Serial number of the certificate
- Digital signature of the issuer

A Certificate Authority issues certificates to users and devices, such as IP Deskphones. A CA is a trusted third party. The certificate issued by a CA contains a variety of data. This data includes the identity of the issuing CA, Certificate Usage, and expiry date for the certificate.

Key components of certificate-based authentication are:

- Trusted certificates
- Device certificates
- Certificate Trust Lists (CTL)
- Security Policy

Trusted certificates are installed on the Deskphone using [USER_KEYS] section of the configuration file. They are used for establishing SIP-TLS and HTTPs and use a PEM certificate format.

Device Certificates are used to establish mutual authentication. They are installed on the Deskphones using [DEV_CERT] section of the configuration file. Device certificates use a password-protected PKCS#12 file device certificate. A PKCS#12 file contains both private and public key pairs of the certificate.

CTL is a predefined list of trusted server certificates which the IP Deskphone views as trusted endpoints. It is used as a mechanism to provide connection to only trusted servers.

IP Deskphones enable the administrator to manage (view and delete) trusted certificates, device certificates, and CTLs through user interface. Events are logged to Security Logs to mark events, such as Certificate Addition and Deletion. The administrator is to view security and error logs from the user interface.

The Security Policy file contains a set of rules that dictates certificate-based authentication on the IP Deskphone, such as the size of the public and private keys used on the certificates.

EAP authentication methods are used to allow the administrator to ensure that individual devices are authorized to access the enterprise LAN environment. The following EAP methods are supported on the device.

- EAP-MD5—User ID/password-based authentication
- EAP-PEAP—certificate-based authentication
- EAP-TLS—certificate-based authentication

EAP-PEAP and EAP-TLS use certificates to authenticate a device on the network. EAP-PEAP requires a trusted anchor certificate to be installed on the IP Deskphone. EAP-TLS requires a trusted anchor certificate and a device certificate to be installed on the IP Deskphone.

Trusted Root certificate

The customer root certificate is a self-signed certificate (a self-issued certificate where the subject and issue fields contain identical DNs, and are not empty. The customer root certificate must be installed on the IP Deskphone and stored in the IP Deskphone trusted store for the following reasons:

- to verify the identity of the various servers that the IP Deskphone can attempt to establish secure connections with, such as TLS and HTTPS
- to authenticate the signatures on software and configuration files that are downloaded onto the IP Deskphone.

Trusted root certificate installation

You can install one or more customer root certificates on the IP Deskphone by using the configuration file 11xxeSIP.cfg.

- The [USER_KEYS] section is added to the configuration file 11xxeSIP.cfg to download a customer root certificate from a provisioning server. For example:

  ```
  [USER_KEYS]

  DOWNLOAD_MODE AUTO

  PROTOCOL HTTPS

  FILENAME custroot.pem
  ```

  The PROTOCOL attribute of the [USER_KEYS] section can be assigned to one of the IP Deskphone supported protocols, such as HTTP, TFTP, HTTPS, and FTP.

  The FILENAME attribute of the [USER_KEYS] section points to the file name of a customer root certificate in Privacy Enhanced Mail (PEM) format.

- After the configuration file is downloaded and parsed by the IP Deskphone, the [USER_KEYS] section is processed and the root certificate is downloaded to the IP Deskphone.
- After the certificate file is downloaded, you must authenticate the contents of the certificate file before installing it on the IP Desklphone. There are two possible situations.
  - If there are no existing customer root certificates on the IP Deskphone, a fingerprint (SHA1 hash) for the file is computed. Depending on the value that is configured in the Security Policy parameter, CUST_CERT_ACCEPT, the user can either be prompted to accept this fingerprint (CUST_CERT_ACCEPT = VAL_MANUAL_A,) or prompted to enter the fingerprint for verification (CUST_CERT_ACCEPT = VAL_MANUAL_B).
  - If there is one or more customer root certificate on the IP Deskphone, the certificate file must be digitally signed with a signing certificate. In this case, there is no interaction with the user. The signature is internally verified and the signing certificate is verified to be issued by a customer root certificate that is already installed on the IP Deskphone.
  - **Note:**

    In the descriptions above, there is reference to the certificate file containing a single customer root certificate. While this is the most common usage, the file can actually contain more than one certificate, where the PEM encoding for each is appended in the file with a blank line between each. If the file's authenticity is successfully verified, all entities in the file are installed on the IP Deskphone.
- If the authentication of the file is successful, the customer root certificate is installed on the IP Deskphone in the trusted certificate store.
- The command to sign a resource file using openssl is as follows:

  ```
  openssl smime
  -sign -in unsigned_file  -signer sign_cert_file  -outform PEM -binary
  -inkey sign_cert_pk_file -out tmp_signature_file
  ```

- CUST_CERT_ACCEPT parameter is a Security Policy Parameter to disable Customer Certificate file signing.
- CUST_CERT_ACCEPT – VAL_NO_CHECK parameters only controls further signing of customer root certificates. The first Certificate must be either signed by Avaya Trusted Certificate or Finger Print Accepted.

  Caution:

  There is a security risk in not having the Trusted Certificates loaded with VAL_NO_CHECK.

When the IP Deskphone tries to establish a secure connection (for example, HTTPS, SIP TLS) with a server, the server provides its certificate which then must be verified by the IP Deskphone.

The following are the possible configurations (depending on the server configuration):

1. Server can provide only its Server certificate.
2. Server can provide the entire certificate chain (up to the Root CA certificate).

In the first scenario, the IP Deskphone only needs the CA certificate which was used to sign the Server certificate. The certificate file must be PEM encoded.

In the second scenario, every certificate in the chain must be verified. Root and Intermediate CA certificates of the chain must be installed in the IP Deskphone Trusted Certificates store. Certificates must be PEM encoded and combined into one file.

Device certificate installation process

A device certificate is a certificate used to prove the identity of the IP Deskphone to a server while establishing various secure connections, such as TLS and HTTPS, between the IP Deskphone and a server. In most cases there may be one or two device certificates installed on the phone. However, to allow for various combinations of sharing device certificates among different applications, the concept of a Device Certificate Profile (DCP) is introduced. Within the DCP, it is possible to identify one or more uses (or purposes) for the device certificate associated with each profile. The default purpose is ALL. This provides a completely flexible model for the sharing of device certificates among phone applications. There are two methods that can be used to install a device certificate on the phone, SCEP and PKCS#12 download. SCEP is a protocol which allows the phone to send a device certificate request to a CA server based on a locally generated private key. This provides more security for the private key since it is never transmitted, even in an encrypted form. However, the SCEP process does have limitations in terms of the limited flexibility permitted in the certificate request by the SCEP server. Limitations vary considerably between various SCEP/CA servers.

PKCS#12 is an industry standard for exchanging certificate and private keys. A device certificate downloaded to the phone in a PKCS#12 file will contain the complete certificate, including its private key, which was generated offline by a Certificate Authority. The PKCS#12 file is encrypted using a password at the time of generation, so there is protection for the private key. This approach provides more flexibility in the definition of the device certificate. It may also be more appropriate where an appropriate SCEP service is not available or cannot be configured for security reasons.

Each device certificate installed on the phone will be attached to a Device Certificate Profile (DCP). Currently SIP supports only 2 profiles. Profile0 (SCEP) and Profile1 (PKCS12).

Installing a device certificate using PKCS12

PKCS#12 is an industry standard for importing and exporting keys and their related certificates. On the IP Deskphone, this method is only used to import the IP Deskphone device certificate and private key.

The [DEV_CERT] section is added to the configuration file `11xxeSIP.cfg` to download the PKCS#12 file device certificate from a provisioning server.

The administrator is responsible for creating the PKCS#12 file with the required device certificate associated with the private key of the device certificate.

The PKCS#12 file device certificate must be in Distinguished Encoding Rules (DER) or BER format. If you are creating the certificate for the first time, you must mark the private key of the certificate as exportable. If you export a certificate to a PKCS#12 file, you must enter a password.

Note:

The PKCS#12 password cannot exceed 12 characters in length and must include only characters that you can enter on the IP Deskphone. These characters include all numbers, upper and lower case letters, and the following special characters: _ - . ! @ $ % & + : ^.

Use the following procedure to install a device certificate using a PKCS#12 file.

1. Add a [DEV_CERT] section to `11xxeSIP.cfg` to enable the IP Deskphone to import a PKCS#12 file device certificate.

   An example of the [DEV_CERT] section is as follows:

   ```
   [DEV_CERT]
   FILENAME "*.p12"         # "*" symbol is automatically substituted with phone MAC
   address
   VERSION <n>
   PROFILE 1                # profile index
   PURPOSE -1               # bitflag with all purposes it can be used for
                            # (default is -1 = ALL)
   ```

   • FILENAME attribute points to the PKCS#12 file device certificate name. If the file name includes "*" then it'll be automatically substituted with the IP Deskphone MAC address to allow the definition of unique filenames for the PKCS#12 files containing the device certificates for each IP Deskphone. The administrator is responsible for creating the PKCS#12 file device certificate.

   • VERSION attribute determines if the file should be downloaded by comparing this VERSION with the VERSION stored in the corresponding device certificate profile.

- PROFILE attribute must be 1. The certificate profile index identifies the file name where the profile is stored in the IP Deskphone memory (SFS), and identifies the device certificate profile.
- PURPOSE attribute is a bit mask that lets a device certificate be used for multiple purposes. PURPOSE must be -1 as the same device certificate is used for all purposes (HTTPS, SIP-TLS, EAP-TLS).

2. The IP Deskphone checks the version in the [DEV_CERT] section against the version stored in the specified PROFILE. If the version in the specified profile is missing or is older, the device certificate file is downloaded.
3. After the PKCS#12 file device certificate is downloaded, the IP Deskphone prompts the administrator to enter the PKCS#12 protected password.

   Note:

   The password can be empty, but the use of an empty password is not recommended except under very controlled conditions.
4. Enter the PKCS#12 protected password.
5. The IP Deskphone validates the device certificate to ensure the following:
   - the correct password is entered
   - key size is >= to the value specified in the Security Policy File
   - key algorithm is RSA
   - the certificate is not revoked
   - the certificate is not expired
6. If the device certificate is validated correctly, the IP Deskphone stores the device certificate and the private key in the IP Deskphone memory (SFS) in the device certificate profile specified in the [DEV_CERT] section.

   The version specified in the [DEV_CERT] section is stored in the profile for future reference when determining if a new device certificate is available for download.
7. PKCS12 imported certificate is stored in Profile 1.

Installing a device certificate using SCEP

Procedure

1. Generate Key Pair.
   - Private key generation algorithm is RSA. Key length is defined via Security Policy. Acceptable values are: 1024 - default, 1536, 2048.
   - The process of generating the key pair can take several minutes. While keys are generated the phone may show the message “Generating Keys …”. This message may

appear approximately 10 seconds after the phone connects and only if key generation is not already complete.

- The private keys will be stored permanently in the SFS ready to be used to create a certificate request.

2. Retrieve Root Certificate.
    - The URL required for sending requests to an SCEP/CA server is provisioned in the manual configuration menu or a provisioning file.
    - Phone sends GetCACert SCEP request to CA server.
    - Phone waits for response.
    - If any error is received (such as a timeout, server unreachable, 404, etc.) the registration process will terminate. The key pair will be retained so they do not need to be regenerated on the next phone boot.
    - Phone accepts the reply which contains the root certificate.
    - If the certificate is not already on the phone, the fingerprint is computed and displayed. The administrator is asked to Accept or Reject the fingerprint.
    - If the CA certificate is rejected the registration process will terminate. The key pair will be retained in case the administrator wants to try again.
    - If the CA certificate is already in the trusted store, no prompt is displayed.
    - If the fingerprint is accepted, the CA certificate is added to the trusted store on the phone.
    - If there is an RA certificate(s) present in the response, it will be stored in volatile memory so that it is available for the remainder of the request process.
    - There may be two RA certificates. In this case, one will be identified as used for encrypting the certificate request by a keyUsage that includes keyEncipherment or enciphermentOnly. The other will be identified as a signing RA certificate by a keyUsage that include digitalSignature.
3. Create a PKCS #10 formatted certificate signing request.
    - The phone's FQDN is built from information in the EAP configuration – the hostname and domain name. If no hostname is defined, it is created using the phone's MAC address according to the form NTIPP012345 – where IPP is an acronym (NorTel IP Phone) and 012345 are the last six hex digits of the MAC address.
    - The FQDN is assigned to the certificate common name (CN) but not the subject alternate name. Some CA servers will reject a request that includes a subject alternate name.
    - Insert challenge password.
    - The challenge password is a 0 to 16 digit value. The administrator is prompted for the password and it is entered using the dial pad. An empty password may also be entered as use of this feature may not be configured on the CA server.
    - Envelope PKCS #10 request plus the challenge password in PKCS #7 packet encrypted by RA/CA cert and send to CA.

4. CA verifies the request automatically or manually.
    - While waiting for approval the phone will display the message “Waiting for Approval …”.The client will poll the server approximately every 10 seconds and leave the “Waiting for Approval …”.message visible.
    - The phone will also display a softkey “Abort” for 30 seconds so the administrator has an opportunity to abort the operation. If the operation is aborted the registration process will terminate. The key pair will be retained in case the administrator wants to try again.
5. CA returns the signed certificate to the phone. The RA signing certificate (or CA certificate if there is no RA certificate) is used to verify the signature on the response.
6. The device certificate will be extracted and stored in the SFS in Profile 0. The private key for the certificate is already stored in the SFS.

Certificate Trust List

The IP Deskphone uses Certificate Trust List (CTL) method to verify the various network elements such as proxy servers and provisioning servers. For the IP Deskphone to trust any network element, the certificate of the IP Deskphone must be added to the CTL.

The CTL is a collection of certificates bundled together into a file and downloaded into the IP Deskphone. The file is signed and all of the certificates in the bundle are inherently trusted by the IP Deskphone (after the file signature is verified).

The use of the CTL is optional. If the CTL is not installed on the IP Deskphone, the authentication of the network element reverts back to the default which is to authenticate the certificate chain to a root certificate trusted by the IP Deskphone

Validating a certificate using the Certified Trust List

The high level sequence of procedures for validating a certificate using the Certificate Trust List is as follows:

1. Create the CTL file including start date, expire date, and a list of certificates concatenated together in PEM format so that the entire file can be signed by a trusted entity. A signed CTL file consists of the following:
    - Validity fields

      `NOT_VALID_BEFORE: 23/11/2007 11:12:13`

      `NOT_VALID_AFTER: 25/10/2011: 22:23:24`
    - Original unsigned file content
    - Digital signature

    The parts are appended together with the Validity periods first, followed by the certificates, and then by the digital signature. The signature must be in the form of a PKCS7 detached signature of the file in PEM format. A detached signature is a signature that does not embed the content that is signed.

The IP Deskphone does not accept unsigned CTL files. After a CTL file is accepted, the included certificates are added to the trusted certificate store of the IP Deskphone.

Important:

Do not insert additional characters between the Certificate and the Digital Signature. Otherwise, the validation fails. Do not change any information from the original file content that was used to create the signature. Otherwise the signature becomes invalid and you must create a new signature.

2. The CTL is provisioned to the IP Deskphone in a secure way. Avaya recommends that you use HTTPS as the secure method to download the CTL file to the IP Deskphone.
3. The IP Deskphone checks the validity periods as follows:
   - Not Valid Before – the CTL file is not used before the validity date.
   - Not Valid After– the IP Deskphone checks this when:
     - the CTL file is downloaded
     - every 24 hours
     - a remote certificate is presented to the IP Deskphone
     - the CTL is expired; the CTL is deleted and an event is logged in the security log.
4. After the IP Deskphone starts a TLS channel with a server (EAP or TLS) and receives a server certificate, the IP Deskphone validates the certificate by checking the availability of the certificate in the CTL and decides whether to trust the certificate or not. If the server certificate is not in the CTL, the server certificate is rejected and a TLS channel is not established.

   The administrator must ensure that the CTL is up to date. If a new CTL is downloaded to the IP Deskphone, the old CTL file is overwritten by the new one.

   Note:

   The IP Deskphone can trust up to ten server certificates in the CTL file.

   An example of a CTL file is as follows:

```
NOT_VALID_BEFORE: 23/11/2007 11:12:13
NOT_VALID_AFTER: 25/10/2011 22:23:24

-----BEGIN CERTIFICATE-----//
the content of the certificate goes here
-----END CERTIFICATE-----
// the content of the digital signature goes here
-----END PKCS7-----
```

Installing a Certified Trust List

About this task

The IP Deskphone uses the Certified Trust List (CTL) method to verify the various network elements, such as proxy servers and provisioning servers.

Procedure

Add the [CTL] section to 11xxeSIP.cfg to allow the IP Deskphone to download a CTL file.

After the 11xxeSIP.cfg file downloads from the provisioning server, the IP Deskphone executes the [CTL] sections and downloads the CTL file.

After the CTL file is downloaded, the IP Deskphone validates the CTL file to ensure that the CTL file is signed by a trusted entity. If the CTL file is validated correctly, the CTL file is stored in the IP Deskphone

Example

An example of the format for the [CTL] section of the 11xxeSIP.cfg file is as follows:

```
[CTL]
DOWNLOAD_MODE AUTO
PROTOCOL HTTPS
FILENAME ctl.pem.sig
```

The filename attribute points to the signed CTL file.

Note:

The CTL file size must not exceed 20 Kbytes

Certificate Trust List events

The following provides a list of events related to the Certificate Trust List (CTL) file.

```
CTL Expiry:
```

```
0020[Information][WED OCT 26 03:02:54 2011][270][n:/fw/build/../util/pki/
pki_mgmt.c:3726] - CTL Expired. CTL Date[26:10:2011] Current
Date[25:10:2011]
```

```
CTL Deletion:
```

```
0015[Information][WED OCT 26 03:02:55 2011][271][n:/fw/build/../util/pki/
pki_mgmt.c:3482] - Deleted CTL
```

```
CTL download error:
```

```
0021[Information][WED MAY 20 03:00:58 2009][154][n:/fw/build/../util/
tftpsecurity/proc_keys.c:227] - Error Importing CTL. Could not get
dates[DD/MM/YYYY HH:MM:SS]
```

Certificate administration

The administrator can view and delete certificates and CTLs. Because a certificate can be deleted, it is critical that the administrator password used to access this function is protected and limited to only those who require it.

Certificate administration is accessed through the **Diagnostics** menu .

To view the Certificate Administration option in the Diagnostics menu:

1. Create Security Policy file (a text file).
2. Add the CERT_ADMIN_UI_ENABLE YES in the Security Policy file.
3. Sign the file using a signing certificate; for example, SecurityPolicy.txt.sig
4. Download the file using the [SEC_POLICY] section in the 11xxeSIP.cfg file.

   After the Security Policy file is enabled, access the Certificate Administration screen from the **Network** screen
5. Select. **Device Settings** > **Diagnostics** > **Certificate Administration**.

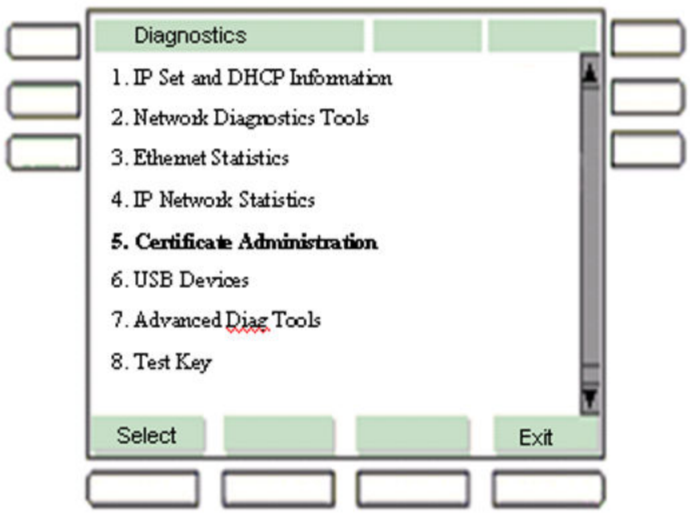


Figure 45: Diagnostics main menu

Certificates Administration main menu

The **Certificates Administration** screen displays the following options:

- Trusted Certificates
- Device Certificates
- CRL
- CTL

To access the **Certificates Administration** screen from the **Network** menu, select **Device Settings** > **Diagnostics** > **Certificate Administration**.

Figure 46: Certificates Administration main menu

The following table describes the function of the context-sensitive soft keys for the **Certificates Administration** screen.

Table 44: Context-sensitive soft keys for the Certificates Administration screen

Context-sensitive soft key	Action
Select	Selects the required option.
Back	Returns you to the Diagnostics menu.

Note:

Trusted Certificates screen

The Trusted Certificates screen displays a list of subject Common Names (CN) of the trusted certificates (root certification authorities) as shown in the following figure:

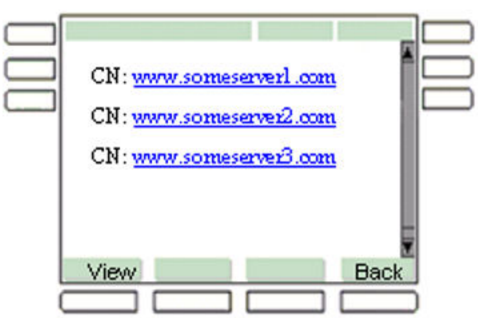


Figure 47: Trusted Certificates screen

The administrator can delete the certificate in the details screen by using the **Delete** context-sensitive soft key. Deletion does not happen automatically; the IP Deskphone displays a warning confirmation screen.

The following table describes the function of the context-sensitive soft keys for the Trusted Certificates screen.

Table 45: Context-sensitive soft keys for the Trusted Certificates screen

Context-sensitive soft key	Action
View	Displays the information of the selected Trusted Certificate which includes the following: • Common Name (CN) • Serial Number (SN#) • Expiry Date • Certificate Status (such as OK or Expired)
Back	Returns you to the previous screen.

Figure 48: Trusted Certificates details

The administrator can delete the certificate in the "Detailed Mode" by using the **Delete** context-sensitive soft key. Deletion does not happen automatically; the IP Deskphone displays a warning confirmation screen.

The following table describes the function of the context-sensitive soft keys for the Trusted Certificates Details screen.

Table 46: Context-sensitive soft keys for the Trusted Certificates Details screen

Context-sensitive soft key	Action
Delete	Displays a warning confirmation. Deletes the selected certificate.
Back	Returns you to the previous screen.

Device Certificates screen

The Device Certificates screen displays a list of subject Common Names (CN) of device certificates as shown in the following figure:

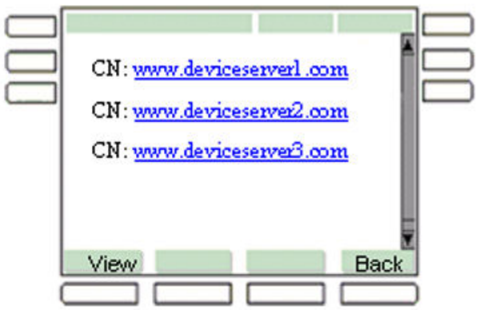


Figure 49: Device Certificates screen

The administrator can delete the certificate in the details screen by using the **Delete** context-sensitive soft key. Deletion does not happen automatically; the IP Deskphone displays a warning confirmation screen.

The following table describes the function of the context-sensitive soft keys for the Device Certificates screen.

Table 47: Context-sensitive soft keys for the Device Certificates screen

Context-sensitive soft key	Action
View	Displays the information of the selected Device Certificate which includes the following: • Common Name (CN) • Serial Number (SN#) • Usage • Expiry Date • certificate profile index • Status (such as, OK or Expired)
Back	Returns you to the previous screen.

Figure 50: Device Certificate details

The administrator can delete the certificate in the "Detailed Mode" by using the **Delete** context-sensitive soft key. Deletion does not happen automatically; the IP Deskphone displays a warning confirmation screen.

CTL screen

The CTL screen displays a list of subject Common Names (CN) of the CTL certificates as shown in the following figure:

Figure 51: CTL certificate screen

The following table describes the function of the context-sensitive soft keys for the CTL screen.

Table 48: Context-sensitive soft keys for the CTL screen

Context-sensitive soft key	Action
View	Displays information on the selected certificate which includes the following: • Common Name CN) • Serial Number (SN#) • Expiry Date • Certificate Status (such as, OK or Expired)
Delete	Displays a warning confirmation. Deletes the CTL.
Back	Returns you to the previous screen.

After you press the **View** context-sensitive soft key on the required certificate, information about the certificate you selected appears on the screen.

The following figure is an example of the CTL Certificate Details screen for the certificate www.ctlserver1.com.

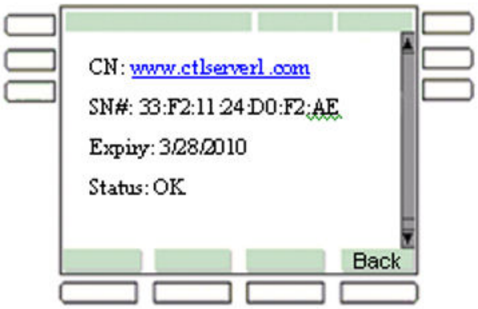


Figure 52: CTL Certificate details screen

You can use the PDT shell command to view an installed CTL.

The following is an example of a command with the output of the command.

```
->listctlcerts
CTL Certificate Count: 2
0) [MAC][172.25.10.171]
    Expires : SUN FEB 26 15:58:31 2010 - (Valid)
    Serial  : 0x26
    SKID    : 6D 0A 57 D7 D6 A8 C3 A2 9D 6B FE E9 92 50 25 96 FF CB B6 51
    AKID    : 34 CF F4 78 82 30 5A CD 64 2D 9D 05 56 02 5B 62 95 8C CE A2
    Usage   : 0x00e0
    ExtUsage: 0x0f
1) [Mac-PCC][one-ia-db.com]
    Expires : SUN NOV 26 21:16:59 2009 - (Valid)
    Serial  : 0x19
    SKID    : 30 AB E0 0F 19 0A 8E 07 D5 E4 63 C5 82 62 88 0D 93 21 DA 0A
    AKID    : 34 CF F4 78 82 30 5A CD 64 2D 9D 05 56 02 5B 62 95 8C CE A2
    Usage   : 0x00e0
    ExtUsage: 0x00
value = 0 = 0x0
```

Figure 53: Example of command output

Important:

The CTL file size must not exceed 20 Kbytes.

CRL screen

The CRL is also used to validate a certificate before the IP Deskphone starts to use it by checking it against the CRL lists stored in the phone. If the certificate is listed in the CRL, and this CRL is issued by this certificate, then this certificate is not trusted and cannot be used. The certificate is deleted from the phone if it was stored.

The CRL is always issued by the CA which issues the corresponding certificates. The certificates for which a CRL should be maintained are often X.509/public key certificates, as this format is commonly used by PKI schemes.

When **CRL** is selected from the **Certificates Administration** menu, the CRL screen displays a list of all serial numbers in the CRL loaded on the phone.

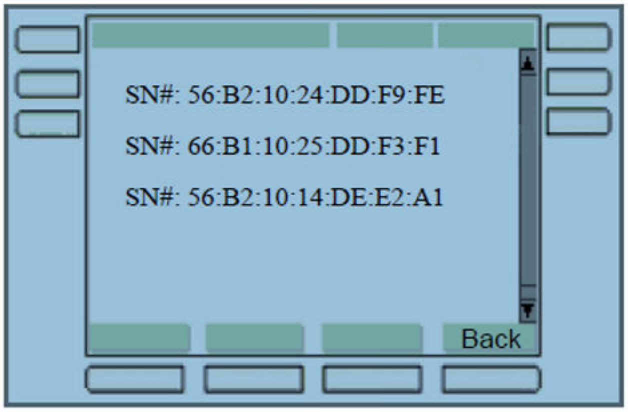


Figure 54: CRL screen

The following table describes the function of the context-sensitive soft keys for the CRL screen.

Table 49: Context-sensitive soft keys for the CRL screen

Context-sensitive soft key	Action
Back	Returns you to the previous screen.

CRL files can be installed on the phone by using the provisioning file in the [CRL] section:

```
[CRL]
DOWNLOAD_MODE FORCED
VERSION 000002
FILENAME crl.pem
PROMPT YES
```

Security Policy

The security policy file contains a set of rules or parameters that dictate certificate-based authentication on the IP Deskphone.

An example of the Security Policy file rules is as follows:

```
CERT_ADMIN_UI_ENABLE NO

SECURITY_LOG_UI_ENABLE NO

KEY_SIZE 1024

KEY_ALGORITHM KEY_ALG_RSA

TLS_CIPHER RSA_WITH _AES_256_CBC_SHA
```

Security policy parameters

The security policy file parameters and the excepted and default values are as follows:

CERT_ADMIN_UI_ENABLE

This parameter determines if the Certificate Administration user interface is enabled on the IP Deskphone. The acceptable values are as follows:

- YES – Certificate Administration user interface is enabled on the IP Deskphone.
- NO – Certificate Administration user interface is disabled on the IP Deskphone (default).

SECURITY_LOG_UI_ENABLE

This parameter determines if the Security Log user interface is enabled on the IP Deskphone. The acceptable values are as follows:

- YES – Security Log user interface is enabled on the IP Deskphone.
- NO – Security Log user interface is disabled on the IP Deskphone (default)..

KEY_SIZE

This parameter determines the default size used when generating keys on the IP Deskphone and acts as the minimum allowed key size that should be enforced when loading certificates from the IP Deskphone. The acceptable values are as follows:

- KEY_SIZE_1024 (default)
- KEY_SIZE_1536
- KEY_SIZE_2048

KEY_ALGORITHM

This parameter is the preferred key generation algorithm. The only acceptable value is as follows:

- KEY_ALG_RSA (default)

TLS_CIPHER

This parameter is the preferred TLS Cipher used for HTTPS to configure a stronger cipher preference when available. The acceptable values are as follows:

- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA (default)

SIGN_SIP_CONFIG_FILES

This parameter overrides the file signing of a file, such as the device configuration file and the dial

	plan file. You cannot override the file signing of the Security Policy and Customer Certificates. The acceptable values are as follows: • YES – Signing is required. • NO – No authentication check is performed (default).
FP_PRESENTED	If the resource file is not signed and if there are no customer certificates, then you are prompted with a Finger Print display with accept or reject options.
FP_ENTERED	If the resource file is not signed and if there are no customer certificates, then you must manually enter the Finger Print value and then select **Accept**.
SUBJ_ALT_NAME_CHECK_ENABLE	This parameter checks the Subject Alternative Attribute in the presented certificate. The acceptable values are YES and NO. The default value is NO. **Note:** Currently only IPv4 IP Address is supported for this attribute.
CUST_CERT_ACCEPT_VAL_NO_CHECK	This parameter is added to the existing values. Acceptable values for this parameter are as follows: • VAL_NO_CHECK • VAL_NO_MANUAL • VAL_MANUAL_A (default) • VAL_MANUAL_B
SEC_POLICY_ACCEPT	This parameter is for Security Policy File acceptance. Acceptable values for this parameter are as follows: • VAL_MANUAL_A – If the resource file is not signed and if there are no customer certificates, then you are prompted with a Finger Print display with accept or reject options (default). • VAL_MANUAL_B – If the resource file is not signed and if there are no customer certificates, then you must manually enter the Finger Print value and then select **Accept**.
CERT_EXPIRE	This parameter is the Certificate Expiration Policy. Acceptable values for this parameter are as follows: • DELETE_CERT –A certificate is deleted when expired. A security log entry is added.

	• LOG_EXPIRE – A certificate is not deleted when it expires A security log entry is added. **Note:** Even though the certificate is not deleted, it still cannot be used to authenticate a file. • NO_EXPIRE_LOG –A certificate is not deleted when it expires. A security log entry is not added. **Note:** Even though the certificate is not deleted, it still cannot be used to authenticate a file.
DWNLD_CFG_ACCEPT	This Parameter defines how all TFTP configuration files are authenticated when there are no customer certificates on the IP Deskphone. When there is a customer certificate installed, this parameter has no effect. Acceptable values for this parameter are as follows: • VAL_ACCEPT – Unsigned and signed files are always accepted if there are no valid customer certificates. • VAL_MANUAL_A – If the resource file is not signed and if there are no customer certificates, then you are prompted with a Finger Print display with accept or reject options (default). • VAL_MANUAL_B – If the resource file is not signed and if there are no customer certificates, then you must manually enter the Finger Print value and then select **Accept**.
SECURITY_POLICY_PARAM_CHANGE	This Parameter defines if configuration files (11xxeSIP.cfg) are forced to be signed if there is a customer certificate installed. This parameter has no effect if there are no installed customer certificates. Acceptable values for this parameter are as follows: • YES– If there is a customer certificate installed, the downloaded file must be signed and fully authenticated. • NO – If there is a customer certificate installed, the downloaded file will be automatically accepted with no authentication (default).

Installing a Security Policy file

About this task

You can install a Security Policy file on the phone by using the configuration file 11xxeSIP.cfg.

Procedure

1. Create a text file, for example SecurityPolicy.txt.
2. Add a security parameter and value in the text file, for example CERT_ADMIN_UI_ENABLE YES. The parameter name and value are separated by a space.
3. Sign the file using a signing certificate. For example, SecurityPolicy.txt.sig file.

   The [SEC_POLICY] section is added to the configuration file 11xxeSIP.cfg to download a security policy file from a provisioning server.
4. After the security policy file is downloaded, its contents must be authenticated prior to being installed on the IP Deskphone. There are 2 possible cases:
   - If there are no existing customer root certificates on the IP Deskphone, a fingerprint (SHA1 hash) for the file is computed. Depending on the value of the Security Policy parameter SEC_POLICY_ACCEPT value on the IP Deskphone, you are either prompted to accept this fingerprint (SEC_POLICY_ACCEPT = VAL_MANUAL_A) or you are prompted to enter the fingerprint for verification (CUST_CERT_ACCEPT = VAL_MANUAL_B).
   - If there are one or more customer root certificates on the IP Deskphone, then the security policy file must be digitally signed with a “signing” certificate. In this case, there is no interaction with the user. The signature is internally verified and the signing certificate is verified to be issued by a customer root certificate that is already installed on the IP Deskphone.

   If the authentication of the file is successful, the security policy file parameters is accepted on the IP Deskphone.

Example

```
[SEC_POLICY]
DOWNLOAD_MODE FORCED
PROTCOL HTTP
FILENAME SecPolicy.txt.sig
```

Security policy logs and diagnostics

Changes made to the security policy file have an entry in the security log file. For example, `SECURITY_POLICY_PARAM_CHANGE 0x1055`.

The security log file stores only the non-sensitive information. For example, if the password is changed, the security log file indicates this change without storing the password value.

The PDT (Problem Determination Tool) shell command can be used to view the output of the security policy command. This command lists the security policy parameters and their values on the IP Deskphone.

The following is the output of the security policy command from the PDT shell.

```
-> securitypolicy
CUST_CERT_ACCEPT = VAL_MANUAL_A
SIGN_SIP_CONFIG_FILES = NO
CERT_EXPIRE = DELETE_CERT
SEC_POLICY_TEXT = YES
AUTO_PRV_ACCEPT = VAL_ACCEPT
DWNLD_CFG_ACCEPT = VAL_ACCEPT
AUTO_PRV_SIGNING = NO
DWNLD_CFG_SIGNING = NO
CERT_ADMIN_UI_ENABLE = YES
SECURITY_LOG_UI_ENABLE = YES
USB_DEVICE_SECURITY_ENABLE = YES
KEY_SIZE = KEY_SIZE_1024
KEY_ALGORITHM = KEY_ALG_RSA
TLS_CIPHER = RSA_WITH_AES_256_CBC_SHA
SUBJ_ALT_NAME_CHECK_ENABLE = NO
FTP_PASSWORD = ****
```

EAP Authentication

EAP-enabled networks allow the administrator to ensure that individual devices or users are authorized to access the enterprise's LAN environment.

The following diagram shows the network architecture for 802.1x and EAP.

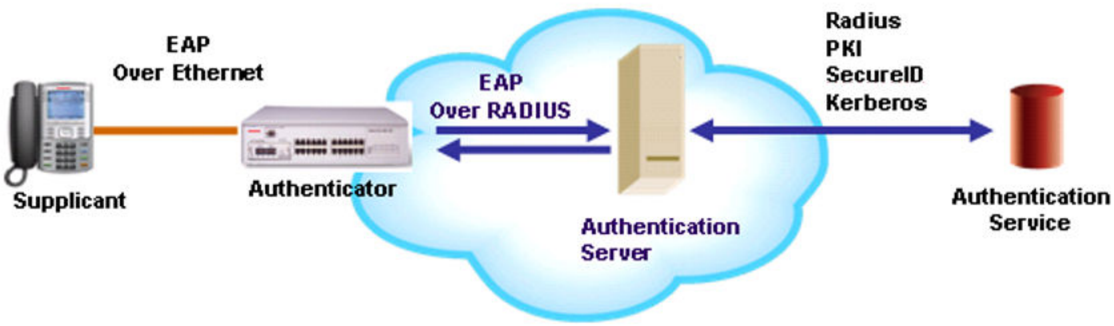


Figure 55: 802.1x and EAP network architecture

IEEE 802.1x defines three roles:

- a supplicant—an entity that requires access to the network for use of its services.
- an authenticator—the network entry point to which the supplicant physically connects, typically a Layer 2 switch. The authenticator acts as a proxy between the supplicant and the authentication server and controls the access to the network based on the authentication status of the supplicant.
- an authentication server—typically a RADIUS server; performs the actual authentication of the supplicant.

There are three supported EAP methods:

- EAP-MD5
- EAP-TLS
- EAP-PEAP/MD5

The administrator selects the EAP method from the EAP configuration menu, as shown in the following figure:

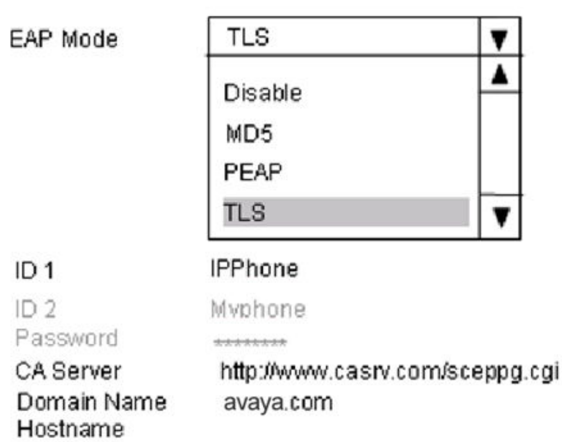


Figure 56: EAP configuration menu

The administrator can do the following:

- When **MD5** is selected, the administrator is prompted to enter ID1 and Password.

- When **PEAP** is selected, the administrator is prompted to enter ID1, ID2 and Password. If the administrator enters only ID1, then ID2 has the same value of ID1.
- When **TLS** is selected, the administrator is prompted to enter ID1.

  Note:

  Before using EAP-TLS, a device certificate must be installed.
- When **Disable** is selected, the existing IDs and passwords are erased.

The following is a list of additional provisioning file parameters for EAP support in addition to the UI parameters on the Device Settings screen

Table 50: EAP Provisioning Parameters

Parameter	Purpose	Default	Allowed
EAP	EAP mode	DISABLED	DISABLED/MD5/PEAP
EAPID1	Device ID1	Empty	String (4 to 20 characters)
EAPID2	Device ID2	Empty	String (4 to 20 characters)
EAPPWD	Password	Empty	String (4 to 12 characters)

EAP Disabled

EAP disabled is the factory default setting. The IP Deskphone does not send a message to the authenticator upon startup, and normal network access is attempted.

If the IP Deskphone receives a Request-Identity message from the Layer 2 switch, the Request-Identity is ignored.

If the Layer 2 switch requires 802.1x authentication, the IP Deskphone is blocked from the network, and the administrator must enable the EAP feature on the IP Deskphone and configure a DeviceID and Password (if required) to access the network after the IP Deskphone is successfully authenticated. Or, the administrator can plug the IP Deskphone to an EAP disabled port on the Layer 2 switch.

EAP-MD5

EAP-MD5 allows the IP Deskphone to authenticate to the RADIUS server before the IP Deskphone can access the network. This procedure requires a user ID and password. If the IP Deskphone fails to authenticate to the RADIUS server, the IP Deskphone displays a `EAP Authenticate-Fail` message, and the IP Deskphone cannot access the network.

EAP-TLS

EAP-TLS allows the IP Deskphone to authenticate to the RADIUS server before the IP Deskphone can access the network. This procedure requires a user ID, root certificate, and device certificate. The root and device certificates must be installed on the IP Deskphone before using this feature. The customer root certificate can be installed using SIP configuration file or using SCEP. For more information, see Trusted Root certificate on page 274 .

The device certificate can be installed using one of two methods:

- Installing a device certificate using PKCS12 on page 277
- Installing a device certificate using SCEP on page 278

If the IP Deskphone fails to authenticate to the RADIUS server or to install the required certificates, the IP Deskphone displays a `EAP Authenticate-Fail` message, and the IP Deskphone cannot access the network.

EAP-PEAP

EAP-PEAP allows the IP Deskphone to authenticate to the RADIUS server before the IP Deskphone can access the network. This procedure requires a user ID1, root certificate, user ID2, and password. EAP-PEAP is the outer authentication protocol that requires a user ID1 and root certificate to establish a TLS channel. EAP-MD5 is the inner authentication protocol that requires a user ID2 and password to pass through this channel in a secure mode. The customer root certificate can be installed using SIP configuration file.

For more information, seeTrusted Root certificate on page 274.

If the IP Deskphone fails to authenticate to the RADIUS server or to install the required certificates, the IP Deskphone displays a `EAP Authenticate-Fail` message, and the IP Deskphone cannot access the network.

EAP Re-authentication

The re-authentication process proceeds in the background without disturbing the ongoing operation of the IP Deskphone. If the re-authentication fails or times out, the IP Deskphone becomes inoperable. Re-authentication interval is controlled by the Layer 2 switch re-authentication interval parameter.

The minimum supported re-authentication interval when EAP-MD5 and EAP-PEAP are configured is 10 seconds; for EAP-TLS, the minimum interval is 20 seconds.

EAP events

EAP Authentication failures are logged using Event 1033.

An example of a TLS authentication failure is as follows:

```
1033 [Minor][FRI MAY 15 13:48:06 2009][10223][n:/fw/build/../bsp/vxWorks/
common/dot
```

```
1x/Supplicant/moceap_tls.c:147] - EAP-TLS Failed to Authenticate
```

Provisioning configuration files download through HTTPS

HTTPS can be used to securely download provisioning configuration files on the IP Deskphone using the following process.

1. The IP Deskphone can contact a provisioning server and download an 11xxeSIP.cfg file to identify additional files and protocols used.
2. When a file is identified, and the protocol specified in the "protocol" parameter is HTTPS, the IP Deskphone contacts the target server and negotiates a TLS connection.
3. The IP Deskphone downloads the specified file and terminates the connection. HTTP connection over TLS is established by using server or mutual authentication.

HTTP connection over TLS is established by using single or mutual authentication.

HTTPS support in BootC mode

When a firmware upgrade is performed and there is not enough memory to allocate a buffer for new firmware, the IP Deskphone automatically reboots and BootC is loaded. HTTPS is supported for downloading provisioning files (for example, 1220SIP.cfg) and firmware images from the Provisioning Server. It uses the embedded and customer certificates that are installed on the IP Deskphone.

BootC downloads the provisioning file (for example, 1220SIP.cfg). Only the [FW] section of this file is processed. BootC uses the same settings (for example, Provisioning Server URL, protocol) that are used in normal mode. BootC performs the firmware upgrade, and the IP Deskphone automatically reboots again. The IP Deskphone starts up with new firmware in Normal mode.

Note:

Regardless of whether the firmware upgrade was successful or not, the [FW] section does not offer to update during the IP Deskphone reboot

Both mutual authentication and server-only authentication methods are supported. The TLS connection cipher is set according to the security policy configured on the IP Deskphone (the security policy must be configured in Normal mode). The default cipher is TLS_RSA_WITH_AES_256_CBC_SHA.

Important:

Customer certificates must be installed in Normal mode.

Server authentication

A server certificate, user name, and password are required to establish TLS connection between the IP Deskphone and the provisioning server. The server certificate must be signed by a certificate authority.

The IP Deskphone uses the server certificate to validate the identity of the provisioning server that the IP Deskphone is connected to; the provisioning server uses the user name and password to authenticate the IP Deskphone. The IP Deskphone must be preloaded with the root certificate used in signing the server certificate. The root certificate is downloaded to the IP Deskphone using a USB flash drive or by connecting to a provisioning server through EAP-MD5, and using one of the insecure protocols supported by the IP Deskphone, such as HTTP, TFTP, or FTP.

EAP-MD5 ensures that the connection between the IP Deskphone and the provisioning server is secure. The user name and password are required to authenticate the IP Deskphone to the provisioning server and must be loaded in a secure manner before the IP Deskphone establishes the HTTPS connection with the provisioning server. There is no mechanism for getting a user name and password on the IP Deskphone in a secure "no-touch" manner; the IP Deskphone must be deployed to a secure network where the TFTP download of insecure files is not transmitted over an insecure network.

Mutual Authentication

A device certificate and server certificate are required to establish TLS connection between the IP Deskphone and the provisioning server.

The server certificate must be signed by a certificate authority. The IP Deskphone uses the server certificate to validate the identity of the provisioning server that the IP Deskphone is connected to; the provisioning server uses the device certificate to validate the identify of the IP Deskphone. The IP Deskphone must be preloaded with the root certificate used in signing the server certificate.

The root certificate is downloaded to the IP Deskphone by a USB flash drive or by connecting to a provisioning server through EAP-MD5, and using one of the insecure protocols supported by the IP Deskphone, such as HTTP, TFTP, or FTP.

EAP-MD5 ensures that the connection between the IP Deskphone and the provisioning server is secure. The administrator must use the existing device certificate (this certificate is used for EAP-TLS, SIP-TLS and HTTPS) to establish mutual authentication.

For information about device certificate installation and certificate profiles, see Device certificate installation process on page 276.

Security and error logs

You can access the Security Log and the Error Log to view errors and failures that may have occurred during the operation of the IP Deskphone.

Before you can access the Security and Error Logs, you must configure the Security Policy file with the SECURITY_LOG_UI_ENABLE YES parameter:

If configured as yes, you can access the Security and Error Logs from the Network screen by selecting **Device Settings** > **Security and Error Logs**.

The Security and Error Logs are stored in the Logs folder. To access the Security and Error Logs, select File Manager > Logs folder, and then press the **Globe** key.

The Logs main menu lets you choose one of the following options:

1. Security Log
2. Error Log

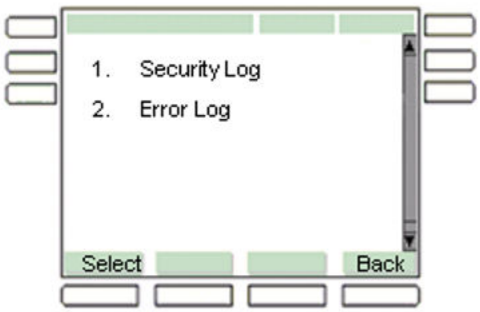


Figure 57: Logs main menu

When the user selects a log file, the screen displays each log item on a full screen, as shown in the following figure:

Figure 58: Log item screen

The following table describes the function of the context-sensitive soft keys for the log item screen.

Table 51: Context-sensitive soft keys for the log item screen

Context-sensitive soft key	Action
Next	Navigates to the next log entry.
Prev	Navigates to the previous log entry.
Back	Returns you to the Logs main menu.

Diagnostic events

All EAP failures are logged in the security log, which includes the following EAP error messages:

`EAP_MD5_AUTH_FAILURE 0x1030`

`EAP_INVALID_DEVICE_CERTIFICATE 0x1031`

`EAP_INVALID_ROOT_CERTIFICATE 0x1032`

`EAP_TLS_AUTH_FAILURE 0x1033`

`EAP_PEAP_AUTH_FAILURE 0x1034`

The following is a list of certificate-related events and failures logged in the Security Log.

`SLC_AVAYA_CERTIFICATE_IMPORTED 0x0006`

`SLC_SERVICE_PROVIDER_CERTIFICATE_IMPORTED 0x0007`

`SLC_AVAYA_CERTIFICATE_REVOKED 0x0008`

`SLC_SERVICE_PROVIDER_CERTIFICATE_REVOKED 0x0009`

`SLC_AVAYA_CERTIFICATE_EXPIRED 0x000A`

`SLC_SERVICE_PROVIDER_CERTIFICATE_EXPIRED 0x000B`

`SLC_CERTIFICATE_DELETED 0x000`

`CSLC_CRL_IMPORTED 0X000D`

`SLC_OLDER_CRL_REMOVED 0x000E`

`SLC_FACTORY_DEFAULTS_RESTORED 0x000F`

`SLC_DEVICE_CERTIFICATE_CREATED 0x0010`

`SLC_CRL_SIGNATURE_REJECTED 0x0011`

`SLC_CTL_CERTIFICATE_EXPIRED 0x0012`

`SLC_AVAYA_CERTIFICATE_DELETED 0x0013`

`SLC_SERVICE_PROVIDER_DELETED 0x0014`

`SLC_CTL_DELETED 0x0015 SLC_CRL_DELETED 0x0016`

`SLC_DEVICE_CERTIFICATE_DELETED 0x0017`

`SLC_DEVICE_CERTIFICATE_REVOKED 0x0018`

`SLC_DEVICE_CERTIFICATE_EXPIRED 0x0019`

`SLC_CTL_EXPIRED 0x0020`

`SLC_CTL_DOWNLOAD_ERROR 0x0021`

The following is a list of minor errors that are logged in the Security Log.

`SLC_AVAYA_CERTIFICATE_EXPIRED_AUTH 0x1002`

`SLC_SERVICE_PROVIDER_CERTIFICATE_EXPIRED_AUTH 0x1003`

`SLC_PROVIDER_CERTIFICATE_IN_AVAYA_KEYS_FILE 0x1004`

`SLC_PKI_MGMT_INIT_FAILURE 0x1005`

The following is the Security Policy parameter change event.

`SECURITY_POLICY_PARAM_CHANGE 0x1055`

Any changes made to the security policy file has an entry in the security log file. For more information, see Security policy logs and diagnostics on page 293.

Fault management behavior

Authentication failures are indicated by a failure message on the IP Deskphone screen and are reported to the error log files. The administrator can view the security logger by using the PDT or the security log viewer. For more information, see Security and error logs on page 300.

A list of authentication failure messages that appear on the IP Deskphone screen when a failure occurs during the operation of the IP Deskphone is as follows:

- EAP Authenticate-Fail – occurs when the IP Deskphone fails to authenticate to an authentication server; the message applies for the three EAP methods: EAP-MD5, EAP-PEAP, and EAP-TLS.
- EAP Authenticate-Timeout – after the third time the IP Deskphone fails to authenticate to an authentication server and the IP Deskphone is connected to an EAP disabled port on the Layer 2 switch.

For EAP failures logged in the security log, see Diagnostic events on page 301.

Creating a signing certificate

About this task

You can create a signing certificate using OpenSSL.

Procedure

1. Add the following section to the openssl.cfg file:

```
[ signing_cert_ext ]
subjectAltName=DNS:www.avaya.com
basicConstraints=CA:FALSE
```

```
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
keyUsage=critical,digitalSignature
extendedKeyUsage=critical,codeSigning,emailProtection
```

2. Use the following OpenSSL command to create a certificate request:

   ```
   openssl req -new -keyout signing_key.pem
               -out signing_req.pem -days 365
   ```

   This creates the following files in PEM format:

   - signing_key.pem, which holds the private key of the signing certificate
   - signing_req.pem, which holds the certificate request

3. Use the following OpenSSL command to create the signing certificate

   ```
   openssl ca     -policy policy_anything -extensions signing_cert_ext
               -out signing_cert.pem -infiles signing_req.pem
   ```

   This command creates the file signing_cert.pem, which holds the signing certificate itself in a PEM format

Next steps

At the end of this process a signing certificate (signing_cert.pem) and its private key (signing_key.pem) are created, which can be used to sign the a resource file using scripts. For information about signing scripts, see

Note:

The above commands are examples of commands that create the files signing_req.pem, signing_key.pem and signing_cert.pem with 365 days lifespan. You can change these names and the lifespan days.

File signing

A file is signed by appending a digital signature, which is created using a Signing Certificate. The Signing Certificate must either be directly issued by a CA root certificate installed on the phone or there must be a certificate chain that can be followed, which ends with a CA root certificate installed on the IP Deskphone. In either case, there must be a trust anchor on the IP Deskphone, which can verify the authenticity of the Signing Certificate.

The file signing certificate requires the following minimum attributes:

- Version –3
- Key Usage – Digital signature
- Extended Key Usage – Code signing, secure e-mail
- Key – 1024 or 2048 bits

In addition, the Signing Certificate cannot be a self-signed root certificate and must have a valid Subject Key Identifier and an Authority Key Identifier (which uniquely identifies the issuing certificate).

You can use many commercial CAs, Open source CAs, such as OpenSSL, and EJBCA to create and manage these certificates. The CA must meet the following requirements:

- The root certificate must be exportable in PEM format without the private key.
- The CA must be capable of issuing a Signing Certificate with the above attributes and an exportable private key.

  This requirement can require additional CA configuration. Often in commercial CAs the private key is not exportable by default. However, the Signing Certificate private key is only required if the CA does not provide built-in support for the creation of detached PKCS7 signatures.

Signing scripts

You can use the following scripts to generate a signed file using OpenSSL (version 0.9.8a or greater) on Linux or Windows. The input requirements in the script include:

- Unsigned data file
  - Validity fields
  - Certificates
- Public Signing Certificate
- Private Key for the Signing Certificate

Important:

• The signing certificate and associated private key must be exported from the Certificate Management system. Some Certificate Management systems (for example, Microsoft CA Server) restrict the ability to export the private key. You must take care when you generate certificates to ensure that you properly configure the ability to export.

You should sign the file in a secure environment because the signing certificate private key must be accessible. If the private key is password-protected, you must enter this password to successfully create a signature.

Examples of two scripts that can be used to sign are resource file (for example, CTL file) are as follows:

- OpenSSL-based Linux script for file signing

```
#!/bin/sh
# $1 - Input Unsigned File
# $2 - Signing Certificate
# $3 - Signing Certificate Private Key
# $4 - Output Signed File
unsigned_file=$1
sign_cert_file=$2
sign_cert_pk_file=$3
signed_file=$4
# Setup temporary files
tmp_signature_file="/tmp/resource$$.tmp"
# Create a detached signature
openssl smime -sign -in ${unsigned_file} -signer ${sign_cert_file}
-outform PEM -binary -inkey ${sign_cert_pk_file} -out ${signed_file}
# Now append the signature to the unsigned file
cat ${unsigned_file} ${tmp_signature_file} > ${signed_file}
```

```
# Clean up
rm -f ${tmp_signature_file}
```

- OpenSSL-based Windows script for file signing

```
REM %1 - Input Unsigned File
REM %2 - Signing Certificate
REM %3 - Signing Certificate Private Key
REM %4 - Output Signed File
set unsigned_file=%1
set sign_cert_file=%2
set sign_cert_pk_file=%3
set signed_file=%4
REM Setup temporary files
set tmp_signature_file="sig.tmp"
REM Create a detached signature
openssl smime -sign -in %unsigned_file% -signer %sign_cert_file% -outform
PEM -binary -inkey
%sign_cert_pk_file% -out %tmp_signature_file%
REM Now append the signature to the unsigned file
copy /y /b %unsigned_file% + %tmp_signature_file% %signed_file%
REM Clean up
del %tmp_signature_file%
```

You can use other Certificate Management systems if the system includes the ability to generate a detached signature.

Chapter 16: Licensing

A license is a "right to use" granted by Avaya, that the customer purchases to enable the features on the IP Deskphone. A license contains at least one entitlement and can contain more than one entitlement. A license usually has an expiry date and is keyed for a specific license server.

An entitlement is the most basic component of a license and represents a single instance of a right to a particular feature or capability. Entitlements are feature-related information passed to the server through licenses. Entitlements are also known as tokens or keycodes.

On Avaya IP Deskphones, the licensing solution uses the Embedded Server Model. In this model, the licensing server is embedded on the IP Deskphone and executes on the phone. There is a one—to—one relationship between the license file and IP Deskphone. There are no multiple IP Deskphones per server in the embedded server model; each IP Deskphone has its own embedded server. The IP Deskphone does not have to connect to a remote server to obtain tokens; instead, it calls the license server locally on the IP Deskphone. There are two modes of operation in this model.

- Node Locked Solution
- Network Locked Solution

In the Node Locked Solution within the embedded server model, the administrator obtains a license file for each IP Deskphone, and the license file is installed onto the IP Deskphone through the provisioning infrastructure.

For the Network Locked Solution within the embedded server model, the administrator obtains a generic license file, and the license file is installed onto the IP Deskphones through the provisioning infrastructure.

The Embedded Server Model does not provide the following capabilities:

- Grace period handling
- SSL communication with the IP Deskphone as the server is local to the phone
- Crediting or transfer of entitlements
- Web-based OAM interface. There is no OAM functionality to upload the license file to an IP Deskphone.

Licensing framework supports two types of tokens.

1. Time Based Tokens — These tokens expire based on the expiry date associated with the key code.
2. Standard tokens — The warranty date on these tokens is verified based on firmware build and contract dates available from the IP Deskphone.

Important IP Deskphone licensing information is located in the Keycode Retrieval System (KRS) User Guide. You must register for access to KRS.

Accessing the Keycode Retrieval System

The Keycode Retrieval System (KRS) User Guide provides important IP Deskphone licensing information. You must register for access to KRS. The ollowing section describes how to access the KRS User Guide.

Registering for access to KRS

1. Go to http://support.avaya.com/krs.

   Users must have an Avaya Access registration profile to access the KRS application
2. Follow the instructions on this page to obtain an Avaya Access registration profile and to request access to KRS.
3. On the right side of the page, click **KRS Site** and log in when prompted
4. Select **IP CLIENTS** from the list for the product whose keycodes you would like to access.

Licensing framework

The licensing framework contains the fundamental infrastructure required to deliver a token-based licensing model that consists of a node-locked based licensing server and a licensing client.

The licensing framework consists of the following components:

- License Server (node-locked)—embedded in the IP Deskphone and calls the server locally.
- License Client—resides in the IP Deskphone and makes requests to the License Server for tokens.
- KRS integration—a key or license generator provided with the CKLT solution which is integrated into the Keycode Retrieval System (KRS).

  Note:

  The KRS generates only standard tokens.

Characteristics of the licensing framework

The following list describes the characteristics of the licensing framework on the IP Deskphone.

- The embedded server relies on a real time clock to calculate when a token expires
- The embedded server (node-locked) enables the license server to execute on the IP Deskphone. The IP Deskphone obtains tokens by calling the server locally.
- The license file is installed on the IP Deskphone through the provisioning server or TFTP server.
- The IP Deskphone does not have an internal real-time clock. The time of day is obtained from the Call Server that the IP Deskphone is registered to on the network.

- The license file contains only one type of token because the IP Deskphone only uses one type at a time.
- The administrator must enter the IP Deskphone system ID directly into the Keycode Retrieval System (KRS).
- A Node Locked license file is keyed for the IP Deskphone so that the license is only valid on a specific IP Deskphone.
- A Network Locked license file can be installed on a limited number of IP Deskphones at a given site.
- The system ID is the MAC of the IP Deskphone.
- When the IP Deskphone is connected to an Avaya server, the IP Deskphone gets an additional token.

License file download

This section describes the procedure for downloading Node Locked license files and the procedure for downloading Network Locked license files.

Node Locked license file download

Use the following procedure to download Node Locked license files keyed to each phone by MAC address from the provisioning or TFTP server.

Downloading Node Locked license files:

1. Configure the IP Deskphone with a provisioning IP address so it can access a provisioning server.

   For more information about provisioning parameters for the IP Deskphone, see Create the SIP provisioning file on the provisioning server on page 46.
2. The IP Deskphone config file must include a [LICENSING] section to enable the IP Deskphone to download the licence file. Add [LICENSING] section to the IP Deskphone .cfg file.

   Examples of IP Deskphone cfg files are 1120eSIP.cfg, 1140eSIP.cfg, and 1165eSIP.cfg.

   The [LICENSING] section specifies a wild card filename which uses the IP Deskphone MAC address as the filename with the ipctoken prefix and cfg suffix.

   For example:

   ```
   [FW]
   DOWNLOAD_MODE AUTO
   VERSION 04.04.09.00
   PROTOCOL TFTP
   FILENAME SIP1140e04.04.09.00.bin
   ...
   ```

```
[LICENSING]
DOWNLOAD_MODE AUTO
VERSION 000001
FILENAME ipctoken*.cfg
```

3. Place the IP Deskphone license file on the provisioning server.

   The generated license file must be named ipctokenMAC.cfg, where MAC is the 12-character MAC address of the IP Deskphone.

   For example, for an IP Deskphone with MAC address "000f1fd304f8", the license file will be named " ipctoken000f1fd304f8.cfg".
4. Start the provisioning server so the IP Deskphone can retrieve the .cfg files when the server starts.

When the new license file is downloaded to the IP Deskphone from the provisioning server, it overwrites the existing license file and reboots the IP Deskphone to activate the new license.

Network Locked license file download

If a Network Locked license file is to be used, the same license file can be installed on all IP Deskphones. In this case, the wildcard "*" is not used in the FILENAME, as the filename is fixed and does not contain the MAC address of each IP Deskphone.

Use the following procedure to download a Network Locked license file from the provisioning or TFTP server.

Downloading a Network Locked license file:

1. Configure the IP Deskphone with a provisioning IP address so it can access a provisioning server. For more information about provisioning parameters for the IP Deskphone, see Create the SIP provisioning file on the provisioning server on page 46.
2. The IP Deskphone config file must include a [LICENSING] section to enable the IP Deskphone to download the licence file. Add [LICENSING] section to the IP Deskphone .cfg file.

   Examples of IP Deskphone cfg files are 1120eSIP.cfg, 1140eSIP.cfg, and 1165eSIP.cfg.

   For example:

```
[FW]
DOWNLOAD_MODE AUTO
VERSION 04.04.09.00
PROTOCOL TFTP
FILENAME SIP1140e04.04.09.00.bin
...
[LICENSING]
DOWNLOAD_MODE AUTO
VERSION 000001
FILENAME ipctoken.cfg
```

3. Place the IP Deskphone license file on the provisioning server.
4. Start the provisioning server so the IP Deskphone can retrieve the .cfg files when the server starts.

When the new license file is downloaded to the IP Deskphone from the provisioning server, it overwrites the existing license file and reboots the IP Deskphone to activate the new license.

[LICENSING] section

The IP Deskphone config file must include a [LICENSING] section to enable the IP Deskphone to download the licence file. The [LICENSING] section specifies a wild card filename which uses the IP Deskphone MAC address as the filename with the cfg prefix and suffix.

The following format is an example of the [LICENSING] section that is added to the IP Deskphone config file (1xxxe.cfg):

[LICENSING] VERSION version FILENAME X*.Y

The following table describes the items in the [LICENSING] section.

Table 52: Description of items in the [LICENSING] section of the config file.

Field name	Field value	Description
[LICENSING]	—	Section header for licensing config file information.
VERSION	000001	The version of the license file.
FILENAME	X*.Y	License filename. The IP Deskphone looks for a file with the IP Deskphone MAC address included in the filename.

The 1xxxe.cfg file can have one, or all, of the following sections:

- [FW]
- [DEVICE_CONFIG]
- [LICENSING]

Although the IP Deskphone [FW] section is not required to activate the token, the provisioning server and the IP Deskphone provisioning server IP configuration must be configured to retrieve, save, and process the license file.

The following is an example of an 11xxe.cfg file that contains the [FW] section and the [LICENSING] section.

```
[FW]

DOWNLOAD_MODE AUTO

VERSION VERSION 04.04.09.00

FILENAME SIP1140e04.04.09.00.bin
```

```
PROTOCOL TFTP
SERVER_IP 47.11.183.165
...
[LICENSING]
VERSION 000001
FILENAME ipctoken*.cfg
```

The following is an example of an 11xxe.cfg file with the [LICENSING] section only.

```
[LICENSING]
VERSION 000001
FILENAME ipctoken*.cfg
```

License information for the IP Deskphone

The Licensing information screen provides information on Embedded Mode, status and other licensing information.

To access the licensing feature, press the **Globe** key twice.

Select **Prefs > Network > Licensing** and select **1. License Info**. Enter admin password (if prompted).

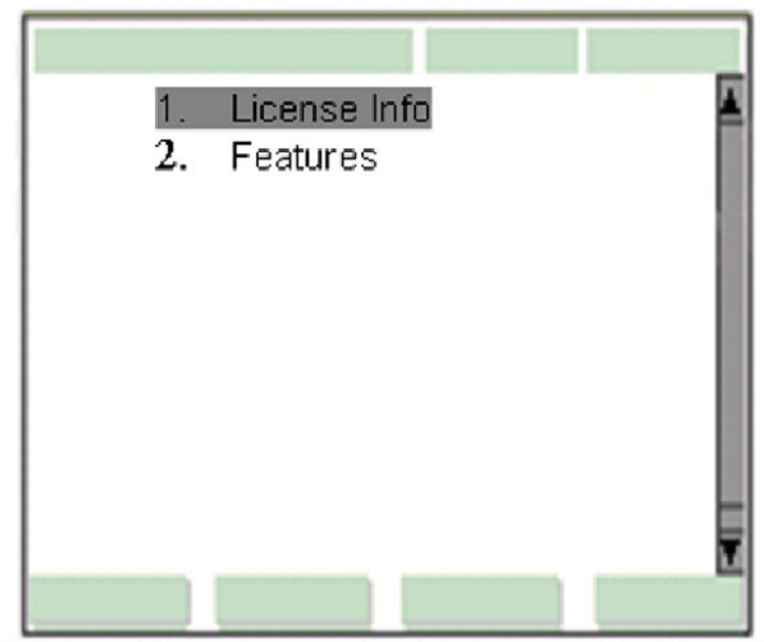


Figure 59: License Info

Licensable features

Licensable features are divided into three groups.

1. Basic Feature Set
2. Enhanced Feature Set - 1 token required
3. Advanced Feature Set - 2 tokens required

Basic Features are always enabled on the IP Deskphone. Enabling the Enhanced Feature Set requires an additional token. Enabling the Advanced d Feature Set requires two tokens.

When connected to an Avaya Server, the IP Deskphone receives an additional token. This means that the Enhanced Feature Set is available when the IP Deskphone connects to an Avaya server.

Note:

When the license is verified, the number of required tokens is set to null if the IP Deskphone is connected with Avaya Aura® Application Server 5300.

Access Licensable features list

The **Licensable features** screen can be accessed through the IP Deskphone menu using **Prefs > Network > Licensing** and selecting **2. Features**.

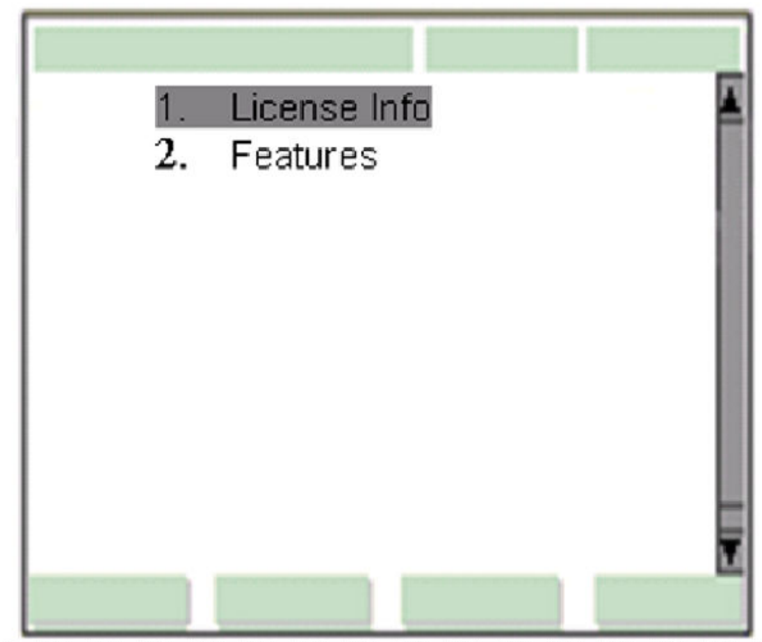


Figure 60: Licensing menu

The **Licensable features** screen displays.

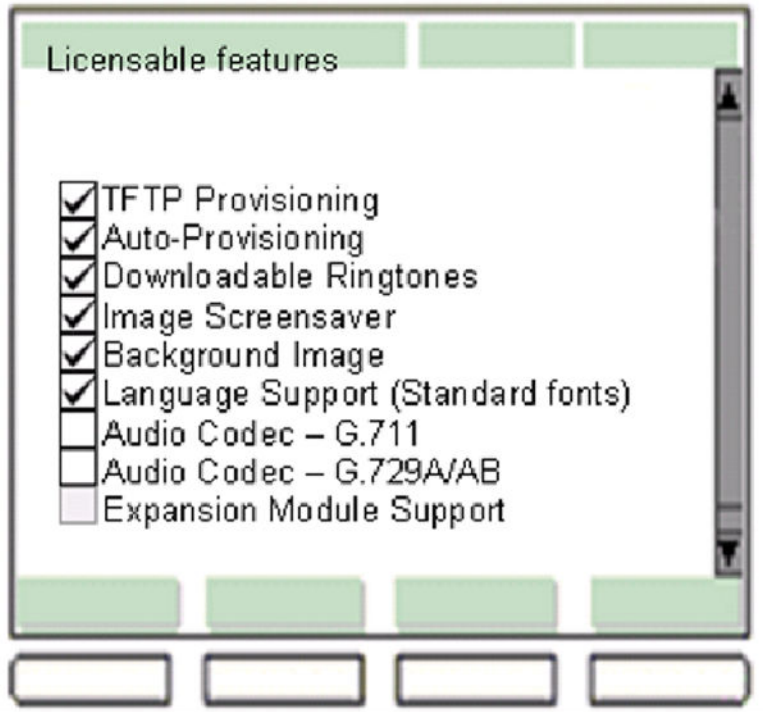


Figure 61: Licensable features screen

Node-locked license mode

In the node-locked license mode, the IP Deskphone uses a license file to acquire the required tokens needed to activate the features. There are two types of tokens: time-based tokens, and standard tokens.

Time-based token

The following figure is an example of a node-locked time-based token. In this example, the embedded server on the IP Deskphone contains 5 tokens and the IP Deskphone is enabled for Advanced Feature Set and connected to a non-Avaya server.

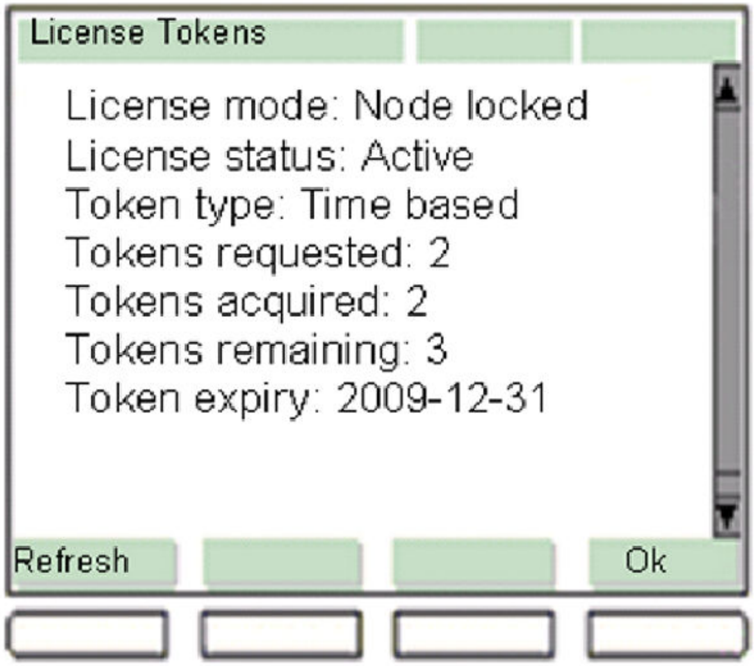


Figure 62: Node-locked license mode — License information for time-based token (connected to non-Avaya Server)

The following figure is an example of a node-locked time-based token. In this example, the embedded server on the IP Deskphone contains 5 tokens and the IP Deskphone is enabled for Advanced Feature Set and connected to an Avaya server.

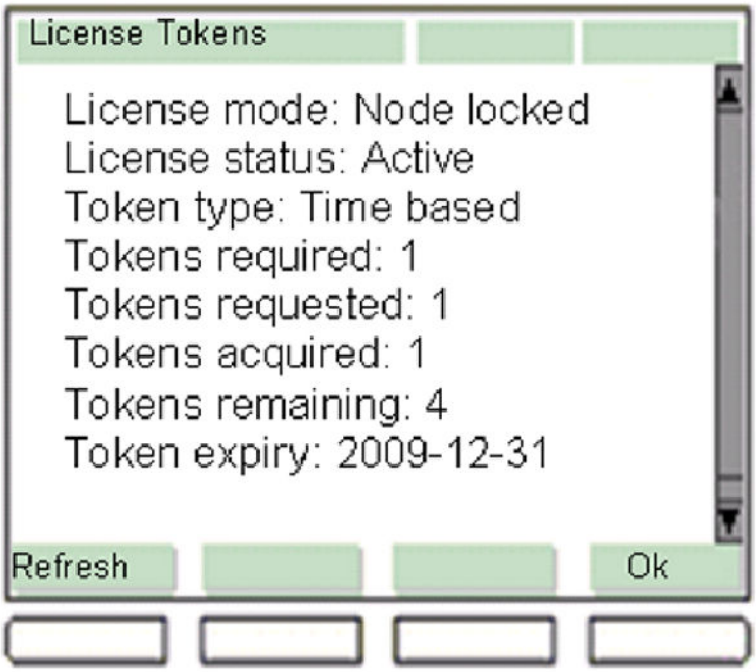


Figure 63: Node-locked license mode — License information for time-based token (connected to Avaya Server)

Note the extra line Tokens Required: 1. This line is displayed only when the IP Deskphone connects to an Avaya Server.

The status of the time-based token can be one of the following:

- Active
- Inactive

A time-based token can be inactive for one of the following reasons:

- Insufficient tokens
- License expired

Standard token

The following figure is an example of a node-locked Standard token. In this example, the embedded server on the IP Deskphone contains five tokens. The IP Deskphone is enabled for Advanced Feature Set and is connected to a non-Avaya server.

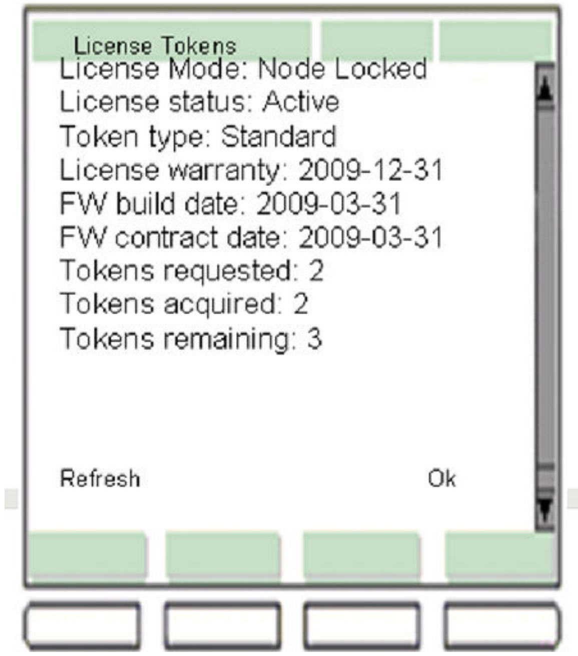


Figure 64: Node-locked license mode — license information for Standard token (connected to non—Avaya Server)

The following figure is an example of a node-locked Standard token. In this example, the embedded server on the IP Deskphone contains five tokens. The IP Deskphone is enabled for Advanced Feature Set and is connected to an Avaya server.

Note that the extra line **Tokens Required: 1** is displayed only when the IP Deskphone connects to an Avaya Server. The extra line **Token Type:** is displayed if a feature requests a token.

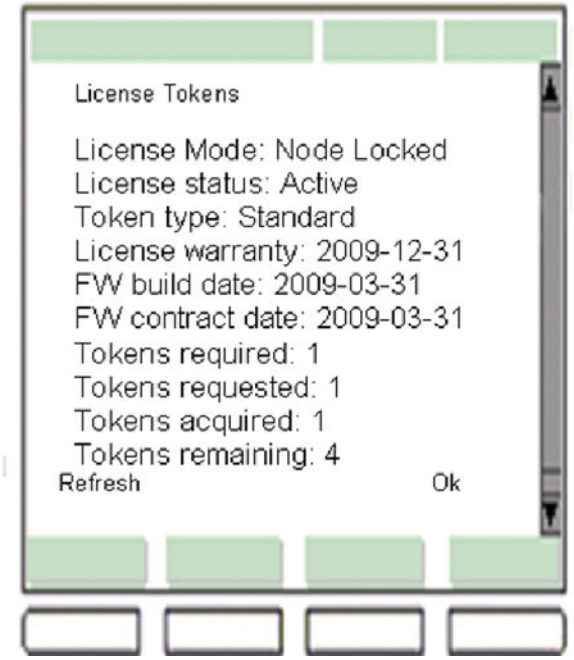


Figure 65: Node-locked license mode — license information for Standard token (connected to Avaya Server)

The status of the standard token can be one of the following:

- Active
- Inactive

A standard token can be inactive for one of the following reasons:

- Insufficient token
- License expired

Invalid or no license file

The following figure is an example of an invalid or no license file.

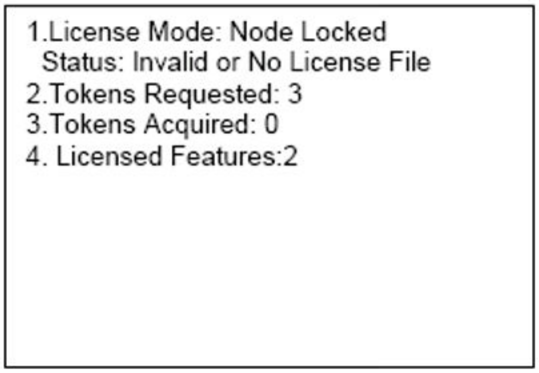


Figure 66: License information — Invalid or no license file

Evaluation period

When the IP Deskphone arrives from the factory, it has a 31–day evaluation period. This period allows users to try licensed features before they actually purchase the tokens. Any time the user loads a valid license file and has tokens granted, the evaluation is terminated immediately.

Note:

Once the evaluation period expires, there is no way to reset it.

The following figure is an example of the IP Deskphone with 15 days left in the evaluation period.

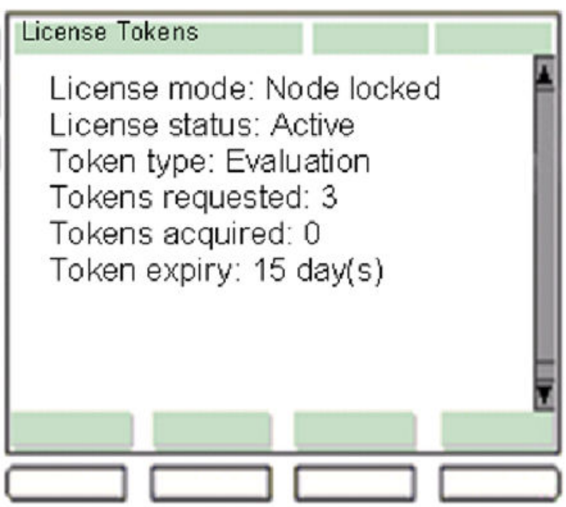


Figure 67: IP Deskphone in an evaluation period

Alarms

The license feature provides notifications on the IP Deskphone screen about the licensing status. The license feature provides notification on the IP Deskphone screen if the following conditions apply:

- No avaliable tokens
- Expired tokens
- Evaluation period has ended

A notification message is displayed in a pop-up window on top of the IP Deskphone screen. The window can be dismissed by pressing the **Stop** key or by lifting the handset. After the message is dismissed, the IP Deskphone closes the warning window. The warning window re-displays every 24 hours at 1:00 am. You can configure the time frame through the IP Deskphone configuration system. If the licensed features are disabled, the IP Deskphone cannot display any type of window warning.

Support warning

A Support warning is used to direct the user to contact technical support. The actual label displayed on the screen and the contact information are specified in the device configuration file.

License not available warning

A warning window, indicating that a license is not available, appears on the IP Deskphone screen when the token request or refresh is rejected due to insufficient tokens available or an invalid license file.

The following figure is an example of a warning window indicating that a license is not available.

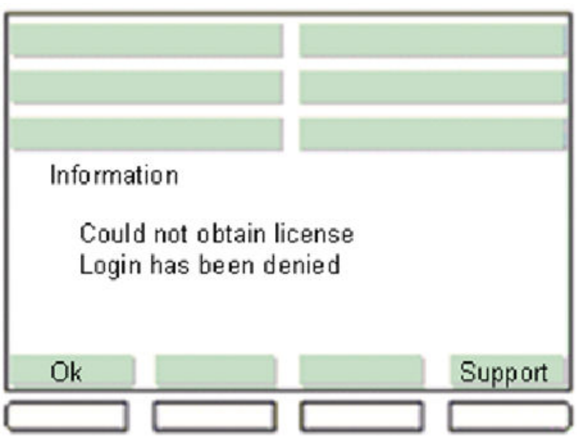


Figure 68: License not available warning

License expiry warning

A warning window, indicating that a license has expired, appears on the IP Deskphone screen when a node-locked license expires.

The following figure is an example of a warning window indicating that a license is expired.

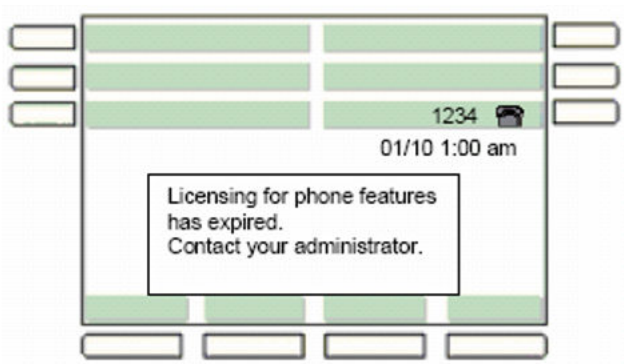


Figure 69: License expiry warning

Evaluation period expiry warning

A warning window, indicating that the evaluation period has expired, appears on the IP Deskphone screen when the evaluation period expires and if the IP Deskphone has never had a valid token grant.

The following figure is an example of a warning window indicating that the evaluation license period is expired.

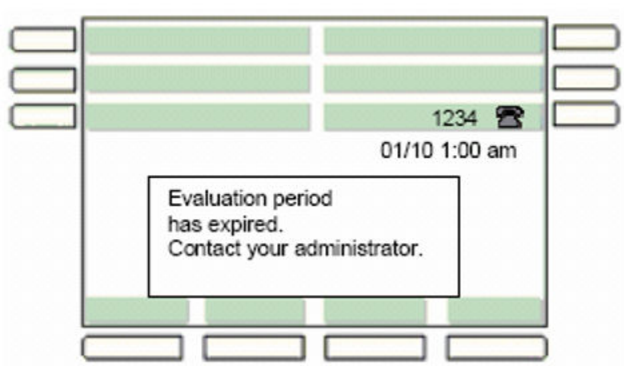


Figure 70: Evaluation period expiry warning

Evaluation threshold warning

A warning window informing you of the approaching evaluation expiration date appears on the IP Deskphone at the following predefined times:

- 15 days before expiration date
- 7 days before expiration date
- 1 day before expiration date

The following figure is an example of the evaluation threshold warning.

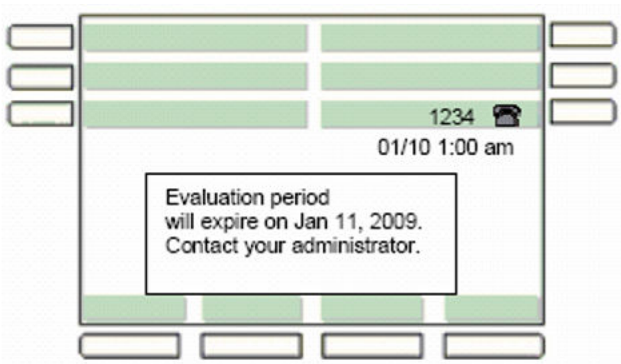


Figure 71: Evaluation threshold warning

Licensing expiry threshold warning

When the expiration date of the node-locked licence approaches,, a warning window is displayed on the IP Deskphone. The warning window indicates when the license will expire, and notifies you at the following predefined times:

- 30 days before the license expires
- 15 days before the license expires
- 7 days before the license expires
- 1 day before the license expires

The following figure is an example of the license expiry threshold warning.

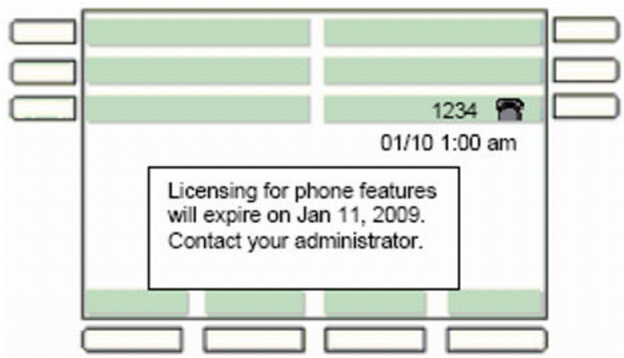


Figure 72: License expiry threshold warning

Licensed features

The following Standard features are available to all users without a token.

- SIP Core Features (RFC3261 and SIPPING 19)
- 3-way calling and conference calling
- Audio codecs - standard and wideband
- Auto Login and Auto Logout
- Background Image
- Busy Lamp Field (BLF)
- Distinctive ringing
- Downloadable ringtones
- Image screensaver and lock
- Standard font languages
- Multiple calls per user
- Server failover redundancy
- Session timers
- SNTP (time server)
- Speed Dial List
- Transfer to VM softkey
- USB flash drive
- Hotline

The following extended features are available with a token or if the IP Deskphone is registered to a recognized Avaya server (Avaya, Avaya Communication Server 1000, or IP Office) then extended features are available without a token.

- Standard features

- Authentication security
- Bluetooth headset support (1140E/1165E)
- Call Server Service Package
- Expansion Module support
- Instant Messaging
- Media Security (SRTP)
- Multiuser login support
- NAT Traversal/STUN
- Proactive Voice Quality Management
- PC Client Control
- Signaling Security (TLS)
- USB headset support for audio
- IPv6 support

The following advanced features are available with two tokens or if the IP Deskphone is registered to a recognized Avaya server (Avaya, Avaya CS 1000, or IP Office) then advanced features are available with one token.

- Standard features
- Extended features
- MLPP (Federal)
- Call Origination Busy
- DoD Network
- FIPS Certified

Chapter 17: Internet Protocol version 6

Internet Protocol version 6 (IPv6) is a network layer for packet-switched internetworks and is the successor of IPv4.

Important:

IPv6 is not supported on Avaya Aura®.

IPv6 provides larger address space, which allows greater flexibility in assigning addresses. The extended address length used within IPv6 eliminates the need to use Network Address Translation to avoid address exhaustion to simplify the aspects of address assignment and renumbering when changing providers.

The IP Deskphones can be configured to support IPv4 and IPv6 protocols. IP Deskphones use IPv4 mechanisms (for example, DHCP) to acquire their IPv4 addresses and IPv6 mechanisms (for example, Stateless autoconfiguration) to acquire their IPv6 addresses.

IPv6 uses a hierarchical method to allocate IP addresses, which provides simplified routing and renumbering.

IPv6 provides the following:

- 128 bits for address space compared to 32 bits for IPv4
- well defined Quality of Service (QoS) mechanism
- simplified configuration (stateless autoconfiguration)

SIP IP Deskphones provide complete support for IPv4 and IPv6 Internet protocols, as follows:

- provides transition mechanism to IPv6
- enables SIP IP Deskphones to interoperate with IPv4 hosts and utilize IPv4 routing
- able to send and receive both IPv4 and IPv6 packets
- interoperates directly with IPv4 nodes using IPv4 packets
- interoperates directly with IPv6 nodes using IPv6 packets

IPv6 and IPv4 IP Deskphones operate in on of two modes:

- both IPv4 enabled and IPv6 stack disabled (default)
- both IPv4 and IPv6 stacks enabled

IPv6 address entry

Addresses are entered using hexadecimal or alphanumeric formats. The tables below list the key sequences.

Table 53: Hexadecimal key sequence

Key	Sequence
0	0
1	1
2	2abc
3	3def
4	4
5	5
6	6
7	7
8	8
9	9
*	.

The dot (.) is entered by pressing the asterisk (*) twice.

Table 54: Alphanumeric key sequence

Key	Sequence
0	0 + = < > $ % & @ ~ ^
1	1 _ - . ! : /\ \ ` ? ! ( ) , ;
2	2abcABC
3	3defDEF
4	4ghiGHI
5	5jklJKL
6	6mnoMNO
7	7pqrsPQRS
8	8tuvTUV
9	9wxyzWXYZ
*	*

IPv6 address format

When an IPv6 address is entered, different but equivalent formats can be used for the same address. For example, the following addresses are all equivalent:

```
2001:0db8:0000:0000:0000:0000:1428:57ab
2001:0db8:0000:0000:0000::1428:57ab
2001:0db8:0:0:0:0:1428:57ab
2001:0db8:0:0::1428:57ab
2001:0db8::1428:57ab
2001:db8::1428:57ab
```

Any of the above formats can be entered. When the IP address is displayed again, the abbreviated format is used; for example, `2001:db8::1428:57ab`. This same rule applies to the Phone IP address, DNS Server IP address, Provisioning Server IP address, and SIP Server IP addresses.

Additional supported redirect scenarios

SIP 4.4 introduces support for the following redirect scenarios:

- Redirect from IPv4 to IPv6 SIP proxy through UDP, TCP and TLS
- Redirect from IPv6 to IPv4 proxy through TCP and TLS
- Redirect from IPv6 to IPv6 SIP proxy with the IPv6 address belonging to a different IPv6 scope through UDP

IPv6 limitations

The list below provides IPv6 limitations.

- IPv6 only mode is not supported.
- Site Local address, Anycast address, IPv6 Addresses with Embedded IPv4. IPv4-Mapped IPv6 Address, Unicast-Prefix-based IPv6 Multicast address are not supported. However, if they are obtained through Neighbor Discovery (ND) or DHCPv6, they are assigned to the interface.
- The Avaya 1120E IP Deskphone provides a smaller FLASH memory footprint (8 Mb), which can limit the amount of functionality that can be implemented (as compared to the Avaya 1140E IP Deskphone with 16 MB of FLASH memory).
- Plug-and-Play is not supported due to DHCPv6 limitations as some DHCPv6 options are not supported.
- A customer must engineer a network to provide both DHCPv4 and DHCPv6 servers.
- BootC does not support IPv6.
- The IP Deskphone supports DHCPv4/DHCPv6, FTPv4/FTPv6/TFTPv4/HTTPv4 and DNSv4/DNSv6 for automatic firmware download.

- For IPv6 RTP only or SRTP only modes are supported. Mixture of RTP and SRTP is not supported.
- SRTP BE-Cap Neg cannot be configured when IPv6 is enabled

IPv6 Stateless address autoconfiguration

The IP Deskphone supports stateless address autoconfiguration as defined by RFC 2463 and RFC 2461.

Stateless and stateful (DHCPv6) address autoconfiguration can be used simultaneously. For example, the IP Deskphone IP address can be obtained by stateless address autoconfiguration and configuration information can be obtained by stateful (DHCPv6) address autoconfiguration.

The IPV6_STATELESS YES | NO device configuration parameter allows stateless address autoconfiguration to be disabled. Stateless address autoconfiguration is disabled by default.

IPv6 stateful address autoconfiguration

IPv6 stateful address autoconfiguration (DHCPv6) protocol can be used separately or concurrently with stateless autoconfiguration to obtain configuration parameters as defined by RFC 3315.

The DHCPv6 server can provide IP addresses to a client and other configuration information, which are carried in options. DHCPv6 is extended through the definition of new options codes in OPTION_VENDOR_OPTS option 17.

DHCPv6 is the primary mechanism for the IPv6 address allocation and the stateless address allocation is optional. DHCP is enabled by default. DHCP can be manually disabled on the IP Deskphone.

DHCP dual mode operation

In a dual mode, DHCPv4 and DHCPv6 clients run in parallel. The DHCPv4 client can provide IPv4 configuration attributes, such as IPv4 address, IPv4 Subnet Mask, GW IPv4 address, Voice VLAN ID, Provisioning Server address, and menulock option). This can complement partial implementation of DHCPv6 client. When IPv6 is disabled, DHCPv6 is disabled, as well.

DHCPv6 provides configuration attributes for the Phone IP address, DNS Server address, and SIP Server address.

A maximum of one Phone IP address, two SIP Server IP addresses, and one Provisioning Server IP address are supported. The first two SIP Server IP addresses are assigned to S1 and S2 for the first domain name. If the DHCPv6 server is configured with the SIP proxy IPv6 address, the IP Deskphone registers with the IPv6 address.

If the DHCPv6 server is configured with the SIP proxy IPv4–mapped address, the IP Deskphone registers with its IPv4 address. If the DHCPv6 server is configured with the SIP proxy IPv4-mapped and IPv6 addresses, the DHCPv6 client calls the destination address selection algorithm and selects the address based on the configured preference. If PREFER_IPV6 is configured to YES, the IP Deskphone selects the IPv6 address of the highest precedence.

Server specifications

All servers in a network can be IPv4 mode, IPv4/IPv6 dual mode, or IPv6 mode.

When the IP Deskphone is configured to operate in dual mode, DHCPv4 or DHCPv6, or a dual mode DHCP server must be available, otherwise the IP Deskphone does not boot up.

Internet Control Message Protocol for IPv6

Internet Control Message Protocol for IPv6 (ICMPv6) is a required IPv6 standard defined by RFC 4443.

With ICMPv6, hosts and routers that use IPv6 communication can report errors encountered in processing packets and send simple echo messages for diagnostics.

ICMPv6 provides the framework for the following:

- • Neighbor Discovery as defined by RFC 2461
- • Multicast Listener Discovery (MLD) as defined by RFC 2710

Configuring the DHCP server

The DHCPv4 and DHCPv6 servers must be installed to run on the same box. If Dibbler DHCPv6 server is used, go to http://klub.com.pl/dhcpv6 for installation guidelines.

To stop and start the DHCPv6 server, use the following:

```
/etc/init.d/dibbler-server run /* prints all server debug messages*/
/etc/init.d/dibbler-server start
/etc/init.d/dibbler-server stop
/etc/init.d/dibbler-server status
```

The configuration file is located at: `/etc/dibbler/server.conf`.

The DHCPv6 configuration file that can be used for the IP Deskphone stateful configuration is as follows:

```
#
# Example server configuration file: per-client configuaration
#
# In this example, some clients receive different parameters than others.
#

# Logging level range: 1(Emergency)-8(Debug)
#
log-level 8

# Don't log full date
log-mode short

iface "eth1" {
T1 600
T2 900
prefered-lifetime 1800-3600
valid-lifetime 3600-86400

#rapid-commit yes
#preference 255

# assign addresses from this pool
class {
   #it might be possible to define multiple pools with the same prefix length
   pool fdde:b1a8:d98d:0000:2F87:9FBC:0A0A:0AC8 - fdde:b1a8:d98d:0000:2F87:9FBC:0A0A:0ACa
}

#assign /96 prefixes from this pool
pd-class {
     pd-pool 3000:458:ff01:ff03:abcd::/80
pd-length 96
     T1 11111
     T2 22222
 }

  # common configuration options, provided for all clients
  option dns-server fdde:b1a8:d98d:0:2f87:9fbc:a0a:a01, fdde:b1a8:d98d:0:2f87:9fbc:a0a:a02
  option lifetime 7200
  option domain example.com
#  option vendor-spec 5678-0x0002aaaa,1234-0x00020102

# provide VoIP parameter (SIP protocol servers and domain names) for all clients
# option sip-server 2000::300,2000::302,2000::303,2000::304
 option sip-server fdde:b1a8:d98d:0:2f87:9fbc:a0a:a01, fdde:b1a8:d98d:0:2f87:9fbc:a0a:a02,

 fdde:b1a8:d98d:0:2f87:9fbc:a0a:a03, fdde:b1a8:d98d:0:2f87:9fbc:a0a:a04, fdde:b1a8:d98d:
0:2f87:9fbc:a0a:a05,
 fdde:b1a8:d98d:0:2f87:9fbc:a0a:a06, fdde:b1a8:d98d:0:2f87:9fbc:a0a:a07, fdde:b1a8:d98d:
0:2f87:9fbc:a0a:a08,
 fdde:b1a8:d98d:0:2f87:9fbc:a0a:a09, fdde:b1a8:d98d:0:2f87:9fbc:a0a:a0a
 option sip-domain sip1.avayaexample.com, sip2.avayaexample.com, sip3.avayaexample.com,

sip4.avayaexample.com, sip5.avayaexample.com

  # special parameters for client with MAC based DUID 00:01:02:03:04:06
  client duid 0x001365FEF48D
  {    #client with DUID 0x001365FEF48D gets this address.
    #DNS and SIP server addresses are assigned from the common options above
        address fdde:b1a8:d98d:0000:2F87:9FBC:0A0A:0AC8
  }
```

```
  client duid 0x0016ca0081f7
  {
    #client with DUID 0x001365FEF48D gets this address.
    #DNS and SIP server addresses are assigned from the common options above
        address fdde:b1a8:d98d:0000:2F87:9FBC:0A0A:0AC9
  }
}
```

Chapter 18: SIP messages supported by the IP Deskphone

SIP methods

The table below provides a list of SIP messages supported by the IP Deskphone.

Table 55: SIP methods

Method	Supported?	Comments
INVITE	Yes	Mid-call re-invites for media changes also supported.
ACK	Yes	
BYE	Yes	
CANCEL	Yes	
OPTIONS	Response only	
INFO	Yes	Optionally used for in-session DTMF signaling, and Avaya Call Server specific NAT detection
PING	Yes	Proxy detection, monitoring and Avaya Call Server specific firewall traversal
REGISTER	Yes	For user registration
REFER	Yes	For transfer
NOTIFY	Yes	
SUBSCRIBE	Yes	
PUBLISH	Yes	For VQMon Publish
PRACK	Yes	No support for PRACK-specific early-media negotiation scenarios
MESSAGE	Yes	
UPDATE	Yes	UPDATE messages received in an early dialog state require reliable provisional responses. If PRACK is disabled, or not used by a local or remote party, some UPDATE operations fail as described in RFC3311. The support of UPDATE messages is not a configurable feature.

SIP responses

The following SIP responses are also supported:

- 1xx Response—Information Responses
- 2xx Responses—Successful Responses
- 3xx Response—Request Failure Responses
- 4xx Response—Server Failure Responses
- 6xx Response—Global Responses

1xx Response—Information Responses

1xx Response	Send	Receive	Comments
100 Trying	Yes	Yes	The IP Deskphone can generate this response for an incoming INVITE if it has taken too long to generate a 180 response. Upon receiving this response, the IP Deskphone waits for a 180 Ringing, 183 Session Progress, or 200 OK responses.
180 Ringing	Yes	Yes	The IP Deskphone begins local ringing through the active transducer.
181 Call is being forwarded	No	Yes	See 183.
182 Queued	No	Yes	See 183.
183 Session progress	No	Yes	The IP Deskphone accepts a 183 response with SDP to allow for early-media negotiation.

2xx Response—Successful responses

2xx Response	Send	Receive	Comments
200 OK	Yes	Yes	
202 Accepted	Yes	Yes	

3xx Response—Redirection responses

3xx Response	Send	Receive	Comments
300 Multiple Choices	No	Yes	When receiving this response, the IP Deskphone redirects the original request to next contact specified.
301 Moved permanently	No	Yes	When receiving this response, the IP Deskphone redirects the original request to the new contact specified. However, the IP Deskphone takes no additional special consideration of the "permanent" status of this change.
302 Moved temporarily	Yes	Yes	This response is sent to an incoming invite if the IP Deskphone has local call-forwarding enabled. When receiving this response, the IP Deskphone redirects the original request to the new contact specified.
305 Use Proxy	Yes	Yes	The IP Deskphone generates these responses when receiving requests that did not come through the configured SIP proxy. When receiving this request, the IP Deskphone contacts the new address in the Contact header field.
380 Alternate service	No	Yes	When receiving this request the IP Deskphone contacts the new address in the Contact header field.

4xx Response—Request failure responses

4xx Response	Send	Receive	Comments
400 Bad request	Yes	Yes	The IP Deskphone generates a 400 Bad Request response for various failure conditions generally when a request is invalid, and a more specific error response does not apply.
401 Unauthorized	No	Yes	Receiving a 401 response results in the IP Deskphone re-issuing the request using HTTP digest authentication.
402 Payment required	No	Yes	See default handling.
403 Forbidden	No	Yes	See default handling.

Table continues…

4xx Response	Send	Receive	Comments
404 Not found	Yes	Yes	The IP Deskphone generates this response for requests to unknown users. Receiving this response falls through to the default handling.
405 Method not allowed	Yes	Yes	The IP Deskphone ends this response to a known method if it is received at a time when the IP Deskphone is not prepared to handle or the request is missing necessary information. Receiving this response falls through to the default handling.
406 Not acceptable	Yes	Yes	The IP Deskphone can send this response when receiving a REFER request which has an unsupported URI. Receiving this response falls through to the default handling.
407 Proxy authentication required	No	Yes	See 401.
408 Request timeout	No	Yes	See default handling.
410 Gone	No	Yes	See default handling.
413 Request entity too large	No	Yes	See default handling. The IP Deskphone does not automatically retry if a retry-after header is present.
414 Request---URL too long	No	Yes	See default handling.
415 Unsupported Media	Yes	Yes	The IP Deskphone can send this response when an incorrect content-type is detected for a request. Receiving this response falls through to the default handling.
420 Bad Extension	Yes	Yes	The IP Deskphone can respond with a 420 when checking required extensions of incoming requests. When receiving a 420, see default handling. The IP Deskphone does not retry the request.
480 Temporarily unavailable	No	Yes	See default handling.
481 Call leg/ transaction does not exist	Yes	Yes	Incoming requests are matched against existing dialogs. If a request appears to be in-dialog, but does not have an existing dialog, the IP Deskphone responds with a 481. For incoming 481 responses, the default handling is used.

Table continues…

4xx Response	Send	Receive	Comments
482 Loop detected	Yes	Yes	Default handling is used when this response is received.
483 Too Many Hops	No	Yes	See default handling.
484 Address Incomplete	No	Yes	See default handling.
485 Ambiguous	No	Yes	See default handling. The IP Deskphone does not attempt to retry the request.
486 Busy Here	Yes	Yes	The IP Deskphone can respond with this if the user is on the IP Deskphone, and the IP Deskphone has reached its maximum number of allowed calls and cannot present the incoming call to the user. When this message is received by the IP Deskphone an error is displayed and a busy tone is played.
487 Request Canceled	Yes	Yes	See default handling.
488 Not Acceptable	Yes	Yes	The response is used by the IP Deskphone when a failed media negotiation occurs.
491 Request Pending	Yes	Yes	The IP Deskphone sends and receive this message in GLARE conditions.

5xx Response—Server failure responses

5xx Response	Send	Receive	Comments
500 Internal Server Error	Yes	Yes	The IP Deskphone can send this response when a request is received but the IP Deskphone software is not in a correct state to handle it. When receiving this message the IP Deskphone displays an error for the user.
501 Not Implemented	No	Yes	See default handling.
502 Bad Gateway	No	Yes	See default handling.
503 Service Unavailable	Yes	Yes	
504 Gateway timeout	No	Yes	See default handling.
505 Version Not Supported	Yes	Yes	

6xx Response—Global responses

6xx Response	Send	Receive	Comments
600 Busy Everywhere	Yes	Yes	The IP Deskphone can send this response when the IGNORE setting is configured to NETWORK, and the user chooses to ignore an incoming call. When received, this response falls through the default handling.
603 Decline	Yes	Yes	The IP Deskphone can send this response when the user declines an incoming call. An optional reason can be supplied.
604 Does Not Exist Anywhere	No	Yes	See default handling.
606 Not Acceptable	No	Yes	See default handling.

Default error handling

All 4xx/5xx/6xx responses (with the exception of 401/407) received by the IP Deskphone when attempting to initiate a call result in the display of an error on the screen, and typically results in fast or regular busy tone.

If a media negotiation fails during dialog setup, the IP Deskphone terminates the dialog.

If an in-dialog failure occurs during media (re)negotiation, the IP Deskphone falls back to previously negotiated media settings. When a failure occurs that makes this impossible, the IP Deskphone attempts to clear the call by terminating the dialog.

SIP header fields

The following table contains the supported SIP headers.

Header field	Supported?
Accept	Yes
Accept-Encoding	Yes
Accept-Language	Yes
Alert-Info	Yes
Allow	Yes

Table continues…

Header field	Supported?
Allow-Events	Yes
Authentication-Info	Yes
Authorization	Yes
Call-Id	Yes
Call-Info	Yes
Contact	Yes
Content-Disposition	Yes
Content-Encoding	Yes
Content-Length	Yes
Content-Type	Yes
Cseq	Yes
Date	Yes
Expires	Yes
Error-Info	Yes
Max-Forwards	Yes
Mime-Version	Yes
Organization	Yes
P-Access-Network-Info	Yes
P-Asserted-Identity	Yes
P-Associated-URI	Yes
P-Called-Party-ID	Yes
P-Charging-Function-Addresses	Yes
P-Charging-Vector	Yes
P-Media-Authorization	Yes
P-Preferred-Identity	Yes
P-Visited-Network-ID	Yes
Path	Yes
Priority	Yes
Privacy	Yes
Proxy-Authenticate	Yes
Proxy-Require	Yes
RAck	Yes
Reason	Yes
Record-Route	Yes
Refer-To	Yes

Table continues…

Header field	Supported?
Referred-By	Yes
Remote-Party-ID	Yes
Replaces	Yes
Reply-To	Yes
Require	Yes
Resource-Priority	Yes
Retry-After	Yes
Route	Yes
RSeq	Yes
Server	Yes
Service-Route	Yes
Subject	Yes
Supported	Yes
Timestamp	Yes
To	Yes
Unsupported	Yes
User-Agent	Yes
Via	Yes
Warning	Yes
WWW-Authenticate	Yes

Session description protocol usage

SDP Headers	Supported?
v--Protocol version	Yes
o--Owner or creator and session identifier	Yes
s--Session name	Yes
t--Time description	Yes
c--Connection information	Yes
m--Media name and transport address	Yes
a--Media attribute lines	Yes

SDP and Call Hold

The IP Deskphone can support sending and receiving of hold using the method specified by RFC2543 and RFC3261/3264.

Transport layer protocols

Protocol	Supported?
Unicast UDP	Yes
Multicast UDP	No
TCP	No

SIP security authentication

Authentication	Supported?	Comments
Digest Authentication	Yes	
Proxy-to-User Authentication	Yes	
User-to-User Authentication	No	The IP Deskphone responds to a 401, but never challenges incoming requests with a 401 response.
S/MIME	No	
AKA	No	

SIP DTMF Digit transport

Transport type	Supported?
RFC2833	Yes
In-band tones	Yes
Out-of-band tones	Yes (vnd.avaya.digits)

Supported subscriptions

Subscription type	Supported	Avaya Call Server specific
address-book	Yes	Yes
call-park	Yes	Yes
dialog	Yes	Yes
presence	Yes	Yes
message-summary	Yes	No
ua-profile	Partial	Yes
service-package	Yes	Yes
network-redirection-reminder	Yes	Yes

Supported instant messaging

Message type	Supported?
plain text	Yes
Avaya unencrypted	Yes
Avaya encrypted	Yes

Chapter 19: Diagnostics and troubleshooting

This chapter contains the following topics:

IP Deskphone diagnostics

Network-related issues can be debugged using the Network Diagnostic Utility (NDU) built into the IP Deskphone.

Another way to diagnose a problem on an IP Deskphone is to capture a message trace using any appropriate software.

The IP Deskphone has Problem Determination Tools (PDT). These can be accessed through a SSH session using the IP address of the IP Deskphone (you can configure the login and password using provisioning or manually in the network configuration window of the IP Deskphone).

Server unreachable after the IP Deskphone is powered up

If the display indicates that the server is unreachable and it continuously resets, some parameters must be configured. Things to consider when configuring parameters:

- Enter requested information in the menu fields by pressing the number keys on the dialpad. Press the asterisk (*) key to enter a period (.) when entering an IP address.
- To record the entry and advance the initialization to the next parameter, press **OK**.
- To abandon the manual configuration process and restart the power-up, press **Cancel**.
- To manually enter parameters, use the **BKSpace** or **Clear** context-sensitive soft keys to edit the default entry. **BKSpace** deletes each character as the key is pressed. **Clear** deletes the entire entry.
- Each parameter must have a corresponding entry.

Software download failure

If you are having trouble downloading software, review the following.

- Are the **Server URL** and **Protocol** parameters correct in the **Device Settings > Provisioning** dialog on the IP Deskphone?
- Is the IP Deskphone connecting to the TFTP server log?

  Check any firewall configuration settings to allow TFTP protocol access.
- Is the syntax within the 11xxe.cfg or 11xxeSIP.cfg correct? See Creating the provisioning files on page 45. Supported sections describe the syntax of the configuration file.
- Does DOWNLOAD_MODE = AUTO and is VERSION less than the current running software version? If a file does not download using the AUTO selection, it is possible the version number is not high enough. A version number exists permanently on the IP Deskphone until a higher version number is downloaded through the device configuration file or you can select **Services > File Manager** on the IP Deskphone.
- Check FILENAME. Does this exist on the TFTP server?
- Check to make sure your firewall settings allow for the provisioning protocol (TFTP, FTP, HTTP, or HTTPS) to go through.

There is a chance of software download failure, leaving the IP Deskphone with no valid application code and only the boot loaders. If this happens, the boot loaders execute and handle the application download.

Software conversion failures

There are four different boot loaders in the FLASH and application load. Various boot loaders are used to recover the IP Deskphone if a failure occurs.

- If a conversion fails before anything is written to FLASH, the IP Deskphone reboots with the previous software load.

- If the software download fails while the application is being written to FLASH, there are two possible recovery methods:
  - If an application file was not created, then after power-up the IP Deskphone jumps to the BootC loader and downloads a new application load using the same mechanism as the application.
  - If the application is executed and the file created is corrupted, the IP Deskphone crashes. In this case, force the IP Deskphone to use BootC by pressing the **UP** key and **2** during power up.

Users of the IP Deskphone complain that their banner is not updated with their custom banner

When the banner is configured as FORCED in the device configuration file, the user's banner is overwritten by the value in the device configuration file.

Provisioning Error is displayed on the IP Deskphone display

The Provisioning Error is displayed on the screen when the IP Deskphone is unable to contact the Provisioning, FTP, HTTP, or HTTPS server.

Local diagnostic tools

Local diagnostic tools provides information about the Avaya 1100 Series IP Deskphone, such as identification, software version, settings, and a set of testing routines for checking network condition.

You can access Diagnostics tools through the **Diagnostics** menu.

The following table describes the Diagnostics menu options.

Table 56: Diagnostics menu options

Diagnostics option	Description
IP Deskphone and DHCP information	Provides detailed information about the IP Deskphone and service configuration.
Network Diagnostics Tools	Provides access to the following testing routines: • ping • tracert
Ethernet Statistics	Provides some Ethernet statistics for Network Interface and PC port.
IP Network Statistics	Provides IP Network statistics.
USB Devices	Provides information about USB devices attached to the IP Deskphone .
Certificates Administration	Supports administration of available certificates.

Table continues…

Diagnostics option	Description
Advanced Diag Tools	Provides information for setting up the following configuration parameters: • Auto Recovery (enable/disable) • SSH (enable/disable) • Port Mirroring (enable/disable) • Debug Port • User ID and Password for SSH
Test Key	Activates key testing mode.

How to access the Diagnostics menu

To activate the Diagnostics menu, access the **Network** menu by selecting one of the following steps:

- Press the **Globe** key twice on the IP Deskphone while the IP Deskphone is in the idle mode.
- Press the **Prefs** context-sensitive soft key, and then select the **Network** item in the **Preferences** menu.

The following screen appears:

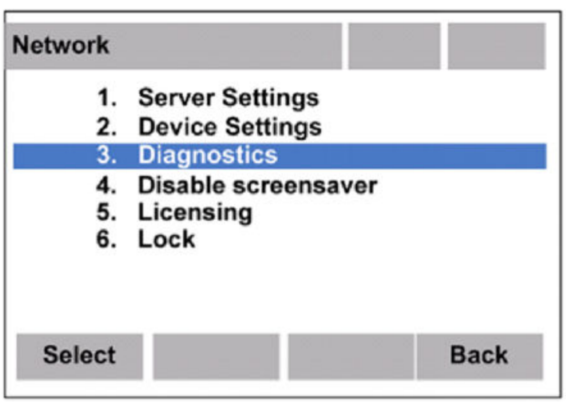


Figure 73: Network menu screen

After you access the Network menu, the following options are available:

- 1. Server Settings
- 2. Device Settings
- 3. Diagnostics
- 4. Disable screensaver
- 5. Licensing

- 6. Lock

Select **Diagnostics**, or press **Back** to return to the **Network** menu.

The following screen appears:

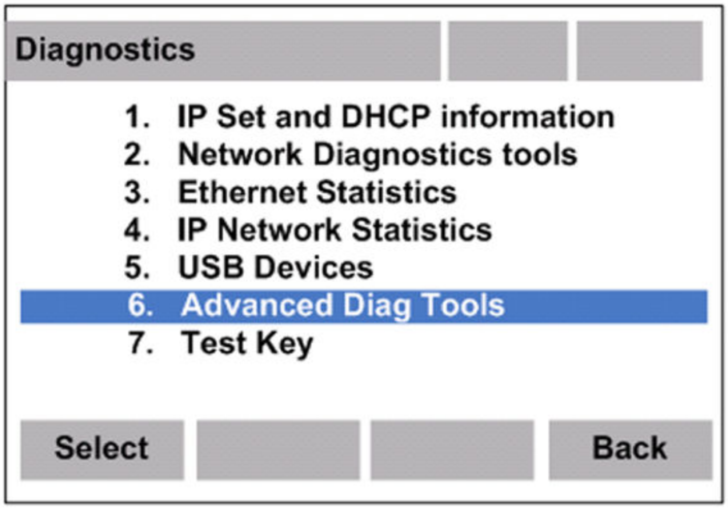


Figure 74: Diagnostics menu screen

The following table describes the function of the Navigation keys for the Diagnostics screen.

Table 57: Navigation

Key	Action
Up and down arrows	Use the up and down arrows to change the selected item in the list.
Enter	Invokes the Select context-sensitive soft key.
Digital keys (number associated with option)	Invokes an appropriate option.
*	Selects the first option Server Settings, but does not activate it.
#	Selects the last option Lock, but does not activate it.

IP Set and DHCP information

The **IP Set and DHCP Information** screen provides detailed information about the IP Deskphone, such as configuration, software version, IP addresses, gateway, and servers. To access the **IP Set and DHCP Information** screen, from the **Diagnostics** menu, choose **IP Set and DHCP information**.

The following screen appears:

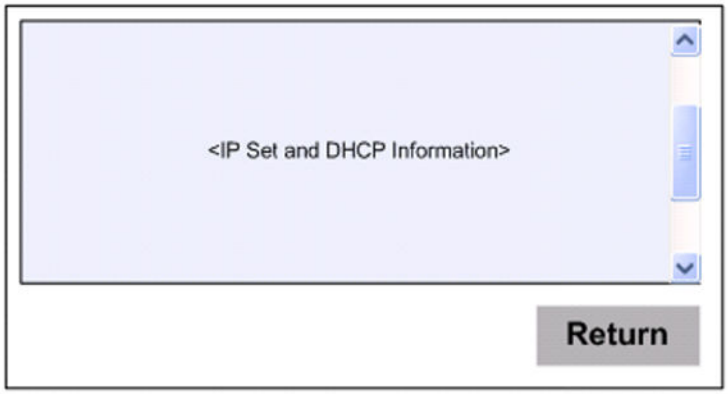


Figure 75: IP Set and DHCP information screen

The following is an example of the information that appears:

1. `Configuration Network Data Valid: Yes`

   `MAC Address Stored: Yes`

   `Perform DHCP: No`

   `Voice VLAN Enable: No`

   `Voice VLAN Config: No`

   `VLAN Voice VLAN Discovered: No`

   `Primary Server: S1`

   `PC Port is: ON`
2. `Software Version: 3.00.09.02 Hardware ID: xxxxxx`
3. `Set IP: xxx.xxx.xxx.xxx (could be in IPv4 or IPv6 format)`
4. `Sub-Mask: xxx.xxx.xxx.xxx (could be in IPv4 or IPv6 format)`
5. `GateWay: xxx.xxx.xxx.xxx (could be in IPv4 or IPv6 format)`
6. `Voice VLAN Priority: 6`
7. `Voice VLAN ID: 6`
8. `DHCP Respond String: ....`
9. `Servers' Information:`

   `S01 IP: xxx.xxx.xxx.xxx`

   `Port: 4100 Act: 1 Retries: 5`

   `S02 IP: xxx.xxx.xxx.xxx`

   `Port: 4100 Act: 1 Retries: 5`

   `S03: IP: xxx.xxx.xxx.xxx`

   `Port: 4100 Act: 1 Retries: 5`

   `S04 IP: xxx.xxx.xxx.xxx`

`Port: 4100 Act: 1 Retries: 5`

10. `Provisioning Server: xxx.xxx.xxx.xxx`

The following table describes the function of the context-sensitive soft keys for the **IP Set and DHCP Information** screen.

Table 58: Context-sensitive soft key for the IP Set and DHCP Information screen

Context-sensitive soft key	Action
Up and down arrows	Use the up and down arrows to scroll the screen.

The following table describes the function of the navigation key for the **IP Set and DHCP Information** screen.

Table 59: Navigation

Key	Action
Return	Press the Return context-sensitive soft key to cancel this screen and return to the Diagnostics menu.

Duplicate IPv6 addresses from DHCPv6 server

If an IP Deskphone receives a duplicate IPv6 address from the DHCPv6 server, the IP Deskphone displays

`Duplicated IPv6 Address`

on the phone screen.

After a 10–second timeout, the IP Deskphone displays

`Starting DHCPv6`

on the phone screen and a DECLINE message is sent back to the DHCPv6 server to inform the DHCPv6 server that this address should not be assigned.

If the DHCPv6 server sends a REPLY message in answer to DECLINE, the IP Deskphone removes the duplicated IP address from the list of IPv6 addresses, resources associated with duplicate address are freed, and the DHCP process restarts.

If no REPLY message is received, the IP Deskphone makes four more attempts to contact the DHCPv6 server. If unsuccessful, the IP Deskphone removes the duplicated IP address from the list of IPv6 addresses, resources associated with duplicate address are freed, and the DHCP process restarts.

DHCP server unreachable

This section describes the IP Deskphone behavior when the DHCPv4/DHCPv6 server is unreachable.

If the DHCPv4/DHCPv6 server is unreachable due to the following scenarios:

- IP Deskphone starts and cannot get IPv4 address from DHCPv4 server (cached IP is disabled)
- IP Deskphone starts and cannot get IPv6 address from DHCPv6 server (cached IP is disabled)
- IPv4 address lease expires (cached IP is disabled)
- IPv6 address becomes deprecated and there are no active calls (cached IP is disabled)
- IPv6 address lease expires (cached IP is disabled)

then the following message is displayed on the IP Deskphone display screen:

`DHCP server unreachable. Trying to contact...`

Note:

If the IPv6 address becomes deprecated and there is an active call, the message is displayed on the IP Deskphone display screen after the active call is released.

When this message is displayed, the user can:

- wait until the IP Deskphone receives the required IP address from DHCP
- open the **Device Settings** menu (by double-pressing the **Services** key) and try to re-configure the IP Deskphone

The message window closes automatically when the IP Deskphone receives a new valid IPv4/IPv6 address.

Network Diagnostics tools

The Network Diagnostics Tools menu provides access to ping and tracert testing routines. To access the Network Diagnostics Tools screen, from the Diagnostics menu, choose **Network Diagnostics Tools**.

The following screen appears:

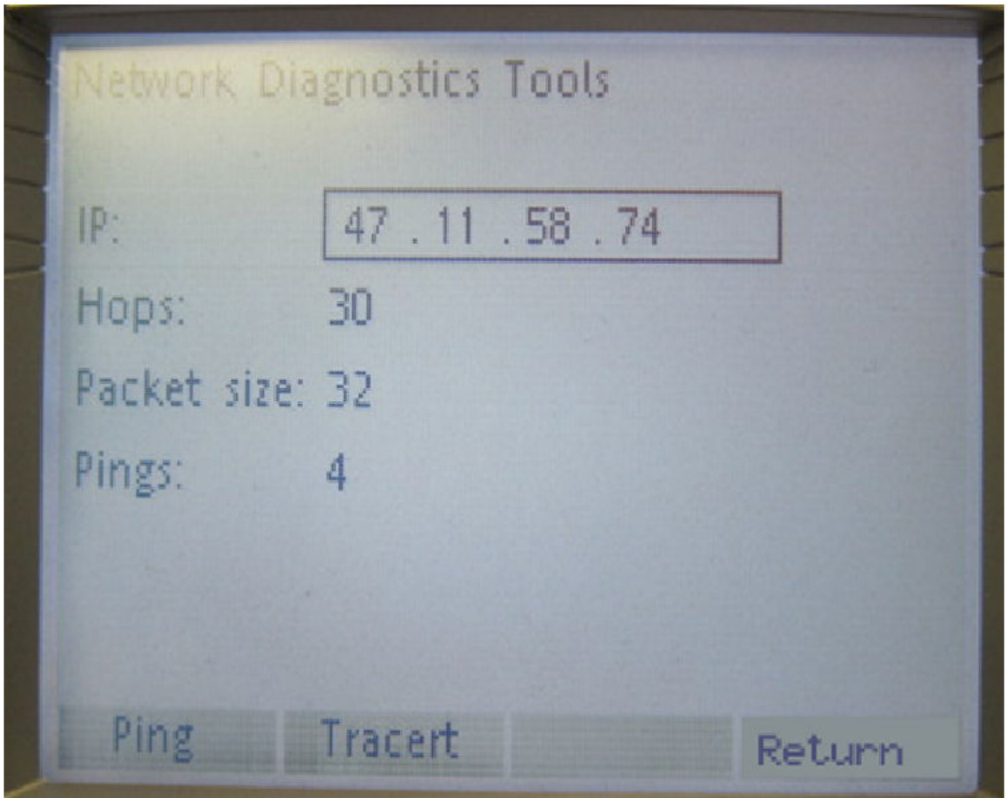


Figure 76: Network Diagnostics Tools screen

The screen contains the following configurable fields:

- IP—The user can enter an IP address.
- Hops—The number of hops used as a configurable parameter for tracert routine.
- Packet Size—Size of the network packet used by the ping routine.
- Ping—The number of ping packages.

The following services are available:

- activate the ping routine
- activate the tracert routine

The following table describes the function of the context-sensitive soft keys for the Network Diagnostics tools screen.

Table 60: Context-sensitive soft keys for the Network Diagnostics Tools screen

Context-sensitive soft key	Action
Ping	Activates the ping routine.
Tracert	Activates the tracert routine.
Cancel	Returns you to the Diagnostics menu.

The following table describes the function of the Navigation keys for the Network Diagnostics Tools screen.

Table 61: Navigation

Key	Action
Up and down arrows	Use the up and down arrows to scroll through a list of testing information.
Left and right arrows	Use the left and right arrows to move through the configurable fields.
Enter	Use the Enter key to enter the editing mode for the active configurable field.

Config option in Network Diagnostics tools

The Config screen provides access to additional configurable parameters used by testing routines. You can access the screen by pressing the **Config** context-sensitive soft key on the IP Deskphone after the Network Diagnostics tools screen is active.

The following screen appears:

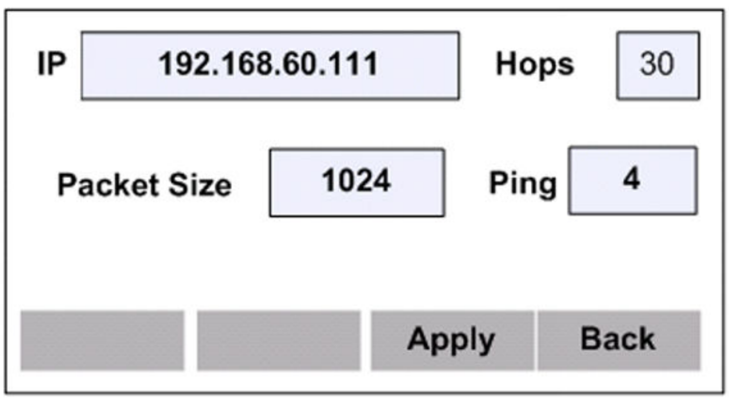


Figure 77: Network Diagnostics tools (Config) screen

The screen contains the following configurable fields:

1. IP—The user can enter an IP address.
2. Hops—The number of hops used as a configurable parameter for tracert routine.
3. Packet Size—Size of the network packet used by the ping routine.
4. Ping—The number of ping packages.

The following table describes the function of the context-sensitive soft keys for the Network Diagnostics tools (Config) screen.

Table 62: Context-sensitive soft keys for the Network Diagnostics (Config) screen

Context-sensitive soft key	Action
Apply	Applies settings, dismisses the screen, and returns you to the Network Diagnostics menu.
Back	Returns you to the Diagnostics menu.

The following table describes the function of the Navigation keys for the Network Diagnostics tools (Config) screen.

Table 63: Navigation

Key	Action
Left and right arrows	Use the left and right arrows to move through the configurable fields.
Enter	Use the Enter key to enter the editing mode for the active configurable field

Ethernet Statistics

The **Ethernet Statistics (NI Port)** screen displays ethernet statistics information for Network Interface (NI) or PC ports, such as the number of incoming and outgoing network packages and network settings.

To access the **Ethernet Statistics (NI Port)** screen from the Diagnostics menu, choose **Ethernet Statistics**.

The following screen appears:

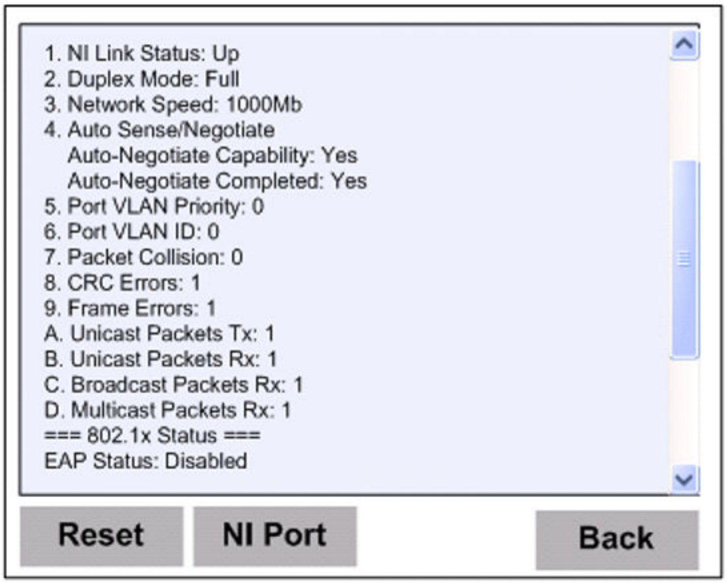


Figure 78: Ethernet Statistics (NI Port) screen

The following is an example of Ethernet Statistics for the IP Deskphone:

```
1. NI Link Status: Up
2. Duplex Mode: Full
3. Network Speed: 1000Mb
4. Auto Sense/Negotiate
Auto-Negotiate Capability: Yes
Auto-Negotiate Completed: Yes
5. Port VLAN Priority: 0
6. Port VLAN ID: 0
7. Packet Collision: 0
8. CRC Errors: 1
9. Frame Errors: 1
A. Unicast Packets Tx: 1
B. Unicast Packets Rx: 1
C. Broadcast Packets Rx: 1
D. Multicast Packets Rx: 1
=== 802.1x Status ===
EAP Status: Disabled
```

The following table describes the function of the context-sensitive soft keys for the **Ethernet Statistics (NI Port)** screen.

Table 64: Context-sensitive soft keys for the Ethernet Statistics (NI Port) screen

Context-sensitive soft key	Action
Reset	Resets statistics value.
NI Port	Switches to the PC Port Ethernet statistics.
Back	Returns you to the Diagnostics menu.

The following table describes the function of the Navigation keys for the **Ethernet Statistics (NI Port)** screen.

Table 65: Navigation

Key	Action
Up and down arrows	Use the up and down arrows to scroll through a list of statistics information.

Ethernet Statistics (PC Port) screen

The **Ethernet Statistics (PC Port)** screen displays Ethernet statistics for the PC port. To access the PC Port from the **Ethernet Statistics** screen, press the **NI Port** context-sensitive soft key.

The following screen appears:

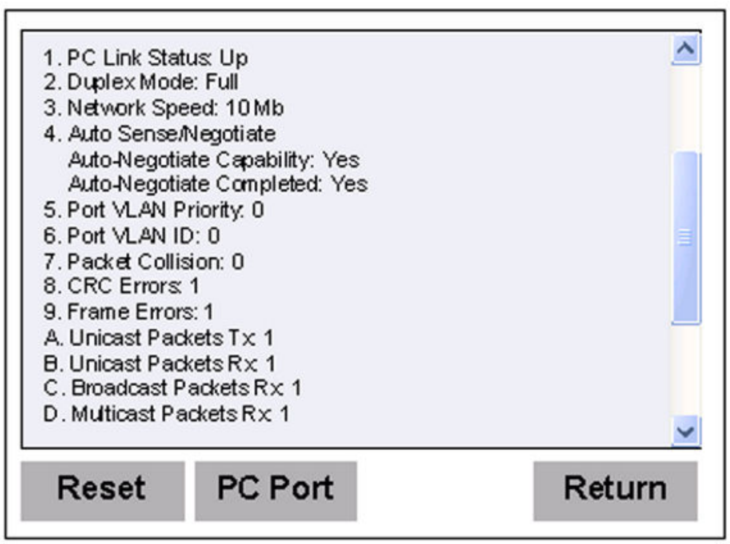


Figure 79: Ethernet Statistics (PC Port) screen

The following is an example of Ethernet Statistics for the PC Port:

```
1. PC Link Status: Up
2. Duplex Mode: Full
3. Network Speed: 10 Mb
```

```
4. Auto Sense/Negotiate
Auto-Negotiate Capability: Yes
Auto-Negotiate Completed: Yes
5. Port VLAN Priority: 0
6. Port VLAN ID: 0
7. Packet Collision: 0
8. CRC Errors: 1
9. Frame Errors: 1
A. Unicast Packets Tx: 1
B. Unicast Packets Rx: 1
C. Broadcast Packets Rx: 1
C. Broadcast Packets Rx: 1
D. Multicast Packets Rx: 1
```

The following table describes the function of the context-sensitive soft keys for the **Ethernet Statistics (PC Port)** screen.

Table 66: Context-sensitive soft keys for the Ethernet Statistics (PC Port) screen

Context-sensitive soft key	Action
Reset	Resets statistics values.
PC Port	Switches to the NI Port Ethernet statistics.
Back	Returns you to the Diagnostics menu.

The following table describes the function of the Navigation keys for the**Ethernet Statistics (PC Port)** screen.

Table 67: Navigation

Key	Action
Up and down arrows	Use the up and down arrows to scroll through a list of statistics information.

IP Network Statistics

The **IP Network Statistics** screen provides information such as the number of incoming and outgoing network packages, number of error packages, and protocols. To access the **IP Network Statistics** screen from the **Diagnostics** menu, choose **IP Network Statistics**.

The following screen appears:

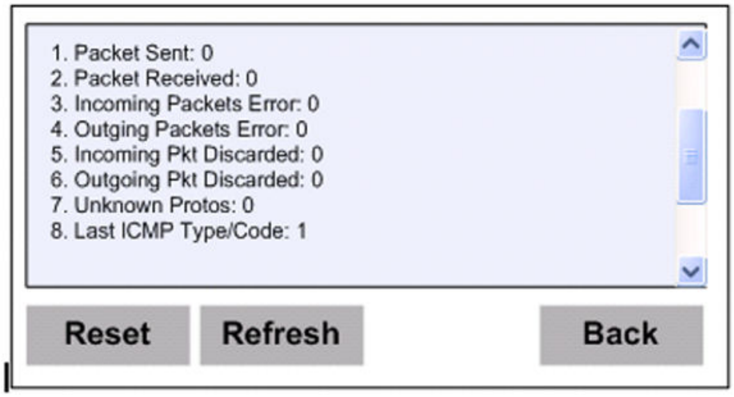


Figure 80: IP Network Statistics screen

The following is an example of IP Network Statistics for the IP Deskphone:

```
1. Packet Sent: 0
2. Packet Received: 0
3. Incoming Packets Error: 0
4. Outgoing Packets Error: 0
5. Incoming Pkt Discarded: 0
6. Outgoing Pkt Discarded: 0
7. Unknown Protos: 0
8. Last ICMP Type/Code: 1
```

The following table describes the function of the context-sensitive soft keys for the **IP Network Statistics** screen.

Table 68: Context-sensitive soft keys for the IP Network Statistics screen

Context-sensitive soft key	Action
Reset	Resets statistics values.
Refresh	Refreshes the IP Network statistics.
Back	Returns to the Diagnostics menu.

The following table describes the function of the Navigation keys for the **IP Network Statistics** screen.

Table 69: Navigation

Key	Action
Up and down arrows	Use the up and down arrows to scroll through a list of statistics information.

USB Devices

The USB Devices screen provides information about USB devices attached to the IP Deskphone. To access the USB Devices screen, from the Diagnostics menu, choose **USB Devices**.

The following screen appears:

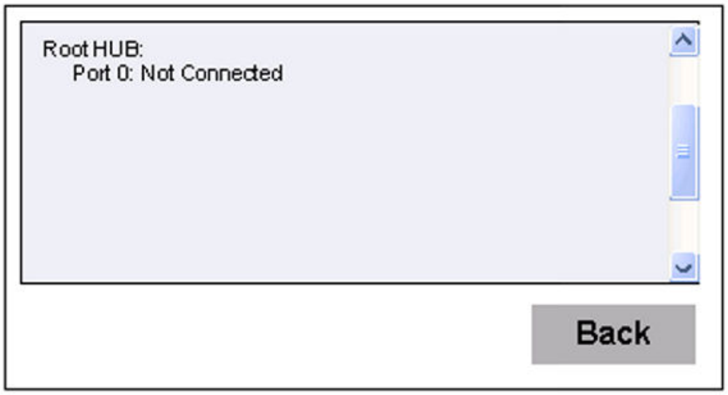


Figure 81: USB Devices screen

Important:

The USB Devices screen contains a list of the USB devices attached to the IP Deskphone.

The following table describes the function of the context-sensitive soft keys for the USB Devices screen.

Table 70: Context-sensitive soft keys for the USB Devices screen

Context-sensitive soft key	Action
Back	Returns you to the Diagnostics menu.

The following table describes the function of the Navigation keys for the USB Devices screen.

Table 71: Navigation

Key	Action
Up and down arrows	Use the up and down arrows to scroll through a list of statistics information.

Advanced Diag Tools

With the Advanced Diag Tools option, you can modify the following parameters:

- Auto Recovery
- Port Mirroring

- Debug Port

To access the **Advanced Diag Tools** screen from the **Diagnostics** menu, choose **Advanced Diag Tools**.

The following table describes the function of the context-sensitive soft keys for the **Advanced Diag Tools** screen.

Table 72: Context-sensitive soft keys for the Advanced Diag Tools screen

Context-sensitive soft key	Action
Apply	Invokes the selected service.
Return	Dismisses the dialog box and returns you to the Diagnostics menu.

The following table describes the function of the Navigation keys for the **Advanced Diag Tools** screen.

Table 73: Navigation

Key	Action
Up and down arrows	Use the up and down arrows to scroll through a list of statistics information.
Enter	Use the Enter key to enter the editing mode for the active configurable field or change the value for check boxes.

Port Mirroring

The ability to use Port Mirroring depends on the device configuration parameter defined in the device configuration file. The following device configuration file parameter manages the PC Port Mirroring option:

PORT_MIRROR_ENABLE [YES | No]

This parameter determines whether or not the Port Mirror option can be managed:

- If PORT_MIRROR_ENABLE is **Yes**, then you can activate or deactivate the Port Mirror option on the IP Deskphone. The Port Mirroring prompt in the **Network >Diagnostics >Advanced Diag Tools** menu is enabled and can be modified.
- If PORT_MIRROR_ENABLE is **No**, then you cannot manage the Port Mirror option on the IP Deskphone. The Port Mirroring prompt in the Advanced Diag Tools menu is disabled (dimmed); Port Mirroring is disabled.

The default value for PORT_MIRROR_ENABLE is NO. This means that Port Mirroring is disabled and cannot be enabled.

Gathering network traces from an IP Deskphone

You can capture network traces from the PC port of the IP Deskphone.

1. Ensure the PC port is enabled on the IP Deskphone.

   Open the **Device Settings** menu. Check to see if the **Enable PC Port** parameter checkbox is displayed and the checkbox is checked. If the **Enable PC Port** parameter checkbox is not visible, do the following:

   - Press the **Auto** soft key and check the **07. PC Port Enable** checkbox in the **Auto Provisioning** window.
   - Press the **Config** soft key to return to the **Network Settings** window.
   - Check the **PC Port** checkbox.
2. Ensure the Port Mirroring feature is enabled through provisioning.
3. Enable port mirroring on the IP Deskphone by pressing the **Services** key twice and opening **Local Tools** > **Network** > **3. Diagnostics** > **6. Advanced Diag Tools**. Select the **Port Mirroring** check box.

   Note:

   If the check box is dimmed and cannot be selected, this means that Port Mirroring was not enabled in the provisioning file.
4. Open the **Services > 4. Check for Updates** menu. Press the **YES** soft key to update the IP Deskphone configuration.
5. Connect your PC to the IP Deskphone PC port.

Debug Port

Foe information about the **Debug Port** option in the **Advanced Diag Tools** menu, see Debug port security. on page 266

Test key

The Test key screen lets you perform a physical key operation test. After you activate the test mode, the `Test key: Press any key` prompt appears on the screen. The IP Deskphone goes into the Do Not Disturb (DND) mode and cannot receive any external calls. Information about the pressed key event (except for the Rls key) appears on the IP Deskphone screen. To access the Test key screen from the Diagnostics menu, choose **Test key**.

The following screen appears:

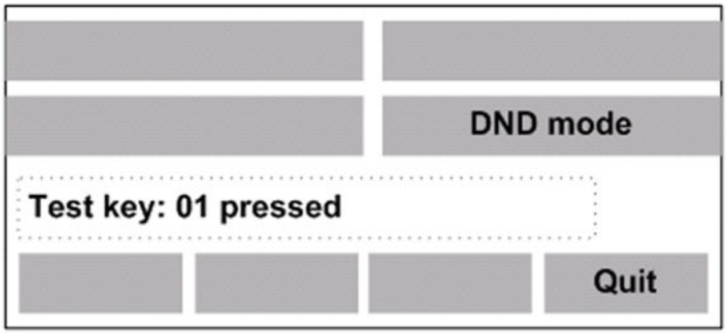


Figure 82: Test key screen

After you activate the test mode, the key event appears on the screen:

- `Key pressing: "Test key: xx pressed"`
- `Key pressing: "Test key: xx pressed"`

The following table describes the function of the context-sensitive soft keys for the Test key screen.

Table 74: Context-sensitive soft keys for the Test key screen

Context-sensitive soft key	Action
Quit	Dismisses the Services menu.

The following table describes the function of the Navigation key for the Test key screen.

Table 75: Navigation

Key	Action
Rls	Closes the test mode and restarts the IP Deskphone.

Reset Factory Settings support

A configured IP Deskphone can be reset to factory defaults to clear all stored information and preference data. By activating this mode, the data stored on the IP Deskphone is erased, and the administrator can reconfigure it for a new user.

The IP Deskphone resets data stored in the EEPROM to factory defaults and erases files in TFFS.

There are two ways to activate Reset to Factory Settings:

1. by entering a Special Key Sequence (SKS), or
2. remotely using SSH-PDT.

Activating Reset to Factory Settings does not affect files stored in the USB flash drive.

After you activate Reset to Factory Settings the action is registered in the ECR-log file.

Activating Reset to Factory Setting by SKS

1. At any point while the IP Deskphone is operating, press the Special Key Sequence (SKS).
2. Enter the following command:

   `**73639<MAC>## (or **renew<MAC>##)`

   For example, the MAC-address, `A1B2C3D4E5F6` can be translated to `212223343536` . Therefore, the SKS would be `**73639212223343536##` .

   After the proper sequence is entered on the IP Deskphone, the confirmation screen appears.
3. Press the **Yes** context-sensitive soft key to reset to factory setting.

   Or

   Press the **No** context-sensitive soft key to close the confirmation screen and return to regular mode.

The following table describes the function of the context-sensitive soft keys for Reset to Factory Setting.

Table 76: Context-sensitive soft keys for Reset to Factory Setting

Context-sensitive soft key	Action
Yes	Activates Reset to Factory Setting.
No	Rejects Reset to Factory Setting, closes the confirmation screen and returns to regular mode.

Activating Reset to Factory Setting using SSH_PDT

1. Enter the PDT-command:

   `>reset2factory`

   The PDT displays the prompt:

   `>Reset to Default setting ... Are you sure?`
2. Enter **Y** to accept.

   Or

   Enter **N** to decline.

   If you select Y, the PDT displays the prompt:

   `>Enter MAC-address:`
3. Type in the IP Deskphone MAC-address.

   `><MAC><enter>`

   For example, if the IP Deskphone MAC-address is `A1B2C3D4E5F6` , you enter:

   `>A1B2C3D4E5F6<enter>`

4. Click **Enter**.
   - If the MAC-address is correct, the IP Deskphone is reset and the remote telnet client is restarted.
   - If the MAC-address is incorrect, the IP Deskphone displays:

     ```
     >Incorrect MAC-address. Action is rejected .
     ```

     Return to Step 1.

Logging System

Logging System contains a subsystem for logging incoming and outgoing SIP packages to the log file in FFS, for the IP Deskphone. You can enable or disable the SIP logging subsystem by selecting the check box for ON (enable) or deselecting the check box for OFF (disable). To access the Logging System menu, press the **Globe** key on the IP Deskphone, and then choose **Logging System** from the Services menu.

The following screen appears:

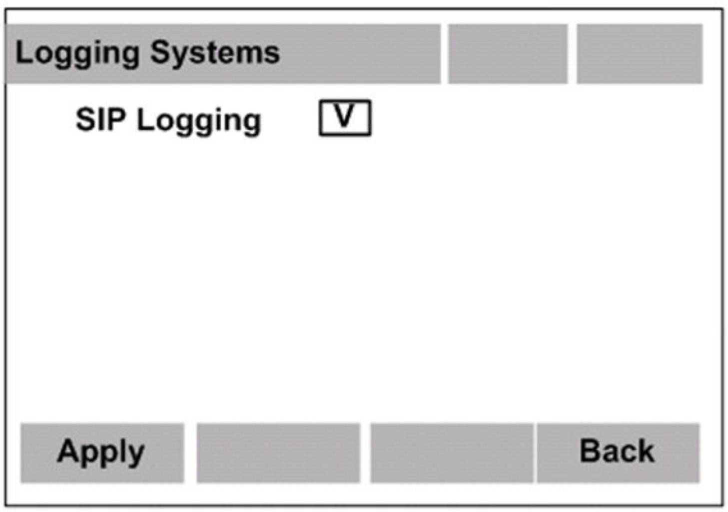


Figure 83: Logging Systems screen

The Logging Systems screen displays the SIP Logging subsystem. Press the **Enter** key in the Navigation key cluster to switch the value of the selected sign from ON to OFF, or OFF to ON. Then press the **Apply** context-sensitive soft key to apply the settings.

The following table describes the function of the context-sensitive soft keys for the Logging Systems screen.

Table 77: Context-sensitive soft keys for the Logging Systems screen

Context-sensitive soft key	Action
Apply	Applies the setting and returns to the parent screen.
Back	Dismisses the setting and returns you to the parent screen.

The following table describes the function of the Navigation keys for the Logging Systems screen.

Table 78: Navigation

Key	Action
Up and down arrows	Use the up and down arrows to scroll the screen.
Right and left arrows	Navigates through the signs.
Enter	Switches the value of the selected sign from ON to OFF, and OFF to ON.

You can enable or disable SIP-logging using the following command in the Device configuration file:

LOGSIP_ENABLE [Yes | No]

If the parameter is Yes, the SIP-logging Manager is active and starts logging SIP incoming and outgoing packages into the log file in FFS. If the parameter is No, the SIP-logging Manager is not active and there is no logging of incoming and outgoing packages into the log file in FFS. The default parameter is No.

Problem Determination Tool (PDT)

The IP Deskphone with SIP Software contains special services that monitor the performance and various other states of the IP Deskphone. These services also automatically collect problem data, and provide symptom analysis support for the various categories of problems encountered by the software. All significant events are registered in special log files.

Error Logging framework

The Error logging framework saves error-related information in the ECR Log file and is the base object used by all the other monitoring services listed as follows:

- ECR Watchdog
- Task Monitor
- CPU Load Monitor
- Stack Overflow Monitor
- Traffic Monitor

ECR Watchdog

The ECR Watchdog tracks the IP Deskphone to ensure the IP Deskphone survives transitions (for example: soft reset). If the watchdog is active and has not detected activity in a certain period of time, the watchdog logs the appropriate error and recovers the IP Deskphone.

Task Monitor

The Task Monitor performs the following functions:

- Tracks the switch of any task to the suspended state. If the task gets to the suspended state, the Task Monitor logs the error-related information (including the suspended task information and summary information about all running tasks), and then initiates recovery of the IP Deskphone.
- Monitors important tasks. The Task Monitor scans these tasks, and if any task is lost without a reason, the Task Monitor logs the error and recovers the IP Deskphone.

CPU Load Monitor

The CPU Load Monitor tracks the CPU usage. If the CPU load reaches 100 percent and stays at that level for more than 1 minute, The CPU Load Monitor logs the appropriate error (including the list of most suspect tasks that could occupy the CPU), and recovers the IP Deskphone.

Stack Overflow Monitor

The Stack Overflow Monitor tracks the stack of all tasks in the real-time mode, detects the stack overflow or corruption, and logs the task trace.

Traffic Monitor

The Traffic Monitor monitors incoming and outgoing IP and SIP traffic and registers events in the ECR-log file when the traffic exceeds predefined thresholds. The Traffic Monitor also registers the content of the incoming and outgoing SIP packages.

PDT commands

The PDT is a troubleshooting tool for the IP Deskphone. The PDT has powerful functions which allow you to perform special testing actions, and can display the content of any log files. The PDT helps to identify the origin of the problem under investigation, reduces the amount of time it takes to reproduce a problem with the proper RAS tracing levels set (trace levels are set automatically by the tool), and reduces the effort required to send the appropriate log information to technical support.

The PDT provides remote access to the IP Deskphone with the problem, using a SSH session. Access is restricted by admin ID and password.

Steps to enable SSH on an IP Deskphone manually:

1. Open **Device Settings** dialog.
2. Check **Enable SSH** checkbox if it is visible. If it is invisible, do the following:
    - Press **Auto** soft key and uncheck the **18. SSH Enable** checkbox in the **Auto Provisioning** window.
    - Press the **Config** soft key to return to the **Network Settings** window.
    - Check the **Enable SSH** checkbox.
3. Enter **UserID** and **Password**.
4. Press the **Apply** soft key.
5. Connect to the IP Deskphone by using any SSH client program.

Steps to enable SSH on an IP Deskphone through provisioning:

1. Open the **Device Settings** dialog.
2. Check the **Enable SSH** checkbox if it is visible. If it is invisible, do the following:
    - Press the **Auto** soft key and check the **18. SSH Enable** checkbox in the **Auto Provisioning** window.
    - Press the **Config** soft key to return to the **Network Settings** window.
    - Check the **Enable SSH** checkbox.
3. Add the following parameters to the IP Deskphone device configuration file SSH YES.

    SSHID <user name>

    SSHPWD <user password>
4. Open **Services/4**. Check for the Update dialog and update the IP Deskphone configuration.
5. Connect to the IP Deskphone by using any SSH client program.

The PDT supports the following set of commands:

Table 79: List of PDT commands

Command	Description
prtlog >prtlog<mngr_dest>	• Prints a content of the ECR-log file.

Table continues…

Command	Description
	• Outputs content of the specified log file to stdout (the screen, a stream, stdout, or a string). The input parameter specifies a type of logging manager: - 0 (default)—ECR-log file - 1—SIP-log file If the input parameter is incorrect, the following notification appears: >prtlog: incorrect type of manager <x>
clearLogFile	Clears a content of the ECR-log file
setLogLevel <loglevel>	Configures log level, where the loglevel is in the range 0...3: • If loglevel == 0—logging disabled • If loglevel == 1—logging only Critical errors • If loglevel == 2—logging Critical and Major errors • If loglevel >=3—logging any type of errors
printLogLevel	Print log level
setRecoveryLevel <reclevel>	Sets up recovery level, where the reclevel is in the range 0...3. If the Auto Recovery option is ON, the IP Deskphone behaves as follows: • If reclevel == 0—recovering disabled • If reclevel == 1—recovering on only Critical errors • If reclevel == 2—recovering on Critical and Major errors • If reclevel >= 3—recovering on any errors
printRecoveryLevel	Prints recovery level
taskMonShow	Prints a list of monitored tasks
I	Prints all task information
ti <taskName | task id>	Print task information
memshow [level]	Show memory information
checkStack <taskName | task id>	Check stack of some task
tt <taskName | task id>	Print Task Trace
info	Print HardwareID, SoftwareID, MAC and BT address
prtcfg	Prints content of the IP Deskphone configuration file, SystemConfig.dat in FFS. The file contains IP Deskphone-specific configuration. The content of this file is formed from the content of several downloadable configuration files: • Device Configuration file • Tones file

Table continues…

Command	Description
	• Language file
lsr	List directory contents (similar to unix ls) and the contents of a directory and any of its subdirectories
ping <host ip> [# of pings]	Ping any host (ping)
tracert <host ip> [max hops]	Traceroute to any host (tracert)
netinfo	Print common network information
routeshow	Display host and network routing tables and stats
arp	Display entries in the system ARP table
listcerts	List all trusted certificates
printcert <index>	Display certificate details
sipapp <start | stop>	Start or stop the SIP application
sendunistim <xx xx....>	Send UNIStim message
rxunistim <on | off	Display UNIStim messages from the Core
txunistim <on | off	Display UNIStim messages to the Core from the SIP application
sendevent <0xmmm <0xnnn>	Simulate an UNIStim event.
lcdparam	Set up LCD parameters for the IP Deskphone
audio <hs | hd | hf | off>	Loopback audio to handset/headset/Handsfree
display <on | off>	Turn all LCD and LED on or off
keypress <on | off>	Turn all key presses on or off
clearlog >clearlog<mngr_dest>	Clears content of the specified log file. The input parameter specifies the type of logging manager: • 0 (default)—ECT-log file • 1—SIP-log file If the input parameter is incorrect, the following notification appears: >clearlog: incorrect type of manager <x>
removelog >removelog<mngr_dest>	Removes the specified log file. The input parameter specifies the type of logging manager: • 0 (default)—ECR-log file • 1—SIP-log file If the input parameter is incorrect, the following notification appears: >removelog: incorrect type of manager <x>
reset2factory >reset2factory	Resets the IP Deskphone to the default setting. See Activating Reset to Factory Setting using SSH_PDT on page 360.
routePrint	Displays GW IPv6 addresses.

Table continues…

Command	Description
ifShow	Displays IPv4 interface.
ping	Sends ICMPv6 Echo Request messages and records the receipt of ICMPv6 Echo Reply messages. With ping, the IP Deskphone can detect network or host communication failures and troubleshoot common IPv6 connectivity problems. Link-Local and Global addresses, as well as other node names, can be pinged.
v6ParmsShow	Displays all of the IPv6 related parameters: • IPv6 Enabled • Phone IPv6 address (if, entered manually or learned from DHCPv6 server) • Phone IPv6 prefix • DNS server 1 IPV6 address • DNS server 2 IPV6 address • Provisioning server data: protocol and IP address.
routePrint, routepr, netstat "-nr"	Display routing table IPv4 and IPV6 entries.
ip6statShow	Display IPv6 interface statistics, such as the total IPv6 packets and fragments sent and received.

You can request the following commands to the support team if you have any issues:

- printSetInfo
- prtcfg
- prtlog 0
- prtlog 1
- netinfo
- arpShow
- memShow
- routeshow
- i

The command (i) displays the list of tasks with TID and STATUS fields. For every task that has SUSPEND status in the list, enter the following commands:

ti 0x. <TID>

tt 0x <TID>

checkStack 0x <TID>

To print out the list of all supported commands and short description, enter the "?" command when the PDT prompt is displayed; for example, `PDT> ?`.

PDT for USB flash drive

The PDT contains commands that allow the IP Deskphone to display file system information on the first valid USB flash drive attached to the IP Deskphone. File system information is not displayed in the True Flash File System (TFFS) because there are already commands in the PDT to perform similar operations for the TFFS.

The following table describes the USB flash drive PDT commands.

Table 80: USB memory stick PDT commands

Shell Commands	Description
`usbFsShow`	Displays MSDOS volume configuration data of `/bd0` (USB flash drive).
`usbls [dirname] [-f]`	Lists the contents of a directory `[dirname]` in `/bd0` . If the -f flag is specified, print details.
`usblsr [dirname]`	Lists the contents of a directory `[dirname]` in `/bd0` and any of the subdirectories.
`usbcd [dirname]`	Changes the directory to `[dirname]` relative to the current directory.

The following is a sample display on the command `usbFsShow` in the PDT, on a 1G Kingston DataTraveler 2.0 flash drive.

```
volume descriptor ptr (pVolDesc):       0x81866bf0
cache block I/O descriptor ptr (cbio):  0x818f2c1c
auto disk check on mount:               NOT ENABLED
max # of simultaneously open files:     34
file descriptors in use:                0
# of different files in use:            0
# of descriptors for deleted files:     0
# of obsolete descriptors:              0

current volume configuration:
 - volume label:        KINGSTON ; (in boot sector:     KINGSTON    )
 - volume Id:           0x88e5e84b
 - total number of sectors:     2,015,200
 - bytes per sector:            512
 - # of sectors per cluster:    32
 - # of reserved sectors:       2
 - FAT entry size:              FAT16
 - # of sectors per FAT copy:   247
 - # of FAT table copies:       2
 - # of hidden sectors:         32
 - first cluster is in sector # 528
 - Update last access date for open-read-close = FALSE
 - directory structure:         VFAT
 - root dir start sector:               496
 - # of sectors per root:               32
 - max # of entries in root:            512

FAT handler information:
------------------------
 - allocation group size:       7 clusters
 - free space on volume:        724,893,696 bytes
```

Figure 84: PDT output on usbFsShow command

Update PDT device configuration information

The PDT device configuration is updated with USB port lock information. You can remotely monitor the individual USB device configuration status using the PDT.

```
*********************SYSTEM CONFIG*************************
 *** SIPdomain1 emsalpha.com
........
 *** DISABLE_USB_PORT: No
 *** USB_MOUSE: UNLOCK
 *** USB_KEYBOARD: UNLOCK
 *** USB_HEADSET: UNLOCK
 *** USB_MEMORY_STICK: UNLOCK
 *** USB_LOCK_OVERRIDE: No
 *** ATA_REGION: NA
........
```

Figure 85: USB Device information from PDT

Device configuration file

The following table describes the configuration commands in the device configuration file for alarms, logs and diagnostics.

Table 81: Alarms, logs and diagnostics configuration commands

Component	Flag	Description
PC Port Mirroring parameter which can be enabled and disabled in the **Advanced Diag Tools** dialog.	PORT_MIRROR_ENABLE	Determines whether the Port Mirror option can be enabled/disabled or not through the IP Deskphone **Advanced Diag Tools** menu. • If PORT_MIRROR_ENABLE is configured as YES, The Port Mirroring prompt in the Advanced Diag Tools dialog is enabled, and you can activate or deactivate the Port Mirror option. • If PORT_MIRROR_ENABLE is configured as NO, the Port Mirroring prompt in the Advanced Diag Tools dialog is disabled (dimmed); the option is deactivated by force, and you cannot access the Port Mirror option. • The values are YES and NO. The default value is NO (disabled).

Table continues…

Component	Flag	Description
Memory Monitor.	MEMCHECK_PERIOD	Determines the time period in seconds when the Memory monitor wakes up (after start-up or the last memory check attempt). • The values are 1800 (0.5 hrs) to 86400 (24 hrs). The default value is 86400 (24 hrs).
SIP-traffic monitor	DOS_PACKET_RATE	Determines the maximum number of packets per second that is allowed.
SIP_traffic monitor	DOS_MAX_LIMIT	Specifies how many packets past DOS_PACKET_RATE the IP Deskphone can receive before packets are dropped. • If packets are received at a rate of DOS_PACKET_RATE +1, then packets start getting dropped after the time specified in DOS_MAX_LIMIT (in seconds).
SIP-traffic monitor	DOS_LOCK_TIME	Specifies the amount of time (in seconds) the IP Deskphone stops processing packets after DOS_MAX_LIMIT is reached. • If DOS_PACKET_RATE is < 1, other values are ignored and packets are not dropped.
Logging System	LOGSIP_ENABLE	Allows the administrator to enable or disable SIP-logging. • If the parameter is YES, the SIP-logging Manager is active and starts logging SIP incoming and outgoing packages into the log files in FFS. • The values are YES and NO. The default value is NO (the manager is not active and the IP Deskphone does not log in SIP incoming and outgoing packages.

Diagnostic Logs

The IP Deskphone supports two types of log files:

- ECR-log
- SIP-log

ECR-log file

The ECR-log file registers and provides detailed information on the errors or bugs that occur during the operation of the IP Deskphone. The ECR-log also contains records indicating some events, such as restart.

Each error is logged as a record. The format of the record is the same regardless of the monitor that generates it or the level of severity of the error. There are three sections to the record.

The first section provides mandatory information for each record including:

- severity level
- severity flag
- time stamp
- software version
- source file information
- error number
- brief description

For example, `=== Record #001 === MAJOR SET Logged 01/07/2002 00:34:35 Firmware: 06A5C1Hd10`

`Description: Task Monitor: the Transport task is suspended`

The second section is optional. If the task is registered in the list of stack overflow events, the following may occur:

```
ERROR*ecrStackShow: :StackOverflow: PDT
```

```
tpStackBase = 0x8194ffa0, pStackLimit=0x8194bfa0, pStackEnd= 0x8194bfa0
```

```
tstack: base 0x8194ffa0 end 0x8194bfa0 size 16368 high 1492 margin 14874
```

The third section includes the supplementary information. The content depends on the flag in the calling function. The flag can be as follows:

- `ECR_LOG_NO_EXTRA_INFO:` – no supplementary information
- `ECR_LOG_TASK_INFO:` – log task information (ti, tt, the stack information from SP-96 to SP +96)
- `ECR_LOG_SUM_TASK_INFO:`– log summary of each task TCB (i)
- `ECR_LOG_MEM_INFO:` –log memory usage information (memShow)

The following is an example of the supplementary information in the ECR-log file:

```
Summary info for all tasks:

  NAME         ENTRY        TID      PRI   STATUS      PC       SP       ERRNO  DELAY
---------- ------------ -------- --- ---------- -------- -------- ------- -----
tExcTask   excTask      81ff93d0   0 PEND       8078cc18 81ff92b0   3006b     0
tLogTask   logTask      81ff6840   0 PEND       8078cc18 81ff6728       0     0
hwtk       8051d994     819c8070  20 SUSPEND    80634554 819c7ff0       0     0
ECR_WDOG   800e977c     81a24ab0  49 PEND       80634554 81a24a38       0     0
BLST       800d2310     81a36bb0 125 PEND+T     80634554 81a36b28       0 87194
DISR       8002187c     819e61f0 125 PEND       80634554 819e6168       0     0

Memory Usage Info:

 status    bytes     blocks   avg block  max block
 ------ ---------- --------- ---------- ----------
current
   free    9498400       186      51066    9249120
  alloc    7210640      4915       1467          -
cumulative
  alloc   81327184     29445       2762          -

Detailed info for task ID 0x819C8070:

  NAME         ENTRY        TID      PRI   STATUS      PC       SP       ERRNO  DELAY
---------- ------------ -------- --- ---------- -------- -------- ------- -----
hwtk       8051d994     819c8070  20 SUSPEND    80634554 819e1938       0     0

stack: base 0x819c8070  end 0x819c6070  size 8176  high 1432  margin 6744

options: 0x4
VX_DEALLOC_STACK

VxWorks Events
--------------
Events Pended on     : Not Pended
Received Events      : 0x0
Options              : N/A

$0     =        0  t0    =        0  s0    =        0  t8    =        0
at     = 80d70000  t1    = 1000ff00  s1    =        0  t9    = 80e70000
v0     =        0  t2    = 80e97e74  s2    =        0  k0    =        0
v1     =      3fe  t3    =        0  s3    =        0  k1    =        0
a0     =       50  t4    = 80e7e308  s4    =        0  gp    = 80d94a50
a1     =       21  t5    =       82  s5    =        0  sp    = 819c7ff0
a2     =        1  t6    = 203ac098  s6    =        0  s8    = 819c8010
a3     = 80efec72  t7    =        0  s7    =        0  ra    = 807830fc
divlo  =        6  divhi =        4  sr    = 1000ff01  pc    = 80634554


Task Trace:

819c8030 _pthread_setcanceltype+ac8a64: KNL_RunReadyThreads (819c8280, ffffffff,
 0, 0)
807830f4 KNL_RunReadyThreads+74 : semQPut (&KNL_gGlobals, 80782dac, 819c8000, 80
0ecb50)

stack dump from sp-96 to sp+96
```

Figure 86: Example of the supplementary information in the ECR-log file

```
819e18d0:                0000 0000 819a f200  *        ......*
819e18e0:  0000 0000 8059 aa48 8039 3890 8086 1884  *..... Y.H.98.....*
819e18f0:  eeee eeee eeee eeee eeee eeee 0000 0000  *................*
...
819e19c0:  819e 95f0 eeee eeee eeee eeee eeee eeee  *................*
819e19d0:  819e 19d8 801f 08a0                      *................*
value = 21 = 0x15
```

Figure 87: Example of the supplementary information in the ECR-log file (continued)

The following is an example of the ECR-log file.

```
PDT>prtlog 0 (----------------> example of the ECR-log file)
```

```
***** ERROR LOG FILE *****
=== Record #000 ===
CRITICAL ERROR SET    Logged 11/26/2007 02:46:46    Firmware: B221C61
File: EcrTaskMonitor.c Line #585 Error #4
Description: Task Monitor: one or more tasks have been suspended
For details see the current record (summary info) and
one or more next records (detailed info for every suspended task)

Summary info for all tasks:
 NAME      ENTRY      TID    PRI  STATUS    PC     SP    ERRNO  DELAY
---------- ------------ -------- --- ---------- -------- -------- ------- -----
tExcTask   excTask    81cf9790   0 PEND     80489bc8 81cf9670  3006b    0
tLogTask   logTask    81cf6c00   0 PEND     80489bc8 81cf6ae8      0    0
tS1811Int  intThread  81a7c610   0 PEND+T   803e50a4 81a7c570  830106  10
tShell     shell      81adc090   1 PEND     803e50a4 81adbcb0  1c0001    0
tUsbdBus   802f451c   81a78400  10 PEND     803e50a4 81a78330      0    0
CpuMon     800e2bac   81941110  19 DELAY    803d0c7c 81941050      0   66
....
DISR       8002f938   81a14600 125 PEND     803e50a4 81a14578      0    0
FLASHICON  8002f494   81a46100 125 PEND     803e50a4 81a46080      0    0
INDR       8004a26c   81cffdb0 125 PEND     803e50a4 81cffd28      0    0
HOOK       8004b990   81cfeb40 125 SUSPEND  803d0c7c 81cfea78      0    0
KTSK       8004caf4   81cfd890 125 PEND     803e50a4 81cfd6a8      0    0
KBDR       8004b330   81cfc5e0 125 PEND     803e50a4 81cfc558      0    0
TPDET      800684e4   818f1370 125 PEND     803e50a4 818f12a8      0    0
DRAWDET    80067f6c   81a42760 125 SUSPEND  803e7604 81a42738      0    0
RTC        800485bc   81991600 125 READY    803e50a4 81991548      0    0
CDT        CDTUpdate  819903f0 125 READY    803e50a4 81990348      0    0
HDDET      80040570   8198f1e0 125 PEND     803e50a4 8198f138      0    0
....
i200xApp   winAppTask 818fffe0 200 PEND     80489bc8 818ffe28      0    0
ETHERSET_TI8019efc0   81537670 201 READY    803e50a4 81537588  3d0004    0
tCertExpire8043e814   8152f820 240 DELAY    803d0c7c 8152f788      0 190327 1
tTimeSave  80451acc   8152a7f0 240 DELAY    803d0c7c 8152a768      0 226509 1
mocSshMn   80127eac   8150b260 240 READY    803e50a4 8150b0f8  3d0004    0
tDcacheUpd dcacheUpd  81ab55b0 250 READY    803d0c7c 81ab54f8      0    0
Idle       800e2b68   819c1c20 253 READY    803d0c7c 819c1b98      0    0
tUsbKbd    802f451c   81559ef0 255 READY    803d0c7c 81559e20      0    0
```

Figure 88: Example of the ECR-log file

```
Memory Usage Info:
 status   bytes    blocks   avg block  max block
 ------ ---------- --------- ---------- ----------
current
  free  13126912      49    267896   12944576
 alloc   8499952    2994     2838         -
cumulative
 alloc  78960576  1306171       60         -
 == Record #001 ==
CRITICAL ERROR_SET    Logged 11/26/2007 02:46:45      Firmware: B221C61
File: EcrTaskMonitor.c Line #548 Error #4
Description: Task Monitor: the HOOK task is suspended
Detailed info for task ID 0x81CFEB40:
 NAME      ENTRY     TID   PRI  STATUS    PC     SP   ERRNO DELAY
---------- ----------- -------- --- --------- -------- -------- ------- -----
HOOK     8004b990    81cfeb40 125 SUSPEND   803d0c7c 81cfea78     0    0
stack: base 0x81cfeb40  end 0x81cfdb40  size 4080   high 460    margin 3620
options: 0x4
VX_DEALLOC_STACK
VxWorks Events
--------------
Events Pended on     : Not Pended
Received Events      : 0x0
Options              : N/A
$0    =      0  t0   =      0  s0   =      0  t8   =       1
at    =      0  t1   =      0  s1   =      0  t9   =       1
v0    =      0  t2   =      0  s2   =      0  k0   =       0
v1    =      0  t3   =      0  s3   =      0  k1   =       0
a0    =      2  t4   =      0  s4   =      0  gp   = 80709230
a1    =      0  t5   =      0  s5   = 81cfeb40  sp   = 81cfea78
a2    =      0  t6   =      0  s6   =      2  s8   = 81cfeac0
a3    =      0  t7   =      0  s7   = 8081b184  ra   = 8004eed4
divlo =      0  divhi =     0  sr   = 1000ff01  pc   = 803d0c7c
Task Trace:
803e7610 vxTaskEntry    +c  : kbdhsSetKey (0, 0, 0, 0)
8004bbfc kbdhsSetKey    +350: bcmOsSleep (2, eeeeeeee, eeeeeeee, eeeeeeee)
8004eecc bcmOsSleep     +18 : taskDelay (81cfeae0, 803e7304, 81cfeb40, 81a6ffe0)

value = 0 = 0x0
```

Figure 89: Example of the ECR-log file (continued)

SIP-log file

The SIP-log file registers incoming and outgoing SIP-packages, and each package is logged as a record. There are two sections:

- The first section requires mandatory information for each record including:
  - type of the package (incoming or outgoing)
  - time stamp
  - software version
- The second section contains the content of the package in the text format.

The following is an example of the SIP-log file.

```
PDT>prtlog 1 (----------------> example of the SIP-log file)
```

```
***** SIP LOG FILE *****
=== Record #001 ===
SIP_MSG_OUT    Logged 11/26/2007 02:46:45      Firmware: B221C61
INVITE sip:2114@10.25.200.148 SIP/2.0
From: sip:2110@10.25.200.148;tag=2c1737
To: sip:2114@10.25.200.148
Call-Id: call-1045244621-19@10.25.200.218
Cseq: 1 INVITE
Contact: <sip:2110@10.25.200.218>
Content-Type: application/sdp
Content-Length: 308
Accept-Language: en
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE
Supported: sip-cc, sip-cc-01, timer, replaces
User-Agent: Pingtel/2.1.3 (VxWorks)
Date: Fri, 14 Feb 2003 17:43:50 GMT
Via: SIP/2.0/UDP 10.25.200.218

v=0
o=Pingtel 5 5 IN IP4 10.25.200.218
s=phone-call
c=IN IP4 10.25.200.218
t=0 0
m=audio 8766 RTP/AVP 96 97 0 8 18 98
a=rtpmap:96 eg711u/8000/1
a=rtpmap:97 eg711a/8000/1
a=rtpmap:0 pcmu/8000/1
a=rtpmap:8 pcma/8000/1
a=rtpmap:18 g729/8000/1
a=fmtp:18 annexb=no
a=rtpmap:98 telephone-event/8000/1 === Record #001 ===
SIP MESSAGE    Logged 11/26/2007 02:46:45      Firmware: B221C61
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.25.200.148:5060;branch=z9hG4bK-li5h35u7wd5l.0;rport=5060
Via: SIP/2.0/UDP 10.25.200.218
From: sip:2110@10.25.200.148;tag=2c1737
To: sip:2114@10.25.200.148;tag=6l895xlhxl
Call-ID: call-1045244621-19@10.25.200.218
Record-Route: <sip:2114@10.25.200.148;maddr=10.25.200.148>
Contact: <sip:2114@10.25.200.220:5060;line=1>
CSeq: 1 INVITE
Content-Length: 0

=== Record #002 ===
SIP_MSG_IN    Logged 11/26/2007 02:46:45      Firmware: B221C61
```

Figure 90: Example of the SIP-log file

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 10.25.200.148:5060;branch=z9hG4bK-li5h35u7wd51.0;rport=5060
Via: SIP/2.0/UDP 10.25.200.218
From: sip:2110@10.25.200.148;tag=2c1737
To: sip:2114@10.25.200.148;tag=61895xlhxl
Call-ID: call-1045244621-19@10.25.200.218
Record-Route: <sip:2114@10.25.200.148;maddr=10.25.200.148>
Contact: <sip:2114@10.25.200.220:5060;line=1>
CSeq: 1 INVITE
Content-Length: 0
```

Figure 91: Example of the SIP-log file (continued)

There are three ways to obtain SIP-logs from an IP Deskphone:

1. Online — connect to the IP Deskphone through SSH and enter the `dbgshell` PDT command. The log messages are printed out during a call to the SSH console.
2. Offline— connect to the IP Deskphone through SSH and enter the `prtlog 1` PDT command. The active SIP log file is printed out to the SSH console.
3. Offline Log File — Log files are stored on the IP Deskphone flash device. You can access the log files through the File Manager of the IP Deskphone and copy them to an external flash card.

Copy Log files through File Manager of the IP Deskphone:

1. Connect a USB flash drive to the USB port of the IP Deskphone.
2. Navigate to **File Manager->Phone->Logs**.
3. Select one of *.log files.
4. Press the **Send** soft key.

You can also obtain the log files through an SFTP connection to the IP Deskphone.

Enable SFTP on the IP Deskphone:

Note:

Changing the SFTP_READ_PATTERNS causes the IP Deskphone to reboot.

1. Open the **Device Settings** menu.
2. Check the **Enable SFTP** checkbox if it is not checked. If it is checked, do the following:
   - Press the **Auto** soft key and check the **SFTP Enable** checkbox in the **Auto Provisioning** window.
   - Press **Config** soft key to return to network settings window
   - Check the **Enable SSH** checkbox.
3. Add the following parameters to the device configuration file of the IP Deskphone:

   SSH YES

SSHID <user name>

SSHPWD <user password>

SFTP YES

SFTP_READ_PATTERNS .txt,.zip,.log

SFTP_WRITE_PATTERNS .txt,.zip,.log

You can then connect through SFTP and obtain the most recent log file — /logs/SIPLogFile.log, and the archive file — /logs/SIPLogFile.log.zip.

PC Client Softphone interworking

If the user does not have access to the pre-authorization configurations in the Feature Options menu, the feature is not enabled. You must verify the device configurations and enable the interworking feature so that the user can access the pre-grant authorization configuration and the IP Deskphone can auto-answer calls from authorized users or user groups. For more information, see Configuring the PC Client Softphone on page 233.

If the call is being received, but is not being automatically answered in a Click-to-Answer scenario, the user must verify that the user making the request is an authorized user. For more information, see Pre-granting authorization for the Answer-Mode on page 229.

Logging and errors

A logon failure is logged in the appropriate security log, and can be reviewed in the PDT using the following command:

```
listsecuritylogs
```

SRTP

If a session changes from secure media to non-secure media, the following event is posted in the security log:

```
1050[Minor]

[TUE JAN 02 19:25:51 2007]

[1406]

[Net/sigma/Sdp Stream.cpp:709] - Secure to Non Secure
```

If there is a media negotiation failure, such as secure telephone to non-secure telephone, the call log (inbox of the called party and the outbox of the caller) contains the following additional information string:

```
Media negotiation failure
```

SSH

If a logon failure for SSH Authentication occurs, the following event is posted in the security log:

```
1040[Minor][TUE JAN 02 20:12:14 2007][4189][i:/fw/buil d/../util/sshapp/
sshServer.c:616] - SSH Authentication Failed
```

Part 2: Avaya Aura® support for 1100 Series IP Deskphones

The Avaya Aura® communications platform (solution comprised of Avaya Aura™ Communication Manager, Avaya Aura™ Session Manager, Avaya Modular Messaging) now supports the 1100 Series IP Deskphone with SIP 4.4 software. The 1100 Series IP Deskphones are directly registered to Session Manager and are supported by Communication Manager configured as an Evolution Server (CM-ES).

Supported platforms

The following Avaya Aura® platforms are supported:

- Avaya Aura® Communication Manager 6.2 FP2
- Avaya Aura® Session Manager 6.2 FP2
- Avaya Aura® Messaging 6.2
- Avaya Aura® Presence Services 6.1
- Avaya Aura® Conferencing 7.0

Telephony features

Some Communication Manager (CM) features can be invoked by dialing a Communication Manager Feature Name Extension (FNE). FNEs must be defined in Communication Manager for each of those features, subject to the existing dial plan.

Some CM features can be invoked by dialing a Communication Manager Feature Access Code (FAC). FACs must be defined in Communication Manager for each of those features, subject to the existing dial plan.

Note:

Most FNEs require first configuring the equivalent FAC.

Chapter 20: Presence support

Presence support for 1100 Series IP Deskphones

SIP 4.4 introduces support for the Presence feature for 1100 Series IP Deskphone users on Avaya Aura® with Avaya Presence Server (PS).

The Presence feature is configured in SIP 4.4 with the following new configuration parameters:

- RPID_PRESENCE_ENABLE <YES/NO>
- PRES_SERVER_IP <IP address of Presence Server>

If the RPID_PRESENCE_ENABLE parameter is set to YES, RPID-based subscription and notification messages, required for Avaya Presence Services, are sent.

PRES_SERVER_IP parameter defines the IP address of the Avaya Presence Server.

Important:

If RPID_PRESENCE_ENABLE is configured as YES:

- The IP Deskphone must be configured to use TLS for connection to the SIP proxy.
- USE_PUBLISH_FOR_PRESENCE must be set to YES.
- USE_DEFAULT_DEV_CERT must be set to YES to use the default device certificate for the TLS connection to Avaya Aura to work with the contact list stored on Avaya Aura Session Manager.
- ENABLE_SERVICE_PACKAGE must be set to PPM.
- In the phone’s Communication Profile, check **Presence Profile** and select the appropriate Presence Server from the drop-down list.

Presence states

Presence dialog has been expanded to include the list of activities according to RFC4480.

The following activities are available when RPID_PRESENCE_ENABLE is set to YES:

Appointment	Permanent absence
Away	Playing
Breakfast	Presentation
Busy	Shopping

Table continues…

Dinner	Sleeping
Holiday	Spectator
In transit	Steering
Looking for work	Travel
Lunch	TV
Meal	Vacation
Meeting	Working
On the phone	Worship
Performance	Unknown

To set the desired presence state and activity, the IP Deskphone user must open the Presence dialog, select the presence state (Connected or Unavailable) and then select the desired activity. Any combination of presence state and activity can be selected.

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382
Presence status in Address Book on page 23

Presence status in Address Book

The status dialog of the Address Book displays the presence state of contacts designated as Friends. In SIP 4.4, the IP Deskphone Address Book displays the presence state of Friends if RPID_PRESENCE_ENABLE is set to YES.

Phone state

Phone state is determined automatically, based on notifications received from Avaya Presence Server. Phone state can be one of the following:

- On hook – when the phone handset is on hook; there are no active calls
- On a call – the user is on a call
- Do Not Disturb – when the user activated Do Not Disturb mode
- Unknown

Note:

Phone state does not depend on the presence state and activity selected by the end user.

Note:

- The 1100 Series IP Deskphones support more presence states than the Aura Presence Server (PS); activity detail appears on the 1100 Series and 1200 Series IP Deskphones but not on Avaya 96xx Series phones.
- Idle 1100 Series IP Deskphones appear as "offline" in the Avaya 96xx Series phones presence status; however, Busy, On the Phone and Away activities are displayed correctly.

Related links

Presence support for 1100 Series IP Deskphones on page 21

Chapter 21: Personal Profile Manager

Personal Profile Manager support

SIP software supports the Personal Profile Manager (PPM) for Avaya Aura Communication Manager/Session Manager.

The PPM is a web service that runs as part of Avaya Aura® Session Manager and the System Manager. PPM processes SOAP messages over HTTP/HTTPS with digest authentication.

PPM is responsible for maintaining and managing an end user's personal information in the system. This information includes (but is not limited to) contact list information, profile information, session history, access control lists, and other permissions management. In addition to communicating with other server components managing the data within the infrastructure servers, the PPM also interfaces directly with the IP Deskphones.

The following functionality is supported with PPM:

- retrieving contact list from PPM
- adding and deleting contacts
- updating contact
- searching user
- retrieving E911 numbers
- PPM reboot mechanism

IP Deskphones authenticate themselves with the PPM, with the same user name and password used during SIP registration; each PPM request to the Session Manager is authenticated using digest authentication (see RFC 2617) over HTTP or HTTPS.

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382
Configuration on page 387
Contact lists and PPM on page 387
Emergency numbers on page 387
Global search with PPM on page 388
PPM reboot mechanism on page 388

Configuration

To enable support for PPM, configure the following parameter in the device configuration file :

ENABLE_SERVICE_PACKAGE PPM

Related links

Personal Profile Manager support on page 386

Contact lists and PPM

PPM is responsible for maintaining and managing an end user's personal information in the system.

The following contact list functionality is supported with PPM:

- retrieving contact list from PPM
- adding and deleting contacts
- updating contact information

When the IP Deskphone user adds, edits, or deletes a contact in their Address Book, a corresponding request is sent to PPM and that information is added to the user's contact list on PPM. PPM does not provide information about contact list size restrictions. This information is retrieved from the device configuration file. The parameter MAX_ADDR_BOOK_ENTRIES defines the size of the contact list and permitted number of friends.

Note:

The PPM contact list does not support a user's groups in the contact list.

Contact name, address, and designation as friend or not must be entered; otherwise, PPM rejects the entry.

Related links

Personal Profile Manager support on page 386

Emergency numbers

The emergency number from PPM should be included in the dialing plan and possess all properties of that emergency number.

PPM data is located first, then data from a Dialing Plan file. Note that PPM data has priority over data from a Dialing Plan file. If the emergency numbers in PPM and the Dialing Plan file are identical, then the number from PPM is dialed. Emergency PPM data and Dialing Plan data from the configuration file can work together.

Note:

Calls to an emergency number are blocked from:

- Conference
- Transfer
- Join
- Hold
- Park

Related links

Personal Profile Manager support on page 386

Global search with PPM

When PPM is enabled, and a global search is initiated from the IP Deskphone, PPM allows the IP Deskphone to search the Session Manager database for administered users. This search is based on search criteria sent in the request. IP Deskphone users can search using the following criteria:

- User Name (login name of the user; for example, 508@abc.com)
- First Name
- Last Name
- Phone Number

All users who correspond to the submitted criteria are retrieved from the database and displayed as a list. A maximum of 250 contacts are displayed.

The IP Deskphone user can search within this list using the standard local search mechanism. Pressing the **Save** soft key for a contact selected from the list saves the contact in the user's Address Book.

It is possible to call any contact in the list, save any contact from the list to the Address Book, and view the contact details.

Related links

Personal Profile Manager support on page 386

PPM reboot mechanism

A soft reboot of the IP Deskphones can be performed on command through PPM.

The Reboot command is accessed through Session Manager. Invoking the Reboot command through PPM causes the IP Deskphone to perform a soft reboot (power cycle). This causes the IP Deskphone to retrieve the 1xxxxSIP.cfg file from the provisioning server and perform a software upgrade if required.

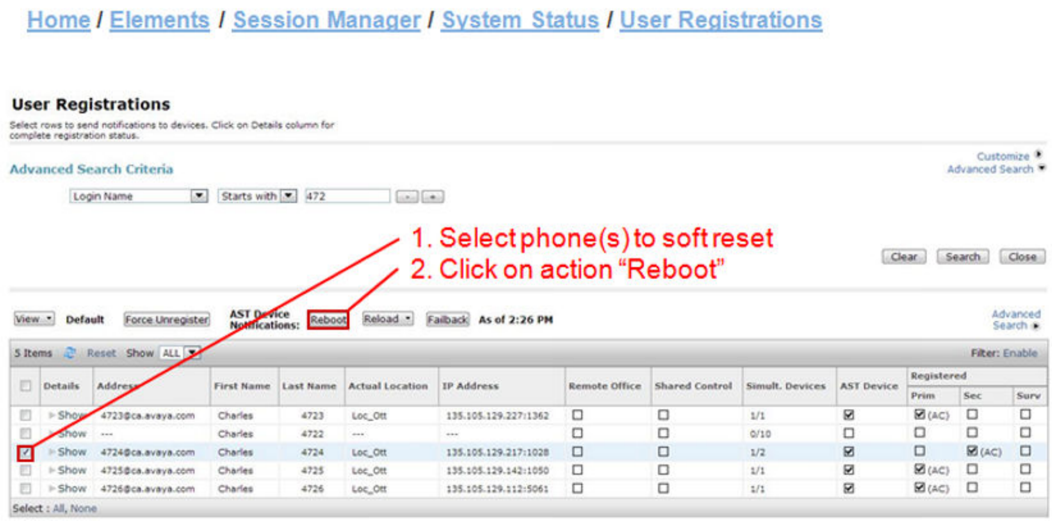


Figure 92: Reboot in Session Manager

Related links

Personal Profile Manager support on page 386

Chapter 22: Embedded Device Certificate

Embedded device certificate support

TLS connection with Avaya Aura® Session Manager requires mutual authentication by default. Mutual authentication requires proper Certificate Authority (CA) and device certificates to be installed on every IP Deskphone.

A default device certificate in the firmware allows easy connection to Avaya Aura® through Session Manager using TLS . The IP Deskphones already have an embedded CA certificate which is trusted by Avaya Aura®; the embedded device certificate eliminates the need for customers to generate and install device certificates manually.

If used, embedded device certificate information is displayed in the IP Deskphone and in the output of appropriate PDT commands.

Important:

The default embedded device certificates are trusted by the Avaya Aura® system. If Aura® is configured so that the default certificates are replaced by customer certificates, then the appropriate CA and device certificates must be installed on the IP Deskphones as well.

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382
Configuration on page 390

Configuration

The following parameter configures the default embedded device certificate.

USE_DEFAULT_DEV_CERT [YES/NO]

— YES – Use the default device certificate if no customer device certificate is installed.

— NO – Do not use the default device certificate (default).

This parameter controls the use of the default device certificate for HTTPS/TLS connections. The default value is NO. It is configured in the device configuration file.

Related links

Embedded device certificate support on page 390

Chapter 23: SRTP with Avaya Aura

SRTP support with Avaya Aura®

SRTP is supported with Avaya Aura®.

The following SRTP modes are supported:

- Secure Only
- Best Effort Capability Negotiation

Note:

To use SRTP, you first have to be using TLS. That is, you cannot have secure media without using secure signalling.

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382
Configuration on page 391

Configuration

The following parameter is used to to support SRTP on Avaya Aura®:

AVAYA_AURA_MODE_ENABLE [YES | NO]

The command specifies if Avaya Aura®-specific features are active on the IP Deskphone or not. The default value is NO. It can be configured through the device configuration file and through server profiles.

— YES – Avaya Aura-specific features are active.

— NO – Avaya Aura-specific features are not active.

Important:

In the device configuration file, the parameter MKI must be set to NO.

Related links

SRTP support with Avaya Aura® on page 391

Chapter 24: Multi-user login on Avaya Aura

Multi-user login on Avaya Aura®

The following multi-user scenarios are supported:

- One user can log on to a maximum of 10 IP Deskphones.

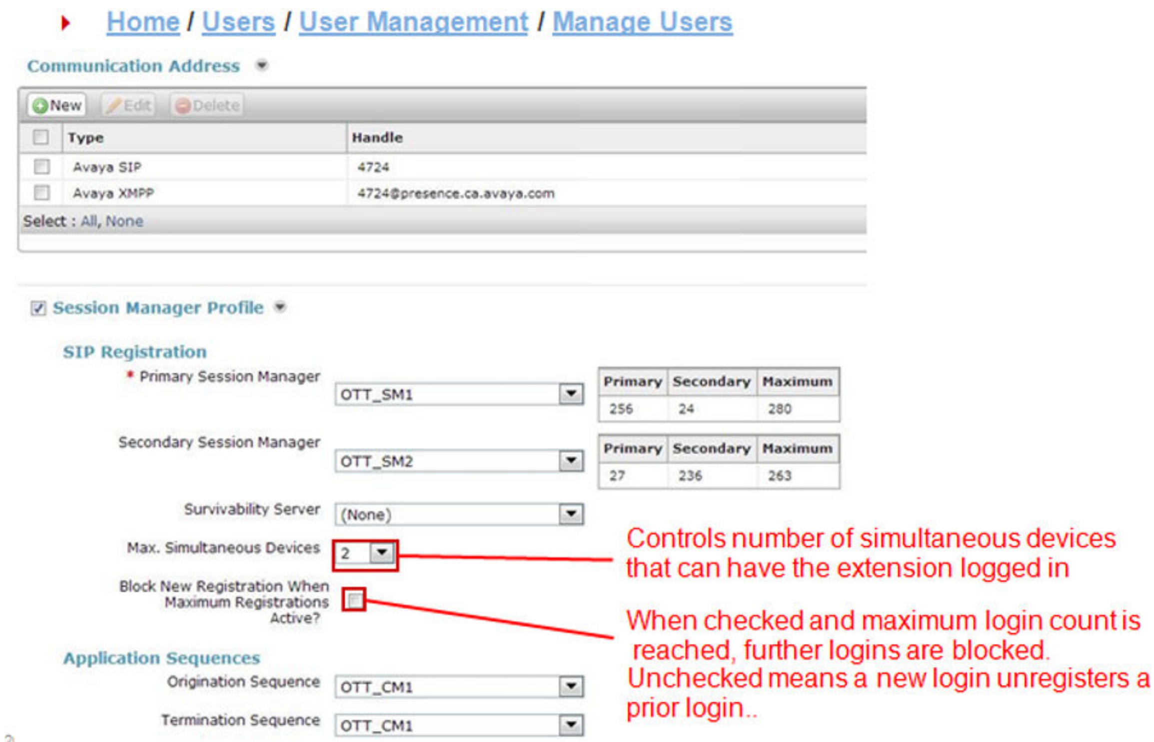
  Note:

  Once the call is answered at one phone, other users cannot see status of that call on the other phones.

- Multiple users (extensions) can log onto one IP Deskphone.
- When multiple users are logged onto one IP Deskphone, the IP Deskphone can be logged into more than one system.

Multi-user functionality requires Avaya Aura® FP2 (or later) with parallel forking.

The maximum number of user logins for one user extension is configured in Session Manager, as shown in the following figure.



Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382

Chapter 25: FNEs and FACs for 1100 Series IP Deskphones

FNEs and FACs with Avaya Aura®

Some Avaya Aura® features are invoked by dialing a Communication Manager Feature Name Extension Extension (FNE) or Feature Access Code (FAC). A speed dial button on the IP Deskphone can be programmed to an FNE or FAC.

Note:

Most FNEs require first configuring the equivalent FAC.

This enables a feature to be easily accessed by pressing a speed dial key on the IP Deskphone instead of dialing an entire FNE or FAC code.

For information on configuring a speed dial key on an IP Deskphone, refer to the User Guide for the specific model of IP Deskphone.

For information on configuring FNEs and FACs in Communication Manager, see *Configuring Avaya 1100 Series and 1200 Series IP Deskphones running Release 4.3 SIP software with Avaya Aura® Session Manager Release 6.1, Avaya Aura® Communication Manager Release 6.0.1, and Avaya Aura® Messaging Release 6.1 - Issue: 1.0*, available at http://avaya.com/support.

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382

Supported features on Avaya Aura®

The following table lists the supported CS 1000 call features with their Avaya Aura® equivilent, and whether they are accessed through an FAC or an FNE.

CS 1000 feature name	Avaya Aura® feature name	Access method
Speed Call/System Speed Call	Abbreviated Dialing List1	FAC
	Abbreviated Dialing List2	FAC
	Abbreviated Dialing List3	FAC

Table continues…

CS 1000 feature name	Avaya Aura® feature name	Access method
	Abbreviated Dial – Prgm Group List	FAC
Ring Again	Automatic Callback	FNE
Call Forward Busy	Call Forwarding Activation Busy/DA	FNE
Call Forward All Calls	Call Forwarding Activation All	FNE
Call Forward Disable	Call Forwarding Deactivation	FNE
Call Park	Call Park	FNE
	Answer Back	FNE
Call Pickup	Call Pickup	FNE
Charge Account, Forced	CDR Account Code	FAC
Calling Party Privacy	Per Call CPN Blocking	FNE
Conference 3 or 6 Party	Ad-hoc Conference	FNE
Selectable Conferee Disconnect (for last party)	Ad-hoc Conference Drop Last Added Party	FNE
Call Pickup, Directed (DPU)	Directed Call Pickup	FNE
Call Pickup, Directed (GPU)	Directed Group Call Pickup	FAC
	Extended Group Call Pickup	FNE
Mobile X	Enhanced EC500	FAC/FNE
Priority Call	Priority Calling	FNE
Remote Call Forward	Extended Call Fwd Busy D/A	FAC
	Extended Call Fwd All	FAC
	Extended Call Fwd	FAC
Do Not Disturb (Remotely activated)	Remote Send All Calls Activation	FAC
(similar to) Station Specific Authorization Code	Station Lock	FAC
Transfer call to VM	Transfer to Voice Mail	FNE
(similar to) Attendant Break-In with Secrecy	Whisper Page Activation	FNE
Group Hunt Deactivate	Hunt Group Busy	FAC
Malicious Call Hold	Malicious Call Trace	FNE
Access Restrictions	Restriction - Controlled	FAC
Recorded Announcement	Announcement Record/Listen	FAC
— —	Change COR	FAC
— —	Change Coverage	FAC

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382

Feature to FAC/FNE Naming

The following table provides a listing of Communication Server 1000 (CS 1000) features and their FAC/FNE equivalents.

CS 1000 feature name	FAC name	FNE name
Speed Call/System Speed Call	Abbreviated Dialing List1 Access Code	—
	Abbreviated Dialing List2 Access Code	—
	Abbreviated Dialing List3 Access Code	—
	Abbreviated Dial – Prgm Group List Access Code	—
Ring Again	Automatic Callback Activation	Automatic Call Back
	Automatic Callback Deactivation	Automatic Call-Back Cancel
Call Forward Busy	Call Forwarding Activation Busy/DA	Call Forward Busy/No Answer
Call Forward All Calls	Call Forwarding Activation All	Call Forward All
Call Forward Disable	Call Forwarding Deactivation	Call Forward Cancel
Call Park	Call Park Access Code	Call Park
	Answer Back Access Code	Call Park Answer Back
Call Pickup	Call Pickup Access Code	Call Pick-Up
Charge Account, Forced	CDR Account Code Access Code	—
Conference 3 or 6 Party	—	Conference on Answer
Selectable Conferee Disconnect (for last party)	—	Drop Last Added Party
Call Pickup, Directed (DPU)	Directed Call Pickup Access Code	Directed Call Pick-Up
Call Pickup, Directed (GPU)	Directed Group Call Pickup Access Code	—
	Extended Group Call Pickup Access Code	Extended Group Call Pickup
Mobile X	EC500 Self-Administration Access Code	—
	Enhanced EC500 Activation	Off-Pbx Call Enable
	Enhanced EC500 Deactivation	Off-Pbx Call Disable

Table continues…

CS 1000 feature name	FAC name	FNE name
Remote Call Forward	Extended Call Fwd Activate Busy D/A	—
	Extended Call Fwd Activate All	—
	Extended Call Fwd Deactivation	—
Access Restrictions	Control Restrict Activation	—
	Group Control Restrict Deactivation	—
Group Hunt Deactivate	Hunt Group Busy Activation	—
	Hunt Group Busy Deactivation	—
Malicious Call Hold	Malicious Call Trace Activation	Malicious Call Trace
	Malicious Call Trace Deactivation	Malicious Call Trace Cancel
Calling Party Privacy	Per Call CPN Blocking Code Access Code	Calling Number Block
	Per Call CPN Unblocking Code Access Code	Calling Number Unblock
Priority Call	Priority Calling Access Code	Priority Call
Do Not Disturb (Remotely activated)	Remote Send All Calls Activation	—
	Remote Send All Calls Deactivation	—
(similar to) Station Specific Authorization Code	Station Lock Activation	—
	Station Lock Deactivation	—
Transfer call to VM	Transfer to Voice Mail Access Code	Transfer to Voice Mail
(similar to) Attendant Break-In with Secrecy	Whisper Page Activation Access Code	Whisper Page Activation
Recorded Announcement	Announcement Access Code	—
	Change COR Access Code	—
	Change Coverage Access Code	—

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382

Feature configuration details

This section provides further details on feature configuration for the IP Deskphones on Avaya Aura®.

Feature / Functionality	Comments
Call Appearances	1. The endpoint template defaults to 3 call appearances. 2. You can add more/remove call appearances in Endpoint Editor.
Autodial List	1. Configure FACs for Abbreviated Dialing List 1/2/3 and Program Group List. 2. Configure abbreviated-dialing group entries. 3. Configure the phone extension with abbreviated dialing group numbers. 4. Use FACs to access lists and/or program entries.
Calling Name/Number Block (similar to Calling Party Privacy)	1. Configure the FAC and FNE for the Calling Name/ Calling Number Block feature. 2. Use FNEs to enable/disable the feature.
Call Forward All Calls (local)	1. Press the IP Deskphone's **CallFwd** soft key to enable Call Forward All Calls on the IP Deskphone. 2. Press the **CallFwd** soft key again to disable the call forwarding.
Call Forward All Calls (server) Recommended over Call Forward All Calls (local) as Communication Manager handles call coverage better with it)	1. Configure the FAC and FNE for enabling and disabling the Call Forward All Calls feature. 2. Use the FNE to enable/disable the feature.
Call Forward Busy/No Answer	1. Configure the FAC and FNE for enabling and disabling the Call Forward Busy/No Answer feature. 2. Use the FNE to enable/disable the feature.
Call Park / Retrieve	1. Configure the FAC and FNE for Call Park and Answerback. 2. Use FNEs to park a call and retrieve the call.
Call Pickup	1. Configure the FAC and FNE for Call Pickup. 2. Configure the pickup group for the phone extension number. 3. Use the FNE to pickup a ringing call in the group.
Call Pickup, Directed	1. Configure the FAC and FNE for Directed Call Pickup. 2. Configure the IP Deskphone extension COR to allow "Can use" and "Can be picked up" by directed call pickup. 3. Use FNE plus the extension number to pickup the ringing call.
Mobile-X	1. Configure FACs for EC500 self administration and to enable/disable the self-administration feature.

Table continues…

Feature / Functionality	Comments
	2. Configure FNEs to enable and disable EC500. 3. Configure the IP Deskphone extension for EC500 through off-pbx-telephone station-mapping. 4. Use the FAC to change the mobile number. User FNEs to enable/disable the feature.
Ring Again	1. Configure the FAC and FNE for enabling and disabling auto callback 2. Configure the auto-callback button in the IP Deskphone's Endpoint Editor. 3. Use FNEs to enable and disable the feature.
Priority Call	1. Configure the FAC and FNE for Priority Call. 2. Configure the IP Deskphone extension COS as "Priority Calling = Y". 3. Use the FNE to activate per-call priority calling. **Note:** An incoming priority call to Avaya Aura® digital phones/ 96xx phones triggers distinctive ringing, but the IP Deskphones do not provide distinctive ringing for an incoming priority call.

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382

Chapter 26: Feature interactions

This chapter provides information on feature interactions for IP Deskphones with SIP Software on Avaya Aura® Communication Manager.

Conf and Join softkeys

The **Conf** and **Join** soft keys on the IP Deskphone support the IP Deskphone's local 3-way conference bridge. The **Conf** and **Join** soft keys do not work with the Communication Manager system's ad-hoc conference

Call Forward All Calls and Call Forward Busy / No Answer on Communication Manager

The Communication Manager system's **Call Forward All Calls** and **Call Forward Busy/No Answer** features are recommended over the IP Deskphone's local Call Forward feature (**CallFwd** soft key) as Communication Manager handles call coverage better with its own features.

If the local CallFwd (**CallFwd** soft key) is used, it cannot be used when the same extension is logged into multiple devices (Multiple login).

Group-Page on Communication Manager

- The Communication Manager **Group-Page** feature is not supported in SIP Release 4.4.

Local 3-way conference with MOH

When the IP Deskphone's local 3-way conference is used, and one party that has Music On Hold (MOH) enabled goes on hold, all remaining conference parties hear the MOH. Use the Communication Manager ad-hoc conference feature to avoid this.

Attended transfer

To use attended transfer, set the Communication Manager parameter "SIP Endpoint Managed Transfer?" to **NO** (found on p.19 of **system-parameter feature** configuration on the Communication Manager interface).

Remote Hold

To see **Remote Hold** displayed on a far-end phone when an 11xx/12xx IP Deskphone with SIP Software places a call on hold, the Communication Manager **Direct Hold** feature must be active so that the CM can forward the hold notification to the far end. The Communication Manager **Direct Hold** is enabled by disabling Music On Hold (MOH). To disable MOH, set **Hear System Music on Hold?** to NO in the IP Deskphone's COR (Class of Restriction).

CONFERENCE_URI[n] configuration parameters

When the AVAYA_AURA_MODE_ENABLE parameter is configured as YES, the CONFERENCE_URI[n] configuration parameters are not processed.

Codec support

Communication Manager offers 4 options for codec G722:

- G.722-64K
- G.722.1-24K
- G.722.1-32K
- G.722.2

Important:

The IP Deskphones only support the G722-64K option.

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382

Chapter 27: IP Deskphone configuration parameters

Device configuration file with Avaya Aura®

This chapter describes the parameters required in the device configuration files for the 1100 Series IP Deskphones when the IP Deskphones are used on Avaya Aura®.

Note:

The **#** symbol preceding a line of text indicates a comment in the device configuration file.

Device configuration file

```
IP_OFFICE_ENABLE NO

# Enable the use of Personal Profile Manager with Avaya Aura SM/CM
ENABLE_SERVICE_PACKAGE PPM

ENABLE_3WAY_CALL YES
ADDR_BOOK_MODE LOCAL
DOD_ENABLE NO
MLPP_PRECEDENCE_ENABLE NO
TRANSFER_TYPE RFC3261
HOLD_TYPE RFC3261
REDIRECT_TYPE RFC3261

#------VMAIL
# Voice mail extension must be the actual number; the following is only
an example.
# Voice mail extension dialed when Messages key is pressed
VMAIL 33000
```

```
# Local Privacy feature disabled in favor of Calling Number Block FNE
DISABLE_PRIVACY_UI YES

#------Audio Codecs
AUDIO_CODEC1 G722
AUDIO_CODEC2 PCMU
AUDIO_CODEC3 G729
AUDIO_CODEC4 PCMA

#YES if Avaya Presence Services with Avaya Aura Session Manager/
Communication Manager are used
RPID_PRESENCE_ENABLE YES

#-----Presence
PRES_SERVER_IP <IP_address_of_Presence_Server>

#For secure calls with Aura
MKI_ENABLE NO
AVAYA_AURA_MODE_ENABLE YES

#For TLS connection with Aura
USE_DEFAULT_DEV_CERT YES
```

Related links

Avaya Aura® support for 1100 Series IP Deskphones on page 382

Part 3: IP Deskphone migration

Part III of this document provides information on how to migrate IP Deskphones in the following scenarios:

- UNIStim IP Deskphone migration from CS 1000 to Avaya Aura® on page 405
- SIP IP Deskphone migration from MCS 5200 to Avaya Aura® on page 413
- UNIStim IP Deskphone migration from CS 1000 to IP Office on page 421

Related links

UNIStim IP Deskphone migration from CS 1000 to Avaya Aura® on page 405
SIP IP Deskphone migration from MCS 5200 to Avaya Aura® on page 413
UNIStim IP Deskphone migration from CS 1000 to IP Office on page 421

Chapter 28: UNIStim IP Deskphone migration from CS 1000 to Avaya Aura®

This chapter provides information on a method to migrate IP Deskphones with UNIStim firmware from a Communication Server (CS 1000) system to Avaya Aura® by using Aura® Utility Server as a provisioning server.

Related links

IP Deskphone migration on page 404
Overview on page 405
Requirements on page 406
Before you begin on page 406
Migrating IP Deskphones with UNIStim software from CS 1000 to Avaya Aura® using Aura® Utility Server on page 407

Overview

Note:

The use of Aura® Utility Server is not mandatory; any TFTP or HTTP server can be used as a provisioning server for the file download.

It is assumed that the IP Deskphones connect to Avaya Aura® through TCP or TLS and that the default embedded device certificates are used for secure connection to Aura SM and Aura Utility Services. For more information on the default certificates, see Embedded Device Certificates on page 390.

Note:

Avaya recommends that a single IP Deskphone of each type be migrated first to verify that the setup is correct.

For large installations, it is not recommended that all IP Deskphones be migrated at the same time.

This chapter does not describe how to configure CS 1000, Avaya Aura®, or third-party applications such as the DHCP and TFTP servers. For this information, refer to the appropriate product documentation.

This chapter does not provide information on how to migrate the CS 1000 users and their profiles over to the Avaya Aura® system. If using this procedure to perform the migration, then the IP Deskphone users must manually input their login and password after migration in order to register with Avaya Aura® and obtain telephony services. Configuring IP Deskphone auto-registration requires knowledge of which phones belong to which users and the passwords for all users; this is out of scope of this procedure.

Related links

UNIStim IP Deskphone migration from CS 1000 to Avaya Aura® on page 405

Requirements

Ensure that the following requirements for migration have been implemented:

- The IP Deskphones are running UNIStim Release 3.3 firmware release or newer.

  The latest firmware is recommended - 062xC8Q.
- DHCP is enabled on the IP Deskphones .

  The DHCP option should be set to YES in the **Network Configuration** menu.
- Auto Provisioning for the Provisioning Server is enabled on the IP Deskphones.

  Check the **Provision Server** option check box in the **Network Configuration > Auto** menu.
- There is access to the Avaya Aura® Utility Services through a web interface.
- There are no network outages during migration.

  The DHCP server, the CS 1000 system, and Avaya Aura® are available in the network.
- There are no power outages during the migration.

  A power outage during the software upgrade can cause corruption of the IP Deskphone software. As a result, the IP Deskphone might not be able to start up and may require repair.

Related links

UNIStim IP Deskphone migration from CS 1000 to Avaya Aura® on page 405

Before you begin

1. Obtain the SIP software images for the IP Deskphones.

   SIP4.4 or later software release is recommended.
2. Obtain a Network Locked License file.

For direct connection to Avaya Aura® Communication ManagerM/Session Manager, a license with no tokens is needed. For connection through Secure Router, a license with one token is needed.

3. Create a device configuration file with the configuration options required for connecting the IP Deskphones to Avaya Aura®.

   Prepare all other SIP-related files to configure your IP Deskphones properly, such as licenses, images, and dial plan.

Important:

If TLS is used for secure connection to Aura® Session Manager, the following option must be added to the device configuration file:

USE_DEFAULT_DEV_CERT YES

Related links

UNIStim IP Deskphone migration from CS 1000 to Avaya Aura® on page 405

Migrating IP Deskphones with UNIStim software from CS 1000 to Avaya Aura® using Aura® Utility Server

About this task

If you have IP Deskphones running UNIStim firmware on a CS 1000 system, and you want to migrate the IP Deskphones to Avaya Aura® with SIP software on the IP Deskphones, use the following procedure.

Procedure

1. Create configuration files for the IP Deskphones with UNIStim firmware, as shown in the following example for the 1140E IP Deskphone.

   Example of configuration file for 1140E IP Deskphone:

   1140eSIP.cfg:

   `[FW]`

   `DOWNLOAD_MODE AUTO`

   `VERSION 04.04.09.00` <— version should be taken from the SIP software file name

   `PROTOCOL HTTP`

   `FILENAME SIP1140e04.04.09.00.bin` <— specify the SIP software file name here

2. Create provisioning files for the IP Deskphones with the following content. The following example is for the 1140E IP Deskphone; the file content for the other IP Deskphone models is similar.

   Example of configuration file for 1140E IP Deskphone:

1140eSIP.cfg:

`[FW]`

`DOWNLOAD_MODE AUTO`

`VERSION 04.04.09.00` <— version should be taken from the SIP software file name

`PROTOCOL HTTP`

`FILENAME SIP1140e04.04.09.00.bin` <— specify the SIP software file name here

`[DEVICE_CONFIG]`

`DOWNLOAD_MODE FORCED`

`FILENAME device_config.dat` <— name of the device configuration file

`PROTOCOL HTTP`

`[Licensing]`

`DOWNLOAD_MODE FORCED`

`VERSION 0002`

`PROTOCOL HTTP`

`FILENAME ipctoken.cfg` <— name of the license file

Additional sections can be specified in the provisioning files if there is a need to upload other files such as dialing plan and languages.

3. Add software images, provisioning files, device configuration files and other files intended for the IP Deskphones to a ZIP archive.

   Warning:

   Do not create any folders in the archive. These folders will not be copied to the Utility Server.

4. Upload the zip archive with provisioning files to the Avaya Utility Services.

   a. Connect to the Avaya Utility Server through a Web browser.

      The following page appears after logging in.

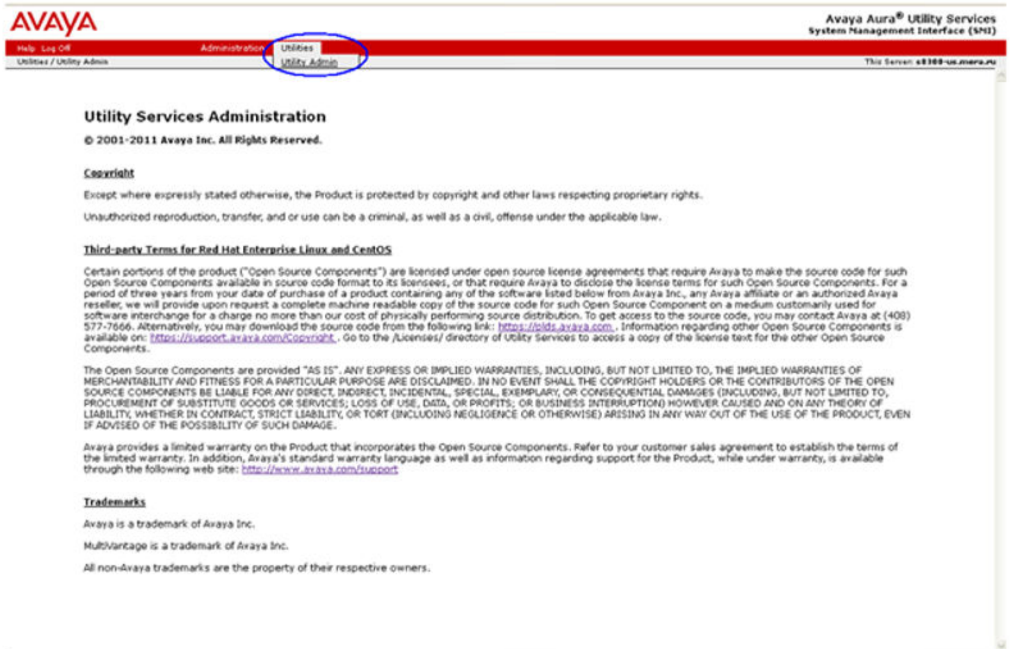


Figure 93: Utility Services main page

b. In the menu at the top of the page, click **Utilities > Utility Admin.**

The **Utility Services Administration** page opens.

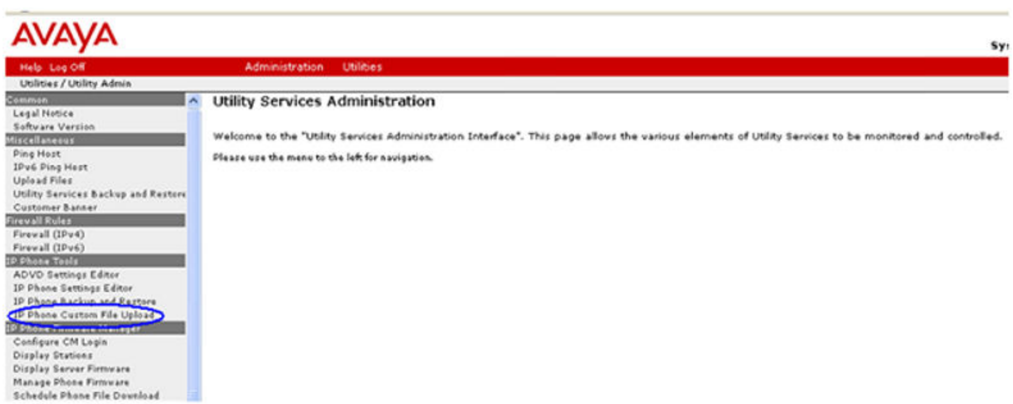


Figure 94: Utility Services Administration

c. In the menu list on the left, click **IP Phone Tools > IP Phone Custom File Upload**.

The **IP Phone Custom File Upload** page opens.

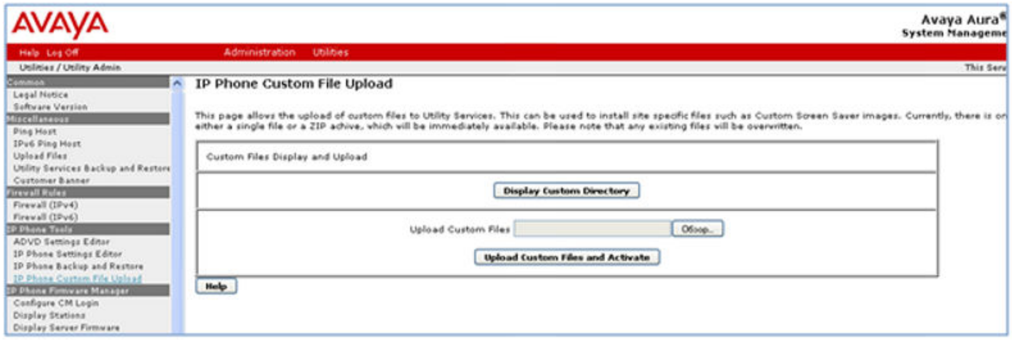


Figure 95: IP Phone Custom File Upload page

d. Click **Browse** and navigate to the created ZIP archive containing the provisioning files.

e. Click the **Upload Custom Files and Activate** button.

f. Return to the **IP Phone Custom File Upload** page after the files have uploaded.

g. Click **Display Custom Directory** and make sure that all files from the zip archive are listed.

Note:

If some of the files already exist on the Utility Server, then they are replaced with the uploaded files.

5. Configure the DHCPv4 server.

The DHCP server must provide option 66 with the IP address of the Avaya Aura Utility Server that will be used as a provisioning server. This functionality can be achieved by providing different DHCP options based on Vendor Class ID. The IP Deskphones with UNIStim firmware report Vendor Class ID “Nortel-i2004-A” or “Nortel-i2004-B”. The IP Deskphones with SIP software report Vendor Class ID “Nortel-SIP-Phone-A”.

The following is an example of an appropriate configuration file for a Linux dhcpd DHCPv4 server. Please refer to the documentation of your DHCP server on how to configure the appropriate configuration file.

```
dhcpd.conf:
.....
class "unistimA" {
     match if substring(option vendor-class-identifier, 0, 14) = "Nortel-i2004-A";
     option tftp-server-name "http://<Avaya Aura Utility Server IP address>/";
    }
class "unistimB" {
     match if substring(option vendor-class-identifier, 0, 14) = "Nortel-i2004-B";
     option tftp-server-name "http://<Avaya Aura Utility Server IP address>/ ";
    }
class "sigma" {
      match if substring(option vendor-class-identifier, 0, 18) = "Nortel-SIP-
Phone-A";
     option tftp-server-name "http://<Avaya Aura Utility Server IP address>/ ";
.....
pool {
range 192.168.xxx.xxx 192.168.xxx.xxx;
allow members of "unistimA";
allow members of "unistimB";
allow members of "sigma";.
}
.....
```

Note:

If there is more than one DHCP server/utility server, the described process must be performed on each DHCP/Utility server, according to the migration plan.

Note:

The IP address of the Provisioning Server can also be pushed to the IP Deskphones with UNIStim firmware using the Nortel i2004-B option and the “prov=” argument of the provisioning info block. Remove the “prov=” argument from the info block on your DHCP server.

Important:

Once the DHCP configuration is put in place, there is no way to prevent random phones migrating to the Avaya Aura environment at an unexpected time due to rebooting caused by a power outage or other reason.

6. Force a reboot of the IP Deskphones by running the `isetResetAll` command in the Signaling Server shell.

Result

1. The IP Deskphone reboots.
2. During bootup, the IP Deskphone sends a DHCP request with Vendor Class Id “Nortel-i2004-A” or “Nortel-i2004-B”. The DHCP server sends back a DHCP response with the IP Deskphone’s IP address and the URL of the Avaya Aura Utility server (in DHCP option 66).
3. The IP Deskphone downloads the SIP software from the Avaya Aura Utility server and upgrades. When the upgrade is completed, the IP Deskphone automatically reboots again.

   Warning:

   A power outage at this stage may cause firmware corruption. If this happens, the IP Deskphone may not be able to boot up, and it may be necessary to return the IP Deskphone for repair.
4. The IP Deskphone starts and downloads the device configuration file, images, licenses, languages, and so on, from the Avaya Aura Utility server.
5. When configuration is complete, the IP Deskphone automatically reboots.
6. The IP Deskphone is ready to use.

Note:

If auto login is not configured in the configuration files, the IP Deskphone displays the login screen. The IP Deskphone user must enter a valid login and password in order to register on Avaya Aura.

Related links

UNIStim IP Deskphone migration from CS 1000 to Avaya Aura® on page 405

Chapter 29: SIP IP Deskphone migration from MCS 5200 to Avaya Aura®

This chapter provides information on a method to migrate 1120E and 1140E IP Deskphones with SIP software from an MCS 5200 server to Avaya Aura® by using Aura® Utility Services as a provisioning server.

Related links

IP Deskphone migration on page 404
Overview on page 413
Requirements on page 414
Before you begin on page 414
Migrating IP Deskphones with SIP software from MCS 5200 to Avaya Aura® using Aura® Utility Server on page 415

Overview

It is assumed that the IP Deskphones connect to Avaya Aura® through TCP or TLS and that the default embedded device certificates are used for secure connection to Aura SM and Aura Utility Services. For more information on the default certificates, see Embedded Device Certificate on page 390.

Note:

Avaya recommends that a single IP Deskphone of each type be migrated first to verify that the setup is correct.

For large installations, it is not recommended that all IP Deskphones be migrated at the same time.

This chapter does not describe how to configure MCS 5200, Avaya Aura®, or third-party applications such as the DHCP and TFTP servers. For this information, refer to the appropriate product documentation.

This chapter does not provide information on how to migrate the MCS 5200 users and their profiles over to the Avaya Aura® system. If using this procedure to perform the migration, then the IP Deskphone users must manually input their login and password after migration in order to register with Avaya Aura® and obtain telephony services. Configuring IP Deskphone auto-registration requires knowledge of which phones belong to which users and the passwords for all users; this is out of scope of this procedure.

Related links

SIP IP Deskphone migration from MCS 5200 to Avaya Aura® on page 413

Requirements

Ensure that the following requirements for migration have been implemented:

- DHCP is enabled on the IP Deskphones .

  The DHCP option should be set to YES in the **Network Configuration** menu.
- Auto Provisioning for the Provisioning Server is enabled on the IP Deskphones.

  Check the **Provision Server** option check box in the **Network Configuration > Auto** menu.
- There is access to the Avaya Aura® Utility Services through a web interface.
- There are no network outages during migration.

  The DHCP server, the CS 1000 system, and Avaya Aura® are available in the network.
- There are no power outages during the migration.

  A power outage during the software upgrade can cause corruption of the IP Deskphone software. As a result, the IP Deskphone might not be able to start up and may require repair.

Related links

SIP IP Deskphone migration from MCS 5200 to Avaya Aura® on page 413

Before you begin

1. Obtain the SIP software images for the IP Deskphones.

   SIP4.4 or later software release is recommended.
2. Obtain a Network Locked License file.

   For direct connection to Avaya Aura® Communication ManagerM/Session Manager, a license with no tokens is needed. For connection through Secure Router, a license with one token is needed.
3. Create a device configuration file with the configuration options required for connecting the IP Deskphones to Avaya Aura®.

   Prepare all other SIP-related files to configure your IP Deskphones properly, such as licenses, images, and dial plan.

Important:

If TLS is used for secure connection to Aura® Session Manager, the following option must be added to the device configuration file:

USE_DEFAULT_DEV_CERT YES

Related links

SIP IP Deskphone migration from MCS 5200 to Avaya Aura® on page 413

Migrating IP Deskphones with SIP software from MCS 5200 to Avaya Aura® using Aura® Utility Server

About this task

If you have IP Deskphones running SIP software on an MCS 5200 system, and you want to migrate the IP Deskphones to Avaya Aura® , use the following procedure.

Procedure

1. Create provisioning files for the 1120E and 1140E IP Deskphones with the following content:.

   Configuration file for 1140E IP Deskphone:

   1140eSIP.cfg:

   `[FW]`

   `DOWNLOAD_MODE AUTO`

   `VERSION 04.04.09.00` <— version should be taken from the SIP software file name

   `PROTOCOL HTTP`

   `FILENAME SIP1140e04.04.09.00.bin` <— specify the SIP software file name here

   `[DEVICE_CONFIG]`

   `DOWNLOAD_MODE FORCED`

   `FILENAME device_config.dat` <— name of the device configuration file

   `PROTOCOL HTTP`

   `[Licensing]`

   `DOWNLOAD_MODE FORCED`

   `VERSION 0002`

`PROTOCOL HTTP`

`FILENAME ipctoken.cfg` <— name of the license file

Configuration file for 1120E IP Deskphone:

1120eSIP.cfg:

`[FW]`

`DOWNLOAD_MODE AUTO`

`VERSION 04.04.09.00` <— version should be taken from the SIP software file name

`PROTOCOL HTTP`

`FILENAME SIP1120e04.04.09.00.bin` <— specify the SIP software file name here

`[DEVICE_CONFIG]`

`DOWNLOAD_MODE FORCED`

`FILENAME device_config.dat` <— name of the device configuration file

`PROTOCOL HTTP`

`[Licensing]`

`DOWNLOAD_MODE FORCED`

`VERSION 0002`

`PROTOCOL HTTP`

`FILENAME ipctoken.cfg` <— name of the license file

Additional sections can be specified in the provisioning files if there is a need to upload other files such as dialing plan and languages.

2. Add software images, provisioning files, device configuration files and other files intended for the IP Deskphones to a ZIP archive.

   Warning:

   Do not create any folders in the archive. These folders will not be copied to the Utility Server.

3. Upload the zip archive with provisioning files to the Avaya Utility Services.

   a. Connect to the Avaya Utility Server through a Web browser.

      The following page appears after logging in.

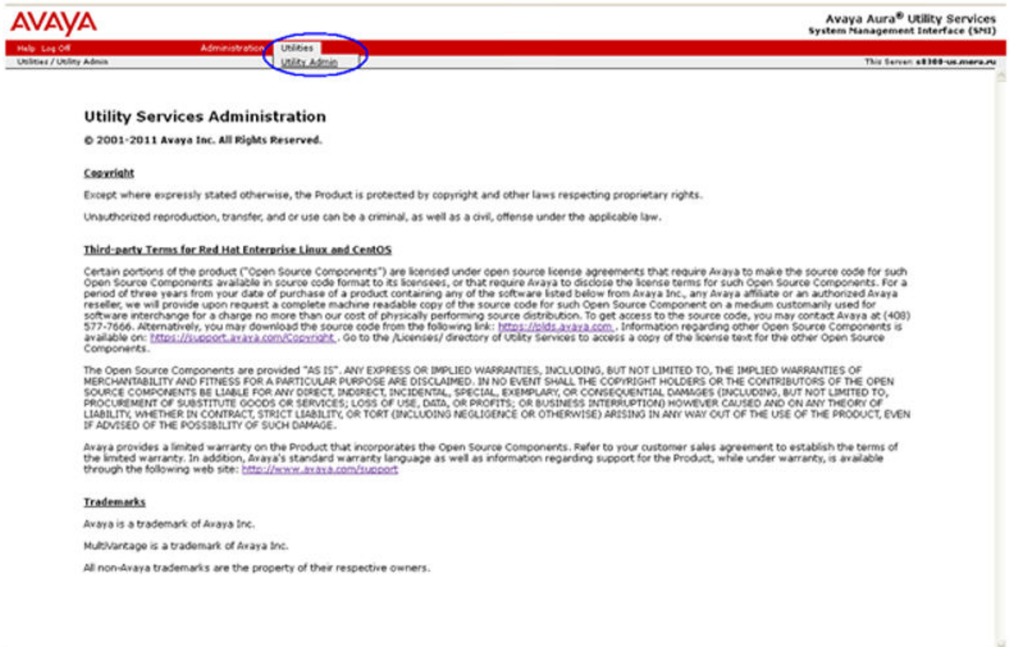


Figure 96: Utility Services main page

b. In the menu at the top of the page, click **Utilities > Utility Admin.**

The **Utility Services Administration** page opens.

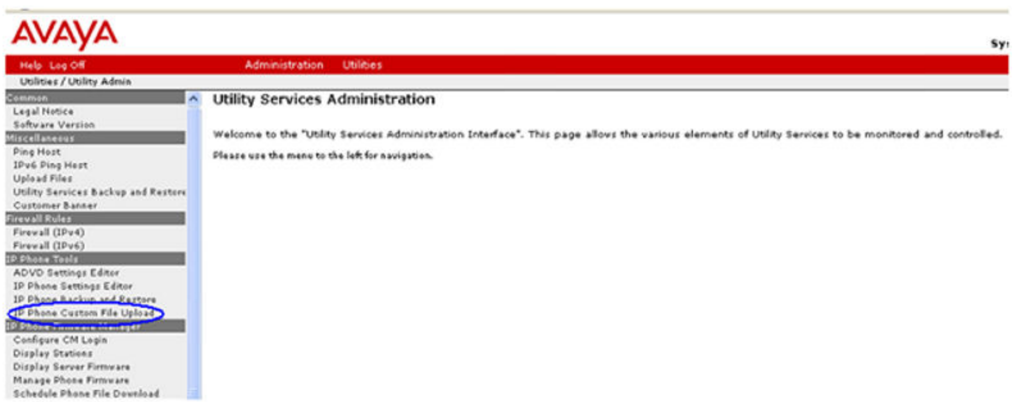


Figure 97: Utility Services Administration

c. In the menu list on the left, click **IP Phone Tools > IP Phone Custom File Upload**.

The **IP Phone Custom File Upload** page opens.

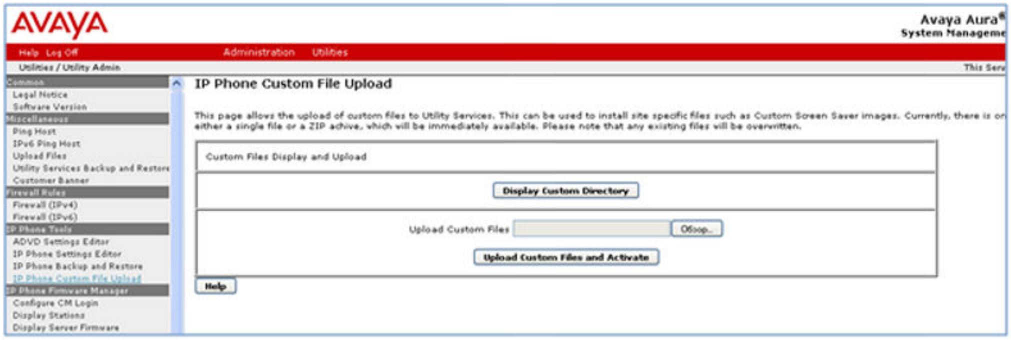


Figure 98: IP Phone Custom File Upload page

d. Click **Browse** and navigate to the created ZIP archive containing the provisioning files.

e. Click the **Upload Custom Files and Activate** button.

f. Return to the **IP Phone Custom File Upload** page after the files have uploaded.

g. Click **Display Custom Directory** and make sure that all files from the zip archive are listed.

Note:

If some of the files already exist on the Utility Server, then they are replaced with the uploaded files.

4. Configure the DHCPv4 server.

The DHCP server must provide option 66 with IP address of the Avaya Aura Utility Server which will be used as a provisioning server. This functionality can be achieved by providing different DHCP options based on Vendor Class ID. The IP Deskphones with SIP software report Vendor Class ID “Nortel-SIP-Phone-A”.

The following is an example of an appropriate configuration file for a Linux dhcpd DHCPv4 server. Please refer to the documentation of your DHCP server on how to configure the appropriate configuration file.

```
dhcpd.conf:
.....
class "sigma" {
       match if substring(option vendor-class-identifier, 0, 18) = “Nortel-SIP-Phone-A”;
       option tftp-server-name “http://<Avaya Aura Utility Server IP address>/ ";
.....
pool {
           range 192.168.xxx.xxx 192.168.xxx.xxx;
           allow members of "sigma";
}
.....
```

Note:

If there is more than one DHCP server/utility server, the described process must be performed in each DHCP/Utility server, according to the migration plan.

Important:

Once the DHCP configuration is put in place, there is no way to prevent “random” phones migrating to the Avaya Aura environment at an unexpected time due to rebooting caused by a power outage or other reason.

5. Force a reboot of the IP Deskphones using one of the following methods.
   - Unplug and re-plug the power supply of the IP Deskphone.
   - If POE is used, shutdown and restart the ports on the network switch(es) to which the phones are connected.
   - If the IP Deskphones are configured to regularly check for updates, force a reboot of the phones by changing one of the following parameters:
     - SRTP_ENABLED
     - SFTP_READ_PATTERNS
     - SRTP_WRITE_PATTERNS
     - SNTP_ENABLE
     - IPV6_ENABLE
     - ENABLE_UPDATE
     - DOD_ENABLE
     - MAX_APPEARANCE
     - USE_PUBLISH_FOR_PRESENCE

     The IP Deskphone reboots when it receives the updated configuration file during the next check for updates.

     Make the change in the device configuration file which is stored on the MCS 5200 Provisioning Server. Specify a temporary value for the chosen parameter. The final value of this parameter can be specified in the device configuration file which is uploaded to Avaya Aura Utility Server; for example, MAX_APPEARANCE 3.

Result

1. The IP Deskphone reboots.
2. During bootup, the IP Deskphone sends a DHCP request with Vendor Class ID “Nortel-SIP-Phone-A”. . The DHCP server sends back a DHCP response with the IP Deskphone’s IP address and the URL of the HTTP provisioning server (in DHCP option 66).
3. The IP Deskphone downloads the SIP software from the Avaya Aura Utility server and upgrades. When the upgrade is completed, the IP Deskphone automatically reboots again.

Warning:

A power outage at this stage may cause firmware corruption. If this happens, the IP Deskphone may not be able to boot up, and it may be necessary to return the IP Deskphone for repair.

4. The IP Deskphone starts and downloads the device configuration file, images, licenses, languages, and so on, from the Avaya Aura Utility server.
5. When configuration is complete, the IP Deskphone automatically reboots.
6. The IP Deskphone is ready to use.

Note:

If auto login is not configured in the configuration files, the IP Deskphone displays the login screen. The user must enter a valid login and password in order to register on Avaya Aura.

Related links

SIP IP Deskphone migration from MCS 5200 to Avaya Aura® on page 413

Chapter 30: UNIStim IP Deskphone migration from CS 1000 to IP Office

This chapter provides information on a method to migrate IP Deskphones with UNIStim firmware from a Communication Server (CS 1000) system to IP Office.

Related links

Overview

It is assumed that the IP Deskphones connect to IP Office through TCP.

Note:

Avaya recommends that a single IP Deskphone of each type be migrated first to verify that the setup is correct.

For large installations, it is not recommended that all IP Deskphones be migrated at the same time.

This chapter does not describe how to configure CS 1000, IP Office, or third-party applications such as the DHCP and TFTP servers. For this information, refer to the appropriate product documentation.

This chapter does not provide information on how to migrate the CS 1000 users and their profiles over to IP Office. If using this procedure to perform the migration, then the IP Deskphone users must manually input their login and password after migration in order to register on IP Office and obtain telephony services. Configuring IP Deskphone auto-registration requires knowledge of which IP Deskphones belong to which users and the passwords for all users; this is out of scope of this procedure.

Related links

UNIStim IP Deskphone migration from CS 1000 to IP Office on page 421

Requirements

Ensure that the following requirements for migration have been implemented:

- The IP Deskphones are running UNIStim Release 3.3 firmware release or newer.

  The latest firmware is recommended - 062xC8Q.
- DHCP is enabled on the IP Deskphones .

  The DHCP option should be set to YES in the **Network Configuration** menu.
- Auto Provisioning for the Provisioning Server is enabled on the IP Deskphones.

  Check the **Provision Server** option check box in the **Network Configuration > Auto** menu.
- There is access to Avaya IP Office Manager.
- There are no network outages during migration.

  The DHCP server, the CS 1000 system, and Avaya IP Office are available in the network.
- There are no power outages during the migration.

  A power outage during the software upgrade can cause corruption of the IP Deskphone software. As a result, the IP Deskphone might not be able to start up and may require repair.

Related links

UNIStim IP Deskphone migration from CS 1000 to IP Office on page 421

Before you begin

Obtain the SIP software images for the IP Deskphones. SIP Software Release 4.4 or later is recommended.

Related links

UNIStim IP Deskphone migration from CS 1000 to IP Office on page 421

Migrating IP Deskphones with UNIStim firmware from CS 1000 to IP Office

About this task

If you have IP Deskphones running UNIStim firmware on a CS 1000 system, and you want to migrate the IP Deskphones to Avaya IP Office, use the following procedure.

Procedure

1. Create configuration files for the 1120E and 1140E IP Deskphones with UNIStim firmware, with the following content.

   Configuration file for 1140E IP Deskphone (1140e.cfg):

   1140eSIP.cfg:

   `[FW]`

   `DOWNLOAD_MODE AUTO`

   `VERSION 04.04.09.00` <— version should be taken from the SIP software file name

   `PROTOCOL HTTP`

   `FILENAME SIP1140e04.04.09.00.bin` <— specify the SIP software file name here

   Configuration file for 1120E IP Deskphone (1120e.cfg):

   1120eSIP.cfg:

   `[FW]`

   `DOWNLOAD_MODE AUTO`

   `VERSION 04.04.09.00` <— version should be taken from the SIP software file name

   `PROTOCOL HTTP`

   `FILENAME SIP1120e04.04.09.00.bin` <— specify the SIP software file name here

2. Create provisioning files for the IP Deskphones with the following content. The following example is for the 1140E IP Deskphone; the file content for the other IP Deskphone models is similar.

   Example of configuration file for 1140E IP Deskphone:

   1140eSIP.cfg:

   `[FW]`

   `DOWNLOAD_MODE AUTO`

   `VERSION 04.03.12.00` <— version should be taken from the SIP software file name

```
PROTOCOL HTTP
FILENAME SIP1140e04.04.09.00.bin <— specify the SIP software file name here
```

```
[DEVICE_CONFIG]
DOWNLOAD_MODE FORCED
FILENAME device_config.dat <— name of the device configuration file
PROTOCOL HTTP
```

```
[Licensing]
DOWNLOAD_MODE FORCED
VERSION 0002
PROTOCOL HTTP
FILENAME ipctoken.cfg <— name of the license file
```

Additional sections can be specified in the provisioning files if there is a need to upload other files such as dialing plan and languages.

3. Create a temporary folder on the hard drive of your PC. Add the software images, provisioning files, device configuration files and other files intended for the IP Deskphones to this folder.

   Important:

   Do not create any subfolders in the temporary folder.

4. Upload the folder content to the Avaya IP Office Manager.
   - Run IP Office Manager and log in.
   - In the IP Office Manager main window, click **File > Advanced > Embedded File Manager…**.

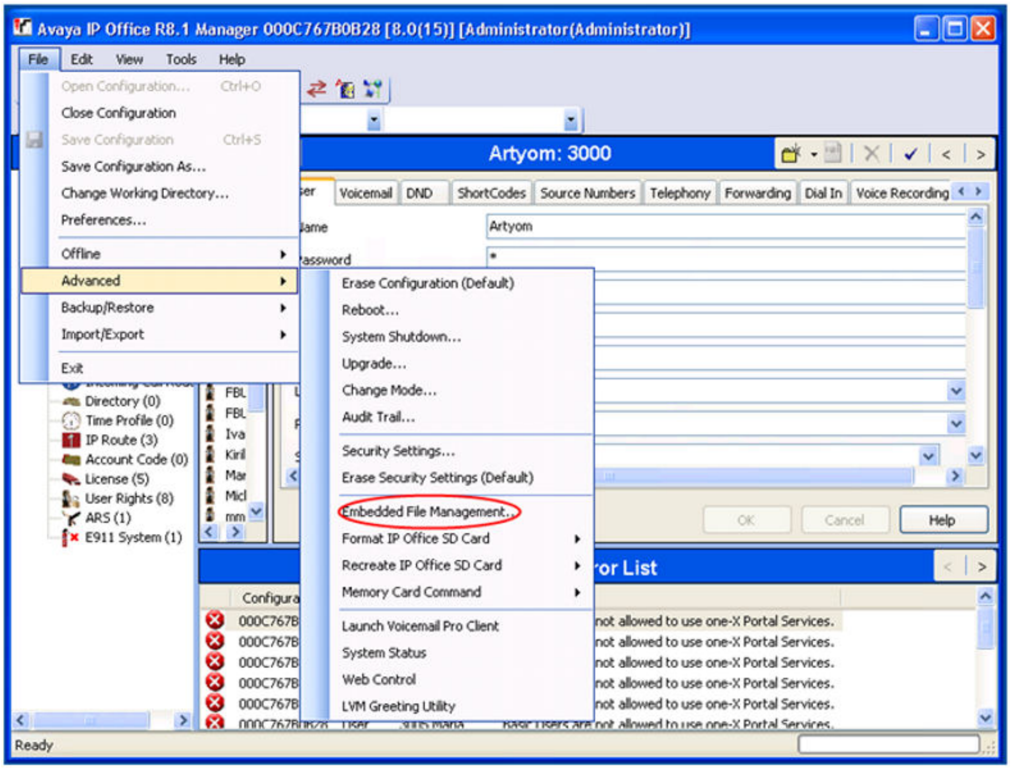


Figure 99: IP Office Manager – main window

- Select IP Office system and log in.

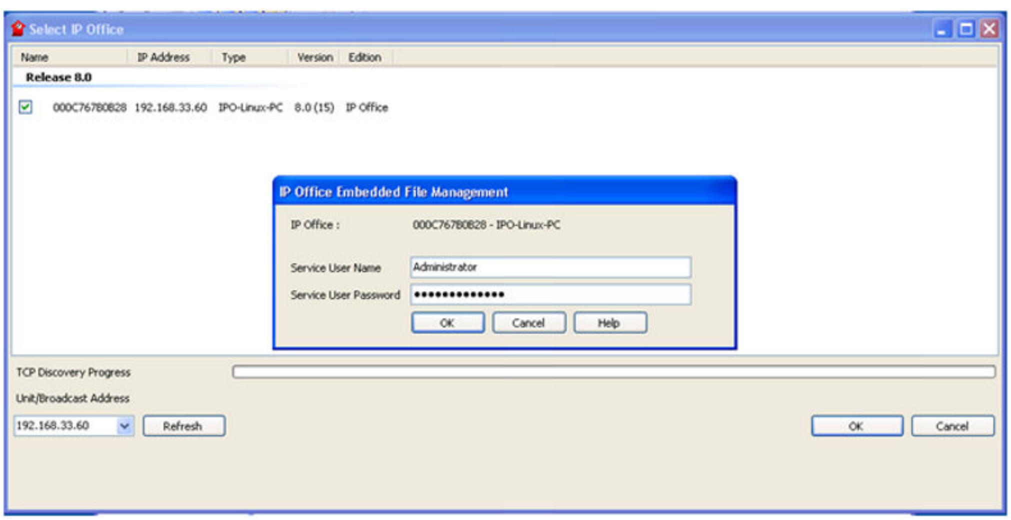


Figure 100: Select IP Office window

- Navigate to the **Disk > system > primary** folder in the Embedded File Management window.

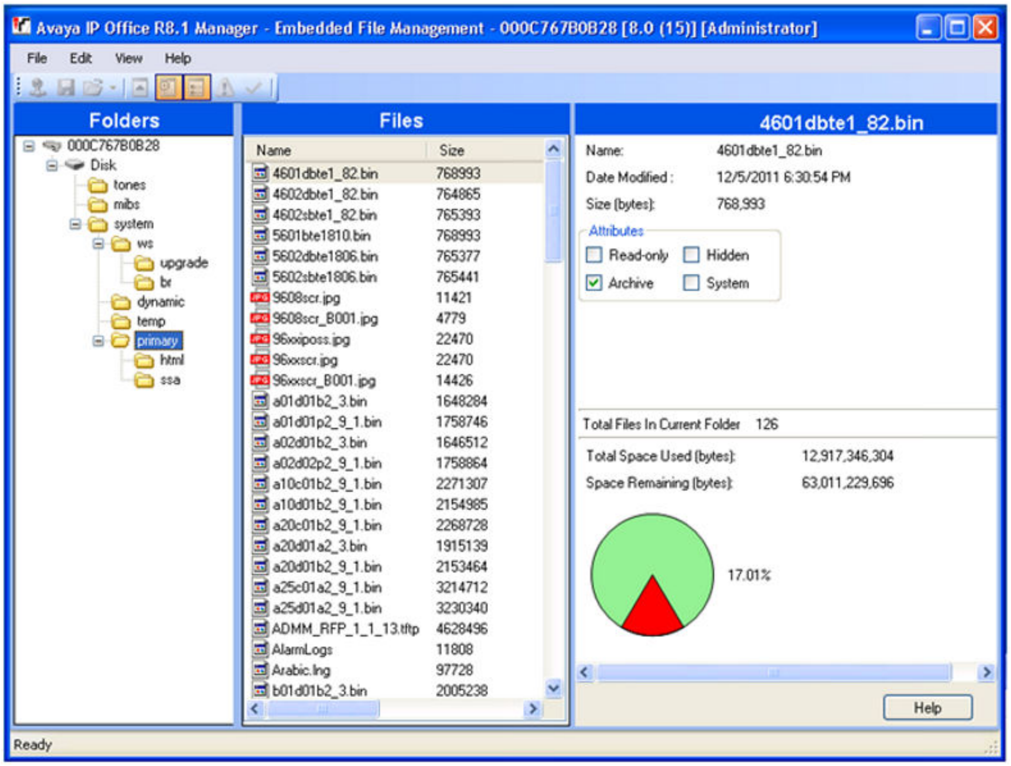


Figure 101: IP Office manager – Embedded File Management window

- In Windows Explorer, open the folder that was created in Step 3.
- Select the created configuration files in Windows Explorer and drag-and-drop them to the **Disk > system > primary** folder in the Embedded File Management window.

5. Configure the DHCPv4 server.

   The DHCP server must provide option 66 with the IP address of the IP Office that will be used as a provisioning server. This functionality can be achieved by providing different DHCP options based on Vendor Class ID. The IP Deskphones with UNIStim firmware report Vendor Class ID “Nortel-i2004-A” or “Nortel-i2004-B”. The IP Deskphones with SIP software report Vendor Class ID “Nortel-SIP-Phone-A”.

The following is an example of an appropriate configuration file for a Linux dhcpd DHCPv4 server. Please refer to the documentation of your DHCP server on how to configure the appropriate configuration file.

```
dhcpd.conf:
.....
class "unistimA" {
     match if substring(option vendor-class-identifier, 0, 14) = "Nortel-i2004-A";
     option tftp-server-name "http://<IP Office IP address>/";
    }
class "unistimB" {
     match if substring(option vendor-class-identifier, 0, 14) = "Nortel-i2004-B";
     option tftp-server-name "http://<IP Office IP address>/ ";
    }
class "sigma" {
      match if substring(option vendor-class-identifier, 0, 18) = "Nortel-SIP-
Phone-A";
     option tftp-server-name "http://<IP Office IP address>/ ";
.....
pool {
range 192.168.xxx.xxx 192.168.xxx.xxx;
allow members of "unistimA";
allow members of "unistimB";
allow members of "sigma";.
}
.....
```

Note:

If there is more than one DHCP server/utility server, the described process must be performed on each DHCP/Utility server, according to the migration plan.

Note:

The IP address of the Provisioning Server can also be pushed to the IP Deskphones with UNIStim firmware using the Nortel i2004-B option and the “prov=” argument of the provisioning info block. Remove the “prov=” argument from the info block on your DHCP server.

Important:

Once the DHCP configuration is put in place, there is no way to prevent random phones migrating to the Avaya Aura environment at an unexpected time due to rebooting caused by a power outage or other reason.

6. Force a reboot of the IP Deskphones by running the `isetResetAll` command in the Signaling Server shell.

Result

1. The IP Deskphone reboots.
2. During bootup, the IP Deskphone sends a DHCP request with Vendor Class ID “Nortel-i2004-A” or “Nortel-i2004-B”. The DHCP server sends back a DHCP response with the IP Deskphone’s IP address and the URL of the IP Office server (in DHCP option 66).
3. The IP Deskphone downloads the SIP software from the IP Office server and upgrades. When the upgrade is completed, the IP Deskphone automatically reboots again.

   Warning:

   A power outage at this stage may cause firmware corruption. If this happens, the IP Deskphone may not be able to boot up, and it may be necessary to return the IP Deskphone for repair.
4. The IP Deskphone starts and downloads the device configuration file, images, licenses, languages, and so on, from the Avaya Aura Utility server.
5. When configuration is complete, the IP Deskphone automatically reboots.
6. The IP Deskphone is ready to use.

Note:

If auto login is not configured in the configuration files, the IP Deskphone displays the login screen. The IP Deskphone user must enter a valid login and password in order to register on IP Office.

Related links

UNIStim IP Deskphone migration from CS 1000 to IP Office on page 421

Appendix A: User provisioning using System Manager 6.3 FP2

This appendix describes how to add an IP Deskphone user to Avaya Aura® using System Manager 6.3 FP2.

Related links

Adding an IP Deskphone user to Avaya Aura® using System Manager 6.3 FP2 on page 429

Adding an IP Deskphone user to Avaya Aura® using System Manager 6.3 FP2

1. Open a browser and navigate to the System Manager (SMGR) login page, as shown in the following figure.

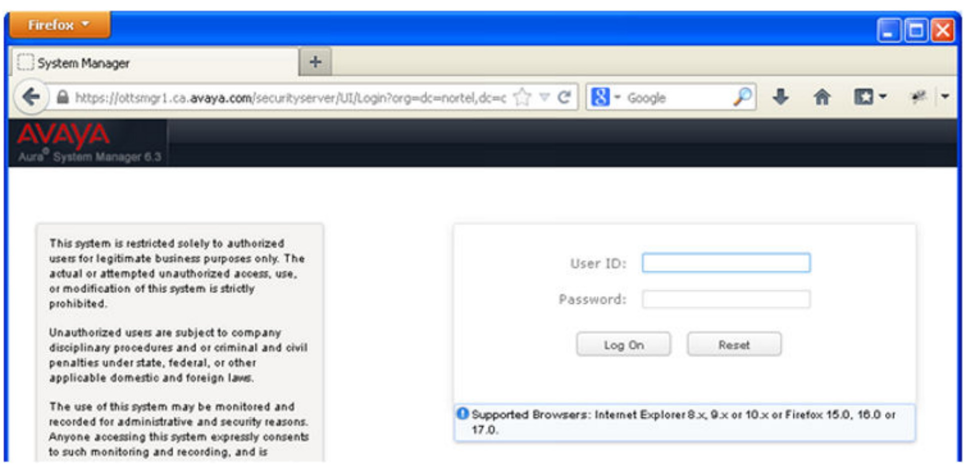


Figure 102: System Manager login page

2. Enter your User ID and password and click **Log On**.

   The **System Manager** front page opens, as shown in the following figure.

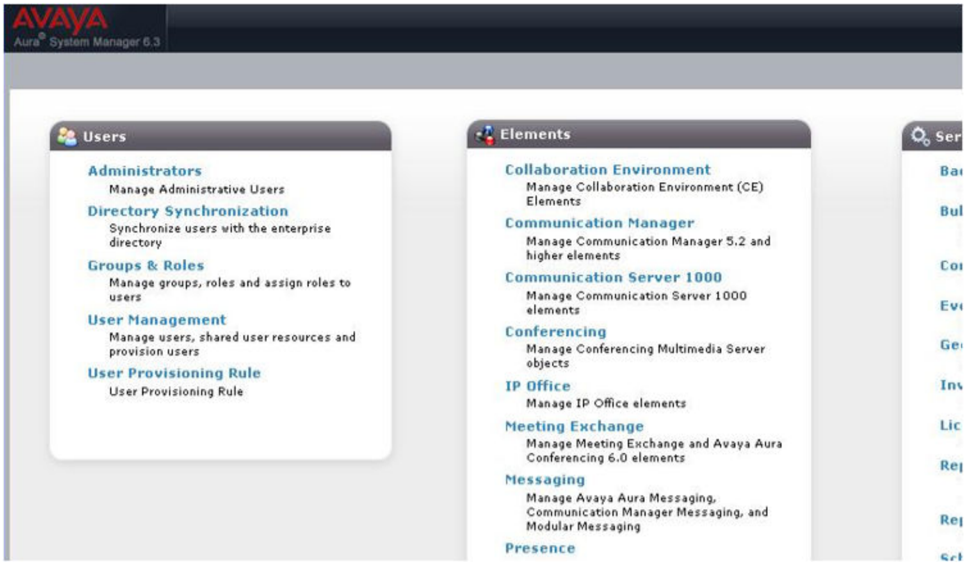


Figure 103: System Manager front page

3. In the **Users** pane on the left, click **User Management**.
4. Click **Manage Users**, and then click **New**, as shown in the following figure.

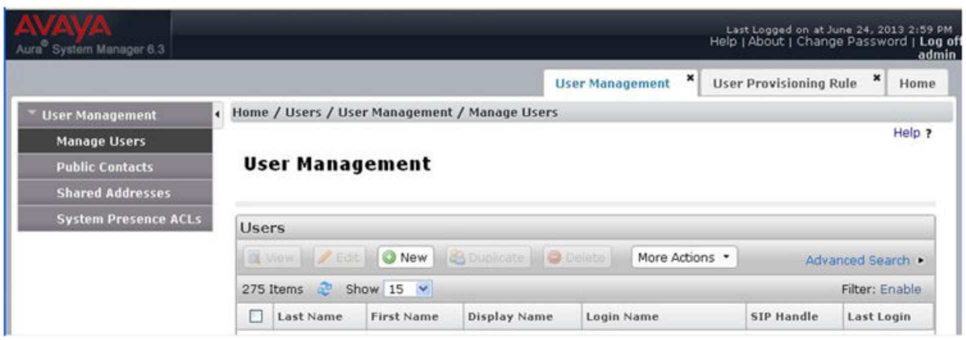


Figure 104: User Management page

5. On the **Identity** tab, shown in the following figure, enter the user information. The minimum information required is **Last Name**, **First Name**, and **Login Name**.

   The **Login Name** format is extension_number@<domain>; for example, 4655@mycompany.com

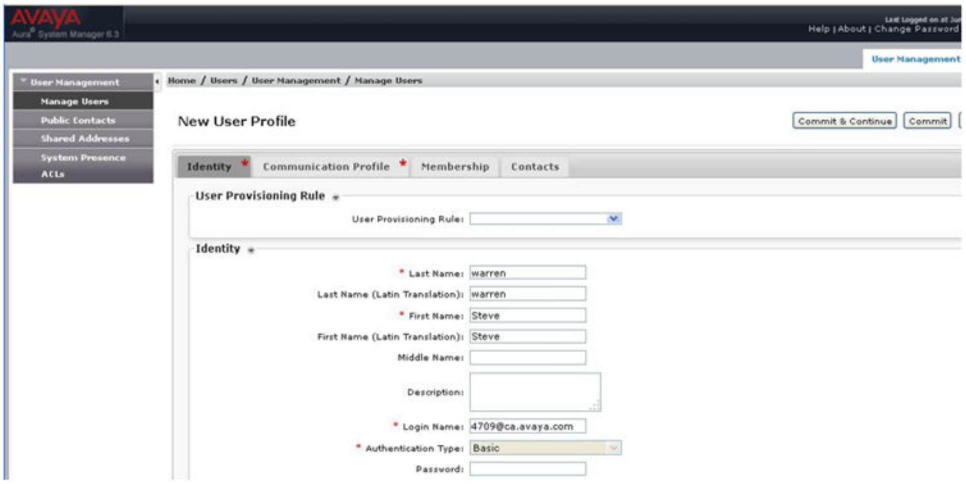


Figure 105: System Manager New User Profile page

6. In the upper-right corner, click **Commit & Continue**.
7. Click the **Communication Profile** tab.

   The **Communication Profile** window opens, as shown in the following figure.

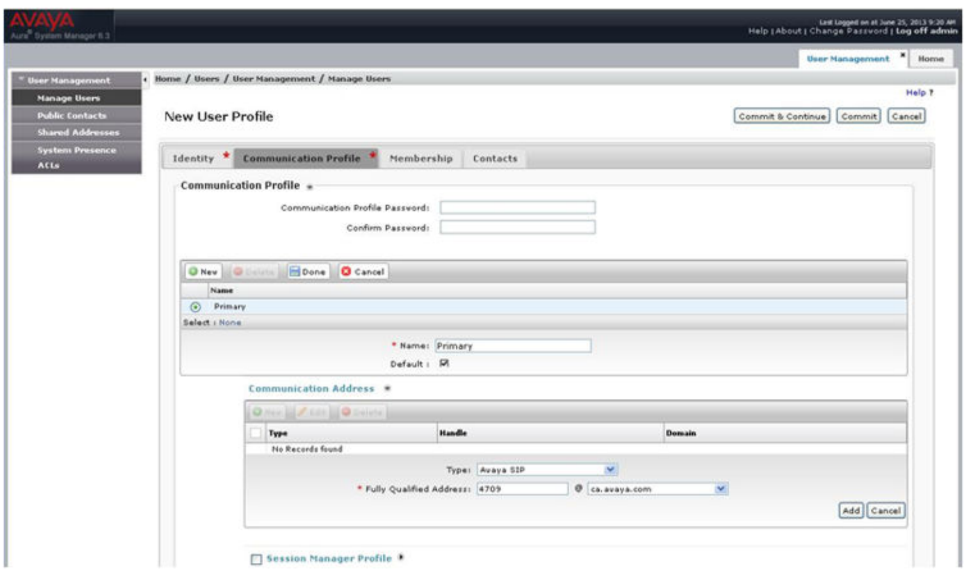


Figure 106: Communication Profile tab

8. In the **Communication Profile** pane, in the **Communication Profile Password** field, enter the password that the user will input to log into the IP Deskphone.

   In the **Confirm Password** field, enter the password again.
9. In the **Communication Address** pane, click **New**.
10. Enter the Fully Qualified Address (for example 4655@mycompany.com), and click **Add**.
11. Scroll down the **Communication Profile** page to the **Session Manager Profile** section, as shown in the following figure.

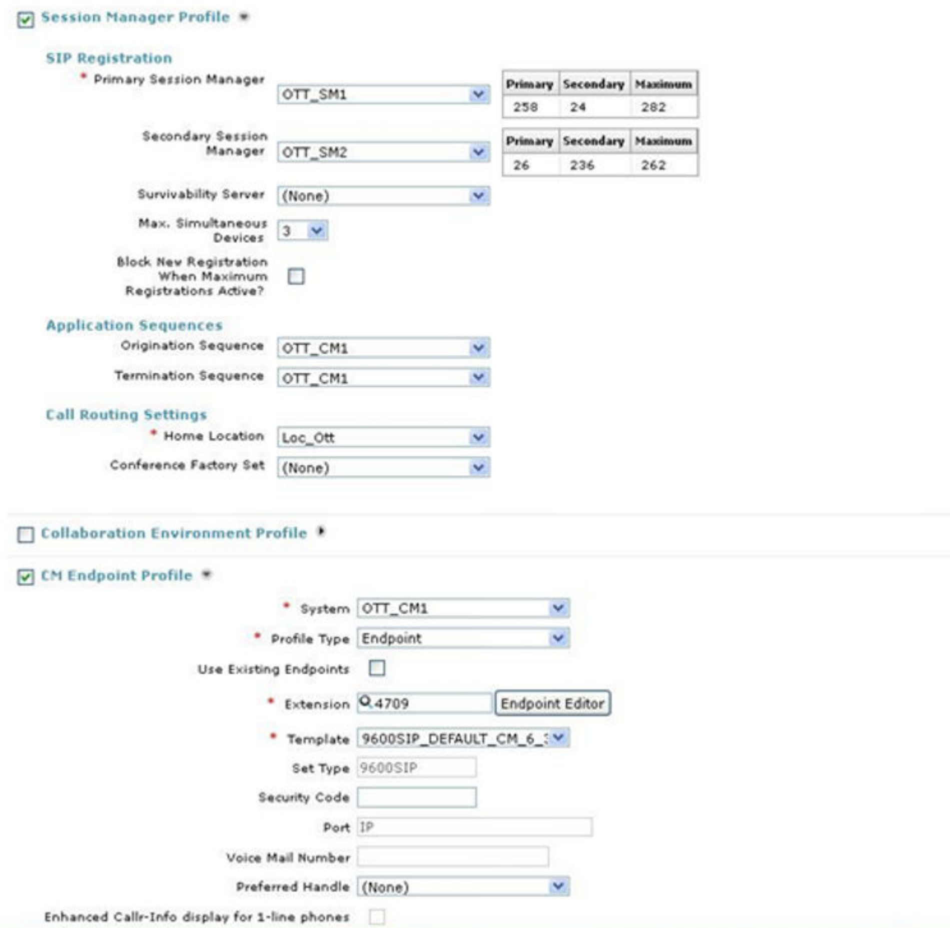
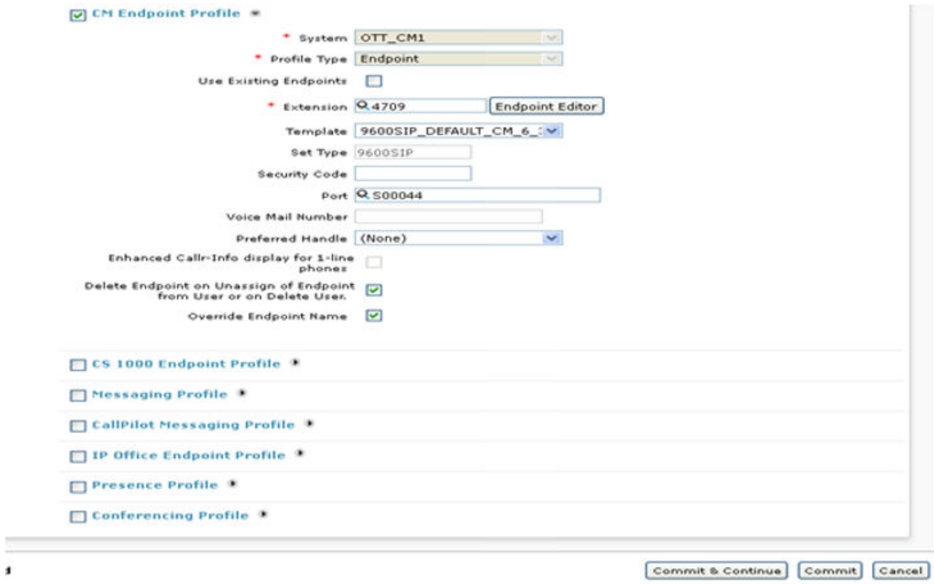


Figure 107: Communication Profile > Session Manager Profile

12. Check the **Session Manager Profile** check box.
13. In the **SIP Registration** section:
    a. Select the **Primary Session Manager** from the drop-down list.
    b. If available, select the **Secondary Session Manager** from the drop-down list.
14. In the **Application Sequences** section, select the Communication Manager for both the **Origination Sequence** and the **Termination Sequence** from the drop-down lists.
15. In the **Call Routing Settings** section, select the **Home Location** from the drop-down list.
16. In the **CM Endpoint Profile** section, in the **Extension** field, enter the same extension number that you entered for the **Login Name**.
17. In the Template field, select **9600SIP_Default_CM** from the drop-down list.
18. At the bottom of the page, click **Commit**. See the following figure.



Related links

User provisioning using System Manager 6.3 FP2 on page 429

Appendix B: Quickstart — Add an 1100 Series IP Deskphone to Avaya Aura®

This appendix is a quickstart guide to adding one IP Deskphone to Avaya Aura®. The 1120E IP Deskphone is used as an example.

Related links

Adding a new IP Deskphone to Avaya Aura® on page 434

Adding a new IP Deskphone to Avaya Aura®

1. Use System Manager (SMGR) to add the new extension.

   Use the same approach/steps as configuring a 96x1 SIP phone.

   Use the **9600SIP_Default_CM_** template.

   You do not have to configure anything in Endpoint Editor for Quickstart use.

2. Create the phone’s **11xxe.cfg** configuration file; for example, 1120e.cfg.

   Example:

   `[FW]`

   `DOWNLOAD_MODE` **`FORCED`**

   `VERSION` **`04.04.09.00`** <— version from the firmware file name

   `PROTOCOL` **`HTTP`**

   `FILENAME` **`SIP1120e04.04.09.00.bin`** <— SIP firmware file name

3. Create the phone’s **11xxeSIP.cfg** configuration file.

   `DEVICE_CONFIG]`

   `DOWNLOAD_MODE` **`FORCED`**

   `FILENAME` **`DeviceConfig.dat`** <— name of the device configuration file

`PROTOCOL` **`HTTP`**

4. Create the phone's **DeviceConfig.dat** device configuration file.

   `AVAYA_AURA_MODE_ENABLE` **`YES`**

   `USE_DEFAULT_DEV_CERT` **`YES`**

   `SIP_DOMAIN1` **`mycompany.com`**

   `SERVER_IP1_1` **`135.20.253.150`**

   `SERVER_TLS_PORT1_1` **`5061`**

5. Store all 3 config files (11xxe.cfg, 11xxeSIP.cfg, DeviceConfig.dat) on the Aura Utility Server using **IP Phone Tools > IP Phone Custom File Upload**, as shown in the following figure.

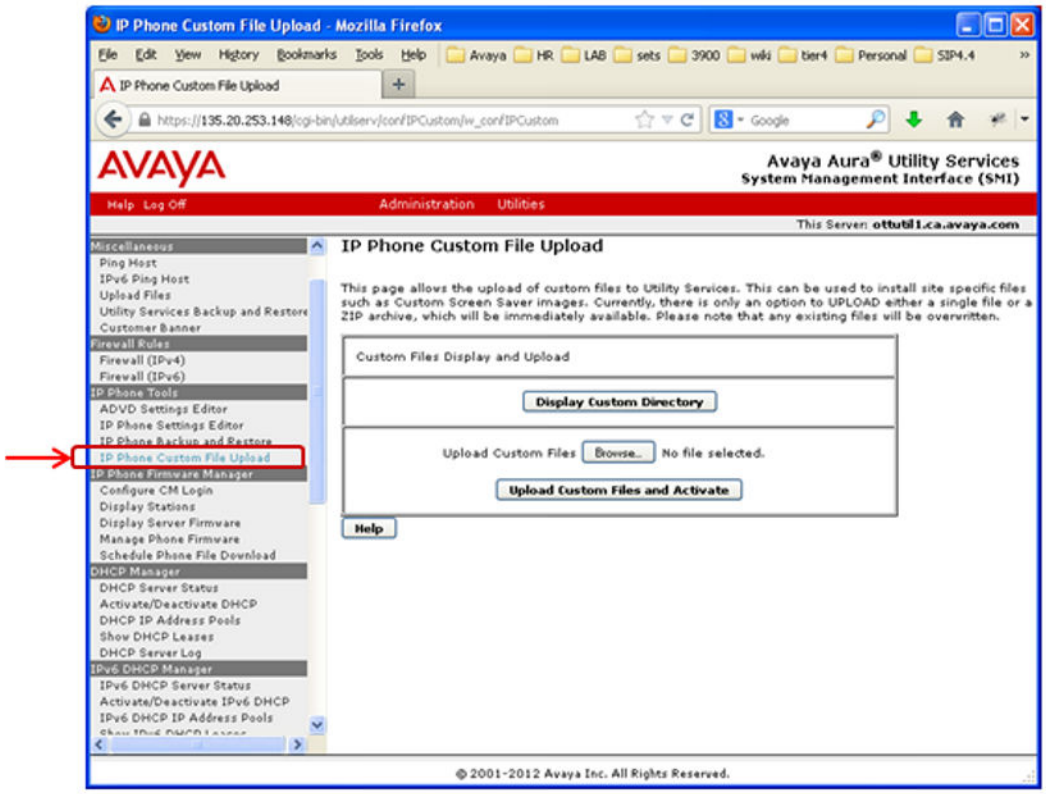


Figure 108: IP Phone Tools > IP Phone Custom File Upload screen

6. Plug in the new IP Deskphone.

   DHCP is the default and an IP address is obtained.

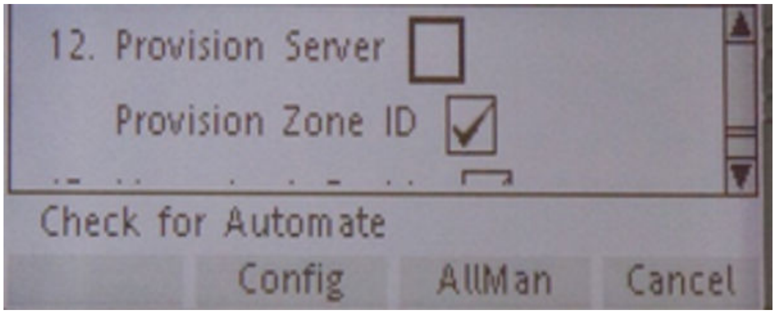
   Note:

   DHCP option 66 can be used to configure the Provisioning URL for large migrations.

7. Enter the Utility Server's IP address as the IP Deskphone's Provision URL.

   a. Double-press the **Services** key quickly, and select **Network Configuration** from the menu.

b. Press the **Auto** soft key. Un-check the **Provision Server** check box and press the **Config** soft key.

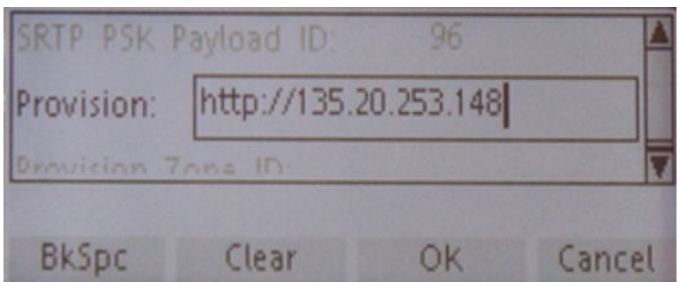


c. In the **Provision** field, enter the Utility Server IP address.

Press the **OK** soft key and then press the **Apply** soft key.

Note:

Toggle the "**1**" key to obtain '**:**', '**/**' and '**.**'.



8. Reboot the IP Deskphone.

   The IP Deskphone may reboot again after obtaining the config.dat file.

9. Log in with the User ID (extension number) and password.

Related links

Quickstart — Add an 1100 Series IP Deskphone to Avaya Aura® on page 434

Appendix C: Configuring FACs and FNEs for the IP Deskphones on Avaya Aura®

This appendix provides information on configuring Feature Access Codes (FACs) and Feature Number Extensions (FNEs) for the IP Deskphones on Avaya Aura®.

Related links

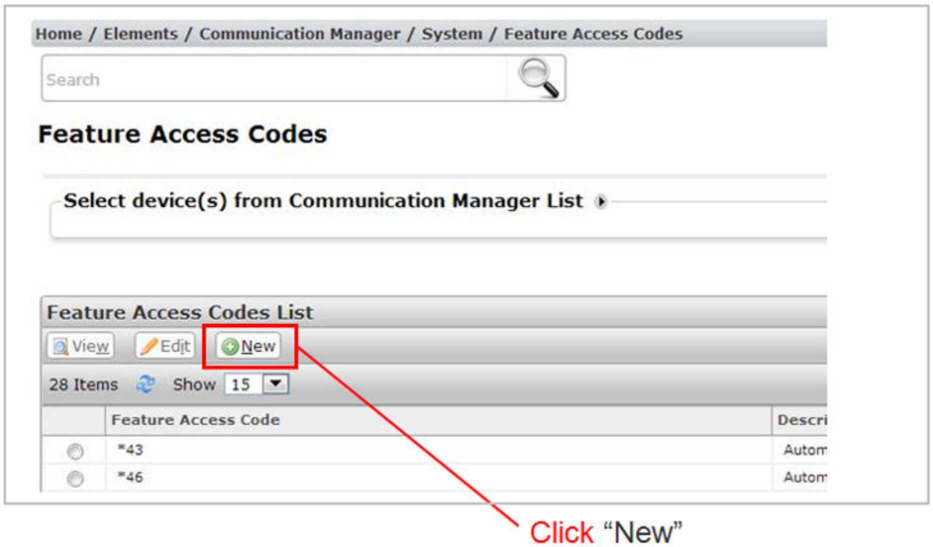
Configuring FACs for the IP Deskphones on page 437
Configuring FNEs on page 439

Configuring FACs for the IP Deskphones

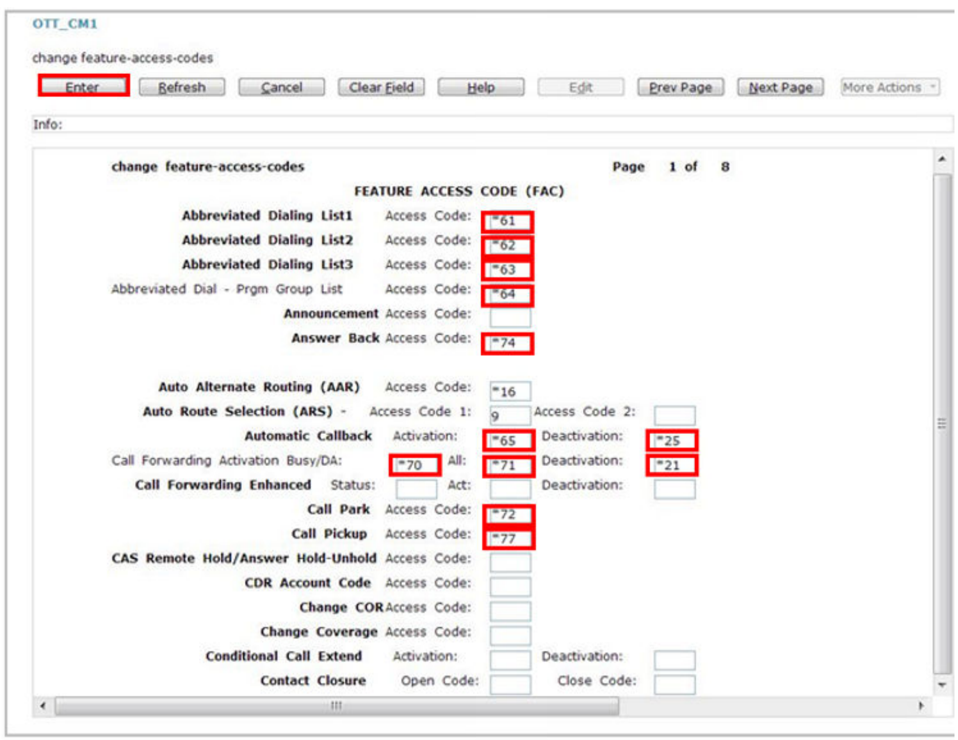
Feature Access Codes (FACs) are configured in System Manager (SMGR). in **Home > Elements > Communication Manager > System > Feature Access Codes**.

Configuring FACs

1. In System Manager, go to **Home > Elements > Communication Manager > System > Feature Access Codes**.
2. Under **Feature Access Codes List**, click **New**.



3. Input FAC codes consistent with your dial plan and click **Enter** when finished.



Related links

[Configuring FACs and FNEs for the IP Deskphones on Avaya Aura®](#) on page 437

Configuring FNEs

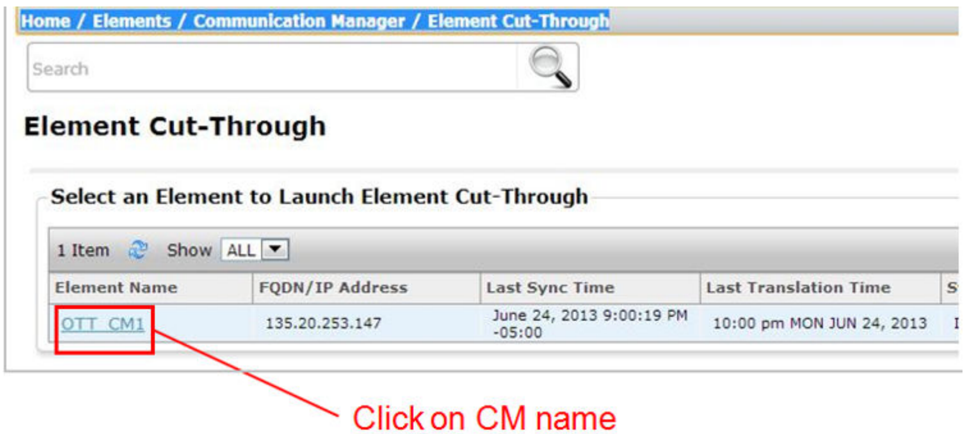
Configuring Feature Name Extensions (FNEs) is a two-part process.

1. Configure the FNEs in **SMGR Cut Through** or in **Communication Manager SAT**.
2. Add the FNEs as Implicit Users to the Session Manager (SM).

Configuring the FNEs

FNEs are configured on Communication Manager but can be accessed through System Manager using the path Home > Elements > Communication Manager > Element Cut-Through.

1. Go to **Communication Manager Element Cut-Through** page.
2. Click the Communication Manager name, as shown in the following figure.

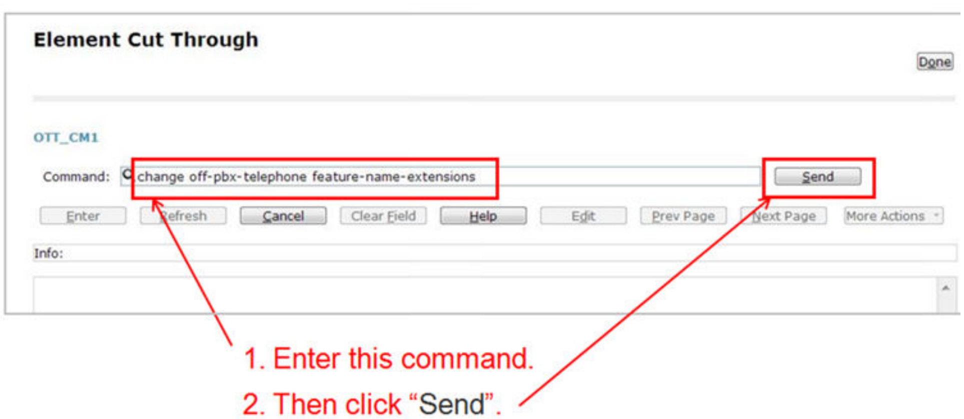


The Communication Manager command page opens.

3. Enter the following in the **Command** field:

```
change off-pbx-telephone feature-name-extensions
```

4. Click **Send**.

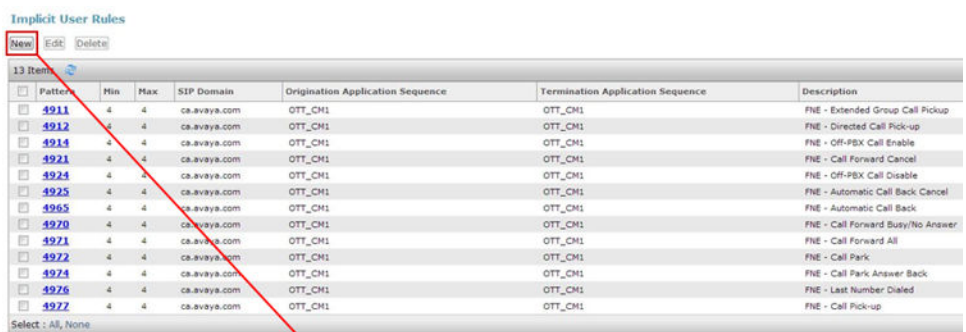


5. Input FNE numbers consistent with your dial plan and click **Enter** when finished.

Adding FNEs as Implicit Users

FNEs are added as Implicit Users in Session Manager after the FNEs have been configured.

1. In System Manager, go to **Home > Elements > Session Manager > Application Configuration > Implicit Users**.
2. Click **New** to add an FNE, or click **Edit** to change an FNE.



Click on “New” to add FNE, “Edit” to change

3. Enter the data for the FNE and click **Commit**.
4. Repeat steps 2 and 3 for each FNE to be added or changed.

Related links

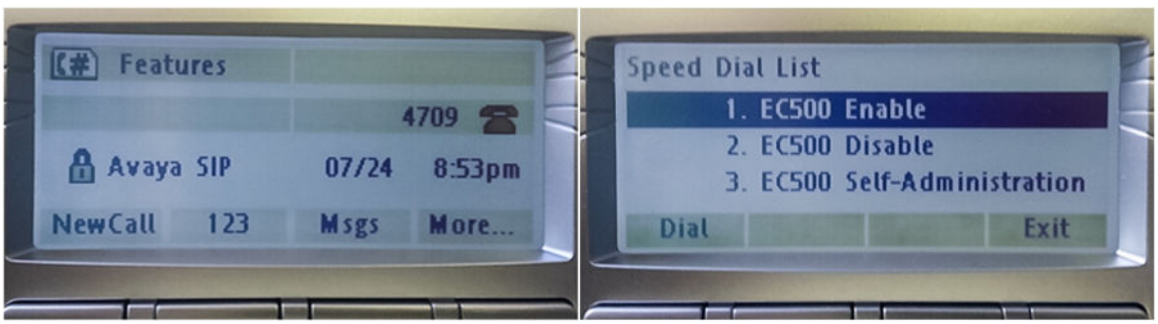
Configuring FACs and FNEs for the IP Deskphones on Avaya Aura® on page 437

Appendix D: Creating a speed dial list

For ease of access to frequently-used features, you can configure a Features speed dial list. Determine the key features that are used and create a speed dial list to easily access those features.

Example:

In this example, a speed dial list has been created for the EC500 feature set. When the **Features** key is pressed, the IP Deskphone displays the EC500 feature options. The user presses 1, 2, or 3 to dial the desired EC500 FNE.



Creating the speed dial list for feature access is a two-part process.

1. Create the Features key on the IP Deskphone. See Creating the Features key in deviceconfig.dat on page 441.
2. Create the speed dial list file. See Creating the speed dial list file on page 442.

Related links

Creating the Features key in deviceconfig.dat on page 441
Creating the speed dial list file on page 442

Creating the Features key in deviceconfig.dat

Create the Features key on the IP Deskphone by adding three parameters to the phone's *deviceconfig.dat* file

1. `SPEEDLIST_KEY_INDEX [x]` — which key
2. `SPEEDLIST_LABEL <KEY Label>` — desired key label

3. `DEFAULT_SPEEDDIALLIST_FILE <Filename` — file with the feature list

Note:

Key numbering ascends from bottom to top, first on the right side, then the left side of the IP Deskphone display screen. Key 1 is reserved and cannot be used.

Key numbering example:

6	**3**
5	**2**
4	**1**

Deviceconfig.dat example

`SPEEDLIST_KEY_INDEX` **`4`**

`SPEEDLIST_LABEL` **`Features`**

`DEFAULT_SPEEDDIALLIST_FILE` **`FNE_Speeddiallist.txt`**

Related links

Creating a speed dial list on page 441

Creating the speed dial list file

Create the speed dial list file with speed dial data entries

Parameter	Definition
[key]	Speed dial key data delimiter. Required.
label=<speed dial name>	Label displayed in speed dial list. Required.
target=<URL>	FNE or FAC digits @ domain Required.
retrieve=NO	Held call retrieved when call is done. Optional.
subject=<display msg>	Message displayed when selected. Optional.
mode=<Always|MidCall|IdleOnly>	When the feature is displayed in the list. Optional.

Example

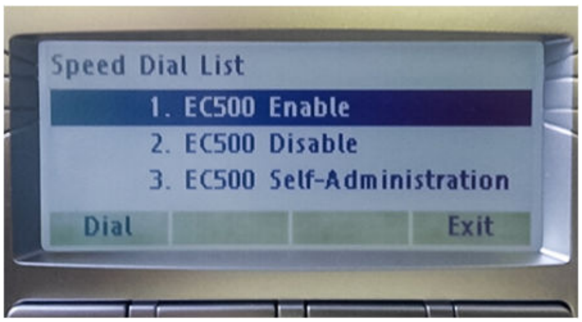
The following is the speed dial list for the EC500 feature set.

FNE_Speeddiallist.txt

[key]
label=EC500 Enable
target=4914@mycompany.com

[key]
label=EC500 Disable
target=4924@mycompany.com

[key]
label=EC500 Self-Administration
target=15@mycompany.com
subject=Enter number



Related links

Creating a speed dial list on page 441

Appendix E: References and additional documentation

Related links

[References](#) on page 444
[Additional documentation](#) on page 445

References

- ***Configuring SMGR 6.2 LDAP Synchronization* white paper**.

  http://support.avaya.com/css/P8/documents/100145665.

- **System Manager "Managing bulk importing and exporting"**. See *Administering Avaya Aura® System Manager Release 6.3*.

  http://support.avaya.com/css/P8/documents/100168146

- ***Application Notes for Avaya 1100- and 1200-Series IP Deskphones R3.2 with Avaya Aura™ Communication Manager R6, Avaya Aura™ Session Manager R6, and Avaya Modular Messaging R5.2***.

  https://downloads.avaya.com/css/P8/documents/100109882

- ***Advanced Feature Support for Avaya 1100 and 1200 Series IP Deskphones 3.2 with Avaya Aura® Communication Manager 6.0 and Avaya Aura® Session Manager 6.0***.

  https://downloads.avaya.com/css/P8/documents/100124770

- ***Configuring Avaya 1100 Series and 1200 Series IP Deskphones running Release 4.3 SIP software with Avaya Aura® Session Manager Release 6.1, Avaya Aura® Communication Manager Release 6.0.1, and Avaya Aura® Messaging Release 6.1 - Issue: 1.0***.

  http://avaya.com/support

- Avaya Software Investment Protection Policy

  http://portal.avaya.com/ptlWeb/gs/so/CS2010106133013664048

Related links

[References and additional documentation](#) on page 444

Additional documentation

User Guides (Avaya Aura® system)

- *Avaya 1120E IP Deskphone with SIP Software on Avaya Aura® User Guide, 16-604273*
- *Avaya 1140E IP Deskphone with SIP Software on Avaya Aura® User Guide, 16-604274*
- *Avaya 1165E IP Deskphone with SIP Software on Avaya Aura® User Guide, 16-604275*
- *Avaya 1220 IP Deskphone with SIP Software on Avaya Aura® User Guide, 16-604276*
- *Avaya 1230 IP Deskphone with SIP Software on Avaya Aura® User Guide,16-604277*

User Guides (other systems)

- *Avaya 1120E IP Deskphone with SIP Software User Guide, NN43112–101*
- *Avaya 1140E IP Deskphone with SIP Software User Guide, NN43113–101*
- *Avaya 1165E IP Deskphone with SIP Software User Guide, NN43170–100*
- *Avaya 1220 IP Deskphone with SIP Software User Guide, NN43170–101*
- *Avaya 1230 IP Deskphone with SIP Software User Guide, NN43170–102*

Quick Reference Guides (Avaya Aura® system)

- *Avaya 1120E IP Deskphone with SIP Software on Avaya Aura Quick Reference Guide*
- *Avaya 1140E IP Deskphone with SIP Software on Avaya Aura Quick Reference Guide*
- *Avaya 1165E IP Deskphone with SIP Software on Avaya Aura Quick Reference Guide*
- *Avaya 1220 IP Deskphone with SIP Software on Avaya Aura Quick Reference Guide*
- *Avaya 1230 IP Deskphone with SIP Software on Avaya Aura Quick Reference Guide*

Quick Reference Guides (other systems)

- *Avaya 1120E IP Deskphone with SIP Software Quick Reference Guide*
- *Avaya 1140E IP Deskphone with SIP Software Quick Reference Guide*
- *Avaya 1165E IP Deskphone with SIP Software Quick Reference Guide*
- *Avaya 1220 IP Deskphone with SIP Software Quick Reference Guide*
- *Avaya 1230 IP Deskphone with SIP Software Quick Reference Guide*

Administration

- *•SIP Software for Avaya 1100 Series IP Deskphones-Administration, NN43170-600*
- *•SIP Software for Avaya 1200 Series IP Deskphones-Administration, NN43170-601*

Related links

References and additional documentation on page 444

Index

Numerics

A

B

C

D

P

Q

R

S

T

U

V

W