SIP Software for Avaya 1100 Series IP Deskphones-Administration

SIP3.2
NN43170-600, 01.02
September 2010

© 2010 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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 Web sites referenced within this site or documentation(s) 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 this product. 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 Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND 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").

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

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 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 Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(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(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 other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: New in this release....5
Revision history....6

Chapter 2: Customer service....7

Chapter 3: Introduction to this guide....9

Chapter 4: Overview....15

Chapter 5: Before installation....21

Chapter 6: Configure the provisioning server....23

Chapter 7: Configure the DHCP Server....89

Chapter 8: Install the IP Deskphone....93

Chapter 9: Upgrade and convert the IP Deskphone software....95

Chapter 10: Provisioning the IP Deskphones....105

Chapter 11: Features....119
Multi-Level Precedence and Preemption....182

Chapter 12: IP Deskphone restrictions....187

Chapter 13: Security....189
Enhanced administrative password security....210

Chapter 14: Audio codecs....213

Chapter 15: Certificate-based authentication....219

Chapter 16: Licensing....249
Licensing framework....250
Licensable Features....254

Chapter 17: Internet Protocol version 6....263

Chapter 18: SIP messages supported by the IP Deskphone....269

Chapter 19: Diagnostics and troubleshooting....281

Index....319

Chapter 1: New in this release

SIP Software for Avaya 1100 Series IP Deskphones- Administration , NN43170-600 is a new document for SIP Software Release 3.2. This document contains administration information for the Avaya 1120E IP Deskphone, Avaya 1140E IP Deskphone, and Avaya 1165E IP Deskphone.

Features

SIP Software Release 3.2 introduces support for:

- Multi Appearance Directory Number support for Avaya on Communication Server 1000
- Security features
- Animated screensaver

Multiple Appearance Directory Number

SIP Software Release 3.2 introduces support for Multiple Appearance Directory Number (MADN) for Avaya Communication Server 1000. For more information, see Multiple Appearance Directory Number on page 137.

Security

SIP Software Release 3.2 introduces many security features for the IP Deskphone including media path security (Secure Real-time Transport Protocol and signalling and SIP over Transport Level Security), such as:

- Transport Level Security (TLS)
- Secure Shell Handler (SSH) and Secure File Transfer
- Secure Real-time Transport Protocol (SRTP)
- Last successful or unsuccessful logon
- Enhanced administrative password security

For more information about security features, see Security on page 189.

Animated screensaver

SIP Software Release 3.2 provides support for an animated screensaver (Avaya 1165E IP Deskphone only). The IP Avaya 1165E IP Deskphone supports a standard screensaver and a customizable screensaver.

For more information about the animated screensaver, see Animated screensaver for the Avaya 1165E IP Deskphone on page 143.

Revision history

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

Navigation

- Getting technical documentation on page 7
- Getting product training on page 7
- Getting help from a distributor or reseller on page 7
- Getting technical support from the Avaya Web site on page 7

Getting technical documentation

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

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at 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://www.avaya.com/support.

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 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.

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
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
IPCM	Internet Protocol Client Manager
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
MAS	Media Application Server
MD5	Message Digest v5
MLLP	Multi-Level Precedence and Pre-emption
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
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 Deskphone administration are:

- *SIP Software for Avaya 1140E IP Deskphone User Guide, NN43113-101*
- *SIP Software for Avaya 1120E IP Deskphone User Guide, NN43112-101*
- *SIP Software for Avaya 1165E IP Deskphone User Guide, NN43170-100*
- *Broadsoft Partner Configuration Guide AVaya SIP Software for IP Deskphones 1120E / 1140E , NN43121-300*

- *Avaya 1100 Series Expansion Module (SIP Software) User Guide, NN43110-301*
- 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 1100 Series IP Deskphones and provides a brief overview of Session Initiation Protocol (SIP). 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 to the provisioning server on page 24.

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 reside. This is not the IP Client Manager (IPCM) of the Call Server.
- 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

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.

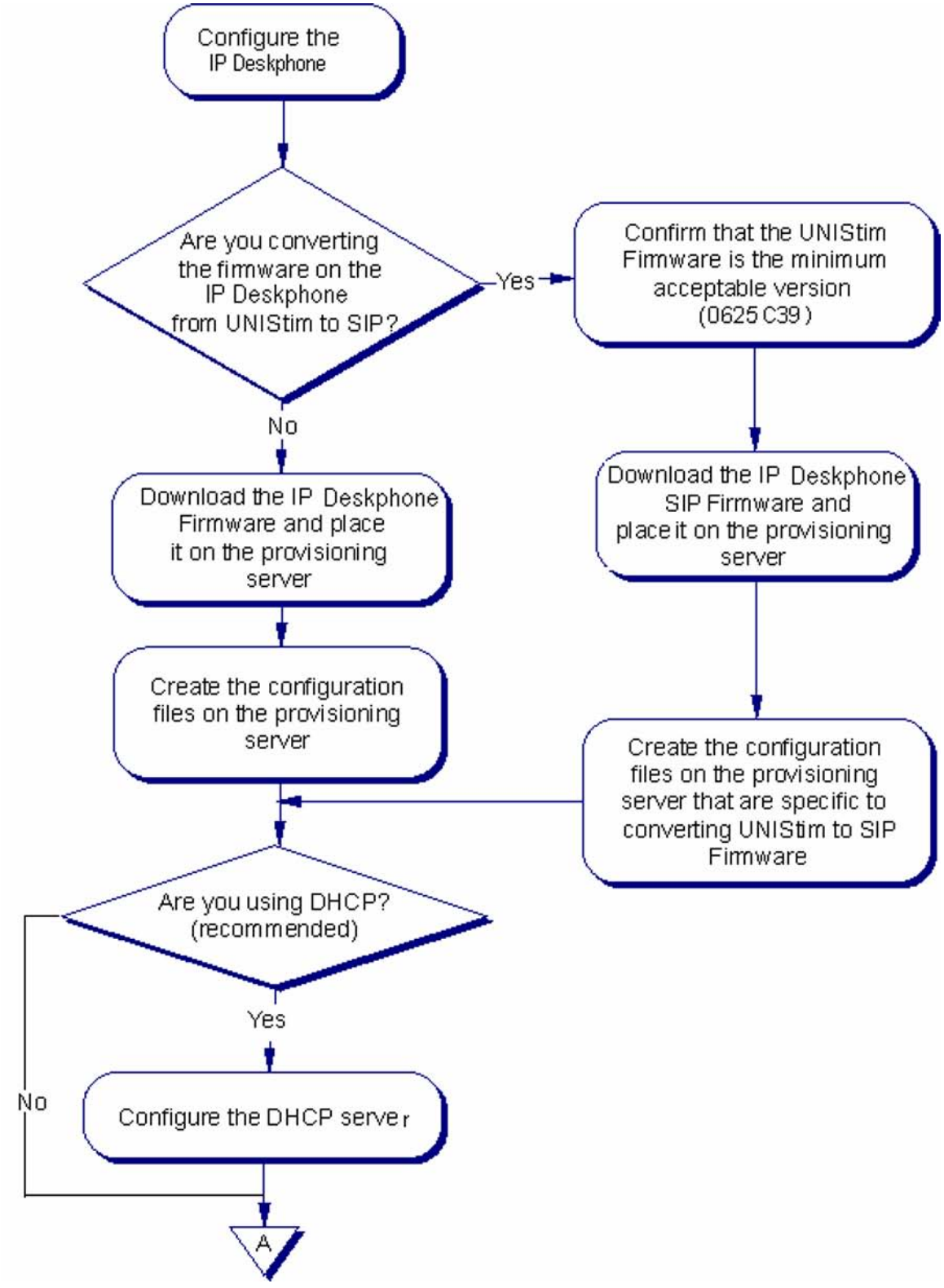


Figure 2: Installation of IP Deskphones with SIP Software, page 1 of 2

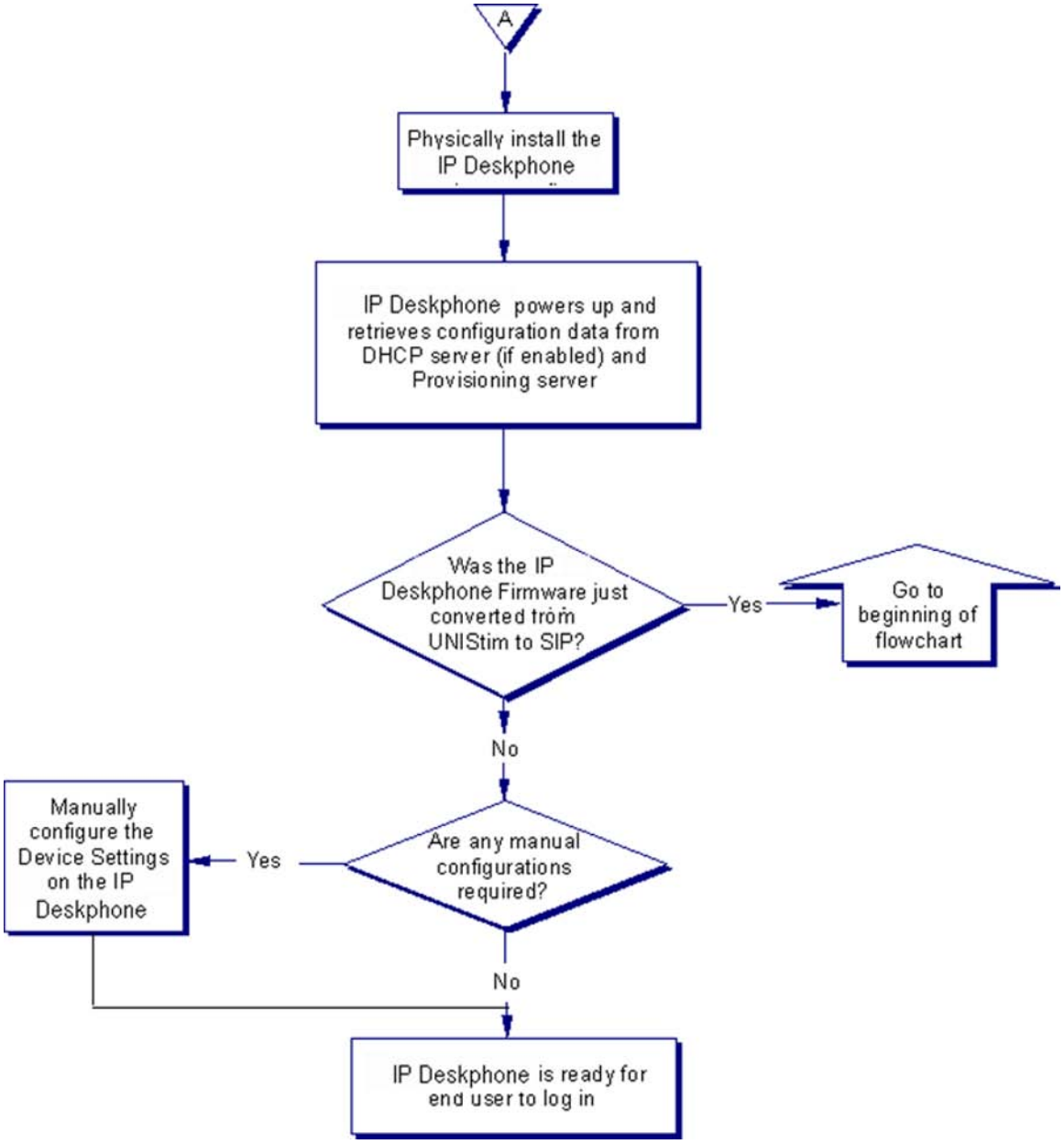


Figure 3: Installation of IP Deskphones with SIP Software, page 2 of 2

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 external power supply. If required, order the external power supply separately.

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

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

CPC code	PEC code	Product description
N0146475	NTYS17BAE6	IP Deskphone Global Power Supply (2000, 1100, 1200) (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, AS5300, and A2E 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: Configure the provisioning server

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 95 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: The end user can manually check for updates by pressing the **Services** key and selecting `Check for Updates`.

  Note:

  The user must be logged in for this to function properly.
- 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 the provisioning server

To download the SIP Software, perform the following procedure.

Downloading SIP Software for the IP Deskphone

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya Web site with a valid Avaya User ID and Password.

   The Support page appears.
3. Enter the IP Deskphone type in the TheInSite Knowledge Base box.
4. Press the red arrow at the end of the TheInSite Knowledge Base box to obtain the Search Results.
5. From the Search Results, select and download the appropriate version of the SIP Software for the IP Deskphone, for example, SIP Avaya 1165E IP Deskphone Release SIP1165e03.02.16.00.bin.
6. Place the selected software on the provisioning server.

Create the SIP provisioning file on the provisioning server

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

`[DEVICE_CONFIG]`
`DOWNLOAD_MODE_AUTO`
`VERSION 000001`
`FILENAME 1120DeviceConfig.dat`
	Device configuration section

`[FW]`
`DOWNLOAD_MODE_AUTO`
`VERSION SIP1120E03.02.16.00`
`PROTOCOL TFTP`
`FILENAME SIP1120e03.02.16.00.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_d24lang FILENAME Portuguese_d24.lang FILENAME Czech_d24.lang FILENAME Russian_d24.lang	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
[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

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
[USER_KERYS]	Root certificates
[LOGIN_BANNER]	Login banner files
[USER_CONFIG]	IP Deskphone-specific configuration files

Provisioning is performed using the commands in the 1xxxeSIP.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. Each language file has a header that contains a software load version with which

this file is associated. Language files are signed by Avaya and are authenticated by the software for security reasons.

- [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 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.
- [USER_KEYS]—this section is used to enable an IP Deskphone to download a customer root certificate.
- [LOGIN_BANNER]—this section is used forto download a text file, the contents of which are displayed on the IP Deskphone immediately after logging on.
- [USER_CONFIG]—this section is used to download device configuration files that are unique to a particular IP Deskphone. This cause the IP Deskphone to look for configuration files that are specific to the MAC address of the IP Deskphone.

  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 19characters, and must follow this format:

SIP1120e03.02.16.00

SIP1140e03.02.16.00

SIP1165e03.02.16.00

SIP12x0e03.02.16.00

Caution:

The version number is stored permanently on the IP Deskphone until a higher version number is downloaded. However, if Forced option is in the 1xxxeSIP.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**Srvcs, System, Erase User Data** 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, 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, 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 name of the server 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 hard 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] is used to determine if the authentication ID screen is presented to the user during login This allows the authentication name to be different than the registration name (for example, the SIP user name). It allows the user to enter an authentication id independent of the log in id. The authentication id is used when the server challenges the phone..This is required for the SCA feature to work on the CS 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 AUTHOLOGIN_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, the IP Deskphone will use 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 **Srvcs, System, Erase User Data**. Any of these actions causes the IP Deskphone to contact the provisioning server and attempt to read the Provisioning file. A Soft Reset (**Srvcs, System, Reset Phone**) does not cause the IP Deskphone to retrieve the Provisioning file.

Setting the default language on the IP Deskphone to French

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.

```
[DEVICE_CONFIG]DOWNLOAD_MODE AUTOVERSION 000002FILENAME
DeviceConfig.dat

[LANGUAGE]DOWNLOAD_MODE AUTOVERSION 0000000001FILENAME French_d24.lng
```

The DeviceConfig.cfg file should contain the following.

```
DEF_LANG French_d24
```

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

For a new user login, the IP Deskphone creates a new user profile. All menus remain in French. 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 on the provisioning server

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

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 SIP provisioning file.

The following is an example of a device configuration file.

```
# Server and Network configuration commands
DNS_DOMAIN corp.yourcompany.com
SIP_DOMAIN1 yourcompany.com
SERVER_IP1_1 10.1.2.3
SERVER_IP1_2 10.1.2.4
SERVER_PORT1_1 5060
SERVER_PORT1_2 5060
SERVER_RETRIES1 3
DEF_USER1 user1

# Voice Feature configuration commands
VMAIL 5555
VMAIL_DELAY 300

# Administrative feature commands
BANNER MCS_4.0
AUTOLOGIN_ENABLE YES

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

Figure 4: Sample device configuration file

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.

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 commands on page 35.

Table 4: Device configuration commands

Configuration command type	Configuration commands	
Server and network configuration commands	SIP_DOMAIN1 SIP_DOMAIN2 SIP_DOMAIN3 SIP_DOMAIN4 SIP_DOMAIN5 SERVER_IP1_1 SERVER_IP1_2 SERVER_IP2_1 SERVER_IP2_2 SERVER_PORT4_1 SERVER_PORT4_2 SERVER_PORT5_1 SERVER_PORT5_2 SERVER_RETRIES1 SERVER_RETRIES2 SERVER_RETRIES3 SERVER_RETRIES4 SERVER_RETRIES5	SERVER_IP3_1 SERVER_IP3_2 SERVER_IP4_1 SERVER_IP4_2 SERVER_IP5_1 SERVER_IP5_2 SERVER_PORT1_1 SERVER_PORT1_2 SERVER_PORT2_2 SERVER_PORT3_1 SERVER_PORT3_2 DNS_DOMAIN DEF_USERS DEF_USER1 DEF_USER2 DEF_USER3 DEF_USER4 DEF_USER5
	UPDATE_USERS SIP_PING REG_REFRESH_INTERVAL SIP_UDP_PORT SIP_TCP_PORT SIP_TLS_PORT REGISTER_RETRY_TIME REGISTER_RETRY_MAXTI ME IPV6_ENABLE PREFER_IPV6 IPV6_STATELESS IPV6_ENABLE_GUI FORCE_REBOOT SRTP_ENABLED SRTP_MODE SRTP_CIPHER_1 SRTP_CIPHER_2	SSH SFTP SSHID SSHPWD SFTP_READ_PATTERNS SRTP_WRITE_PATTERS HASH_ALGORITHM EAP EAPID1 EAPID2 EAPPWD CA CA_DOMAIN HOST_NAME DOD_ENABLE MLPP_NETWORK_DOMAIN MLPP_PRECEDENCE_DOMAIN ENABLE_LLDP
Feature configuration commands	VMAIL VMAIL_DELAY AUTOLOGIN_ENABLE AUTO_UPDATE AUTO_UPDATE_TIME AUTO_UPDATE_TIME_ RANGE USER_FILE_ENABLE	DEF_LANG MAX_IM_ENTRIES MAX_ADDR_BOOK_ENTRIES ADDR_BOOK_MODE PROXY_CHECKING ENABLE_BT AUTH_METHOD BANNER FORCE_BANNER

Configuration command type	Configuration commands	
	AUTOLOGIN_AUTHID_KEYxx PROMPT_AUTHNAME_ENABLE TRANSFER_TYPE REDIRECT_TYPE ENABLE_PRACK SELECT_LAST_INCOMING MAX_LOGINS MAX_INBOX_ENTRIES MAX_OUTBOX_ENTRIES MAX_REJECTREASONS MAX_CALLSUBJECT MAX_PRESENCENOTE	LOCAL_CFWD_ENABLE ENABLE_ANSWER_MODE ANSWER_MODE_MAXALLOWEDADDR ANSWER_MODE_MICMUTE DISPLAY_CALL_SENDER_IM_KEY DST_ENABLED TIMEZONE_OFFSET FORCE_TIME_ZONE IM_MODE IM_NOTIFY
	DEF_DISPLAY_IM CALL_WAITING DISTINCTIVE_RINGING USE_RPORT TOVM_SOFTKEY_ENABLE TOVM_VOICEMAIL_ALIAS TOVM_VOICEMAIL_PARAM MAX_RING_TIME ENABLE_UPDATE E911_USERNAME E911_PASSWORD KEEP_ALIVE_TYPE CONN_KEEP_ALIVE AUTOLOGIN_ID_KEYxx AUTOLOGIN_PASSWD_KEYxx ENABLE_LIGHT HOLD_TYPE ENABLE_3WAY_CALL	DISABLE_PRIVACY_UI DISABLE_OCT_ENDDIAL FORCE_OCT_ENDDIAL SNTP_ENABLE SNTP_SERVER MADN_TIMER MADN_DIALOG DEFAULT_CFWD_NOTIFY FORCE_CFWD_NOTIFY RTP_MIN_PORT RTP_MAX_PORT SCA_HOLD_BEHAVIOR SCA_APPEARANCES SCA_BROADWORKS EXP_MODULE_ENABLE FORCE_REBOOT PROMPT_ON_LOCATION_OTHER E911_PROXY
	E911_TXLOC MENU_AUTO_BACKOUT AUTOCLEAR_NEWCALL_MSG LOGIN_BANNER_ENABLE SECURE_UI_ENABLE SCRNSVR_ENABLE SCRNSVR_UPASS_ENABLE SCRNSVR_UNPRTCTD_ENABLE SCRNSVR_TEXT SCRNSVR_MODE SCRNSVR_DELAY	BLF_ENABLE BLF_RESOURCE_LIST_URI FM_SOUNDS_ENABLE FM_IMAGES_ENABLE FM_CERTS_ENABLE FM_CONFIG_ENABLE FM_LOGS_ENABLE ENABLE_USB_PORT USB_MOUSE USB_KEYBOARD USB_HEADSET USB_MEMORY_STICK HOTLINE_ENABLE HOTLINE_URL

Configuration command type	Configuration commands	
	SCRNSVR_IMAGE BG_IMAGE_ENABLE BG_IMG_SELECT_ENABLE USE_BG_IMAGE SPEEDLIST_KEY_INDEX SPEEDLIST_LABEL	SESSION_TIMER_ENABLE SESSION_TIMER_DEFAULT_SE SESSION_TIMER_MIN_SE
	SET_REQ_REFRESHER SET_RESP_REFRESHER MAX_ALLOWEDADDRESSES PORT_MIRROR_ENABLE MEMCHECK_PERIOD DOS_PACKET_RATE DOS_MAX_LIMIT DOS_LOCK_TIME LOGSIP_ENABLE CUST_CERT_ACCEPT CERT_ADMIN_UI_ENABLE SEC_POLICY_ACCEPT SECURITY_LOG_UI_ENABLE KEY_SIZE KEY_ALGORITHM TLS_CIPHER SIGN_SIP_CONFIG_FILES FP_PRESENTED FP_ENTERED SUBJ_ALT_NAME_CHECK_ENAB LE CERT_EXPIRE SECURITY_POLICY_PARAM_CHANGE AUTO_PRV_ACCEPT	DWNLD_CFG_ACCEPT AUTO_PRV_SIGNING DWNLD_CFG_SIGNING FTP_PASSWORD CALL_WAITING_TONE MAX_APPEARANCE DISABLE_SPKRPHN CALL_ORIGIN_BUSY SLOW_START_2000K USER_FILE_ENABLE DEFAULT_ADDRESSBOOK_FILE DEFAULT_SPEEDDIALLIST_FILE DEFAULT_CUSTOMKEYS_FILE LOGINALPHA_ENABLE
QoS and ToS commands	DSCP_CONTROL 802.1P_CONTROL DSCP_MEDIA	802.1P_MEDIA DSCP_DATA 802.1P_DATA
Tone configuration commands	DIAL_TONE RINGING_TONE BUSY_TONE	FASTBUSY_TONE CONGESTION_TONE
NAT configuration commands	NAT_SIGNALLING NAT_MEDIA NAT_TTL STUN_SERVER_IP1	STUN_SERVER_IP2 STUN_SERVER_PORT1 STUN_SERVER_PORT2
Voice Quality Monitoring	VQMON_PUBLISH VQMON_PUBLISH_IP	JITTER_ENABLE JITTER_WARN

Configuration command type	Configuration commands	
(VQMon) configuration commands	LISTENING_R_ENABLE LISTENING_R_WARN LISTENING_R_EXCE PACKET_LOSS_ENABLE PACKET_LOSS_WARN PACKET_LOSS_EXCE	JITTER_EXCE DELAY_ENABLE DELAY_WARN DELAY_EXCE SESSION_RPT_EN SESSION_RPT_INT
System commands	ADMIN_PASSWORD ADMIN_PASSWORD_EXPIRY ENABLE_LOCAL_ADMIN_UI HASHED_ADMIN_PASSWORD	
Audio Codecs	G729_ENABLE_ANNEXB G723_ENABLE_ANNEXA DEF_AUDIO_QUALITY AUDIO_CODEC1 AUDIO_CODEC2 AUDIO_CODEC3	AUDIO_CODEC4 AUDIO_CODEC5 AUDIO_CODEC6 AUDIO_CODEC7
Deskphone Recovery command	RECOVERY_LEVEL	

Device configuration commands

Important:

The device configuration file uses the following syntax:

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

For example, AUDIO_CODEC[ ] [ ] < >

Important:

The syntax of the device configuration file is case sensitive. Verify that the commands entered 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 CS 2000, AS5200, and AS5300 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 – the corresponding primary and secondary IP addresses. 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 – the corresponding primary and secondary IP addresses. y=1 indicates the primary address and y=2 indicates the secondary address.
- port_number – the SIP proxy signaling port (default is 5060).

SERVER_RETRIES[x] [number_of_retries]

This parameter confirms the number of retries for each domain. The default number of retries is 3. confirms the number of retries for each domain. The default number of retries is 3.

- x – the domain number from 1 to 5.
- number_of_retries – the number of retry attempts to connect to the proxy server.

DNS_DOMAIN [domain]

This parameter is the DNS domain of the IP Deskphone.

DEF_USERS[x] [user_name]

This parameter allows you to enter the default user name for all domains. When the device configuration file gets downloaded, the default user name is used when logging in.

- x – the domain number from 1 to 5.
- user_name – the default user name.

UPDATE_USERS [YES | NO]

This parameter affects the default user names stored in the IP Deskphone. If this flag is configured as YES, the default user names are overwritten each time a new device configuration file is downloaded.

- YES – the default user names are overwritten each time a new device configuration file is downloaded.
- NO – the default user names are not overwritten each time a new device configuration file is downloaded.

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 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
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 IPV6_ENABLE parameter is changed in the configuration file, FORCE_REBOOT [YES] [NO] parameter must be configured to [YES]. When the protocol is changed the IP Deskphone automatically restarts and updates the Device Settings on the IP Deskphone. If the FORCE_REBOOT parameter is configure to NO, the Device Settings menu is not updated 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 YES 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.
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 is 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_ENABLE [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-CapNeg | SecureOnly]	This parameter configures SFTP configuration values. The default value is BE-2MLines. - BE-2MLines (default) - BE-CapNeg - 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.
SSHPW [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 SIP client. 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 writer from the SIP client. 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_ALGORITH [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 – MIK is not configured
EAP [MD5 | TLS | PEAP | DISABLE]	This parameter allows the administrator to ensure that individual devices are authorized to access the enterprise's 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

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 AS5300 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_PARA [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. This is used with the Broadsoft proxy.

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. This is used with the Broadsoft proxy.

RTP_MIN_PORT [x]
The minimum RTP port value is an integer between 1024 and 65535, exclusive of the restricted SIP ports between 5059 and 5080. The default value is 50000.

RTP_MAX_PORT [x]
The maximum RTP port value is an integer between 1024 and 65535, exclusive of the restricted SIP ports between 5059 and 5080. The default value is 50100.

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 50000 and RTP_MAX_PORT is reset to the default value of 50100. An error message is logged. The SystemConfig file stores 50000 and 50100, rather than the erroneous configuration values, to indicate that the configuration attempt has been rejected.

CALL_WAITING [SPEAKER | STREAM]
- 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.

DISTINCTIVE_RINGING [YES | NO]
This feature works with the CS 2000 proxy and the Broadsoft proxy.

- YES – turns on the distinctive ringing feature. This is the default option.
- NO – turns off the distinctive ringing feature.

USE_RPORT [YES | NO]

- 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.

EXP_MODULE_ENABLE [YES | NO]

- 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.

MAX_RING_TIME [x]

This parameter is an n integer between 30 and 600 that configures the number of seconds for incoming calls to ring before ignoring them. The default value is 120.

ENABLE_UPDATE [YES | NO]

- YES – enables UPDATE message support and adds “UPDATE” to ALLOW header. This is the default option.
- NO – disables UPDATE message support.

Note:
ENABLE_UPDATE is provisioned after user logoff.

FORCE_REBOOT [YES | NO]

- YES – forces hard reboot after device configuration update.
- NO – does not force hard reboot after device configuration update. This is the default option.

Note:
In order for FORCE_REBOOT to reboot the IP Deskphone, the VERSION of the device configuration file must be incremented, even if DOWNLOAD_MODE is configured as FORCED.

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 number 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, Message 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

AUTOLOGIN_ENABLE [YES | NO | USE_AUTOLOGIN_ID] or [1 | 0 | 2]

This parameter controls whether the IP Deskphone attempts to automatically log on to the proxy server.

- YES – turns on the auto login feature.
- NO – turns off the auto login feature.
- USE_AUTOLOGIN_ID – 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 using this setting, the user is prevented from logging off the IP Deskphone.

or

- 1 – turns on the Autologin feature.
- 0 – turns off the Autologin feature.
- 2 – enables the Autologin ID feature using the User ID 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 using this setting, the user is prevented from logging off the IP Deskphone.

Note:

If Autologin ID is enabled in the IP Deskphone-specific configuration file, it is recommended that AUTOLOGIN_ENABLE be configured as either Yes/No or 1/0 in the device configuration file. This recommendation facilitates migrating an IP Deskphone that uses the IP Deskphone-specific configuration file to not using the IP Deskphone-specific configuration file. The migration to just using the device configuration file can be done by deleting the IP Deskphone-specific configuration file. If the device configuration file does not have the matching parameters in the IP Deskphone-specific configuration file, the IP Deskphone continues to use the previously assigned settings after the IP Deskphone-specific configuration file is deleted. This recommendation applies to other parameters in the IP Deskphone-specific configuration file.

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 disabled.

- 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 set.

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.
-

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.

ENABLE_ALLOWEDADDRESS [x]

This parameter limits the size of the list of user and domain addresses stored for auto-answered authorization. The default value is 100.

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.

AudioCodec <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 213

DEF_AUDIO_QUALITY [Low | Medium | High]

This parameter is used to configure the default audio quality used for each new call. Audio quality can be changed when the call is active. If this command is not present in the configuration file, the IP Deskphone uses High quality as its default value. The possible parameters for this command are High, Medium, and Low. If any other parameter is entered or these commands are misspelled, the IP Deskphone uses High as the default setting. This allows the ptime to be changed on a particular codec. The default is High.

The following codecs are used for each selection:

- Low – G729 ptime 30
- Medium – G711 ptime 30
- High – G711 ptime 20 (default)

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 Savings Time (DST) mechanism. The time received from the server is GMT and is converted to the proper timezone by the IP Deskphone. If the Daylight Savings Time 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. The default value is YES.

- YES – enables Daylight Savings Time (default).
- NO – disables Daylight Savings Time.

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 5: Time zone offset

Location	Time zone offset (seconds)
(GMT-10:00) Hawaii	-36000
(GMT-09:00) Alaska	-32400
(GMT-08:00) Pacific time (US and Canada)	-28800
(GMT-07:00) Mountain time (US and Canada)	-25200
(GMT-06:00) Central time (US and Canada)	-21600
(GMT-05:00) Eastern time (US and Canada)	-18000
(GMT-04:00) Atlantic time (US and Canada)	-14400
(GMT-03:00) Brasilia, Buenos Aires	-10800
(GMT+00:00) Greenwich, Dublin, Lisbon, London	0
(GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Madrid, Paris	3600
(GMT+02:00) Athens, Istanbul, Cairo, Helsinki, Jerusalem	7200
(GMT+03:00) Moscow, St. Petersburg	10800
(GMT+05:30) Bombay, Calcutta, Madras, New Delhi	18000
(GMT+08:00) Beijing, Chongqing, Hong Kong, Singapore, Taipei	28800
(GMT+09:00) Osaka, Sapporo, Tokyo, Seoul	32400
(GMT+10:00) Canberra, Melbourne, Sydney	36000

Location	Time zone offset (seconds)
(GMT+12:00) Auckland, Wellington	43200

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.

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.

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.

DEF_LANG [language]

This parameter configures the default language. Select one of the supported languages from the language list downloaded. 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 default language used.

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 and takes a number as a parameter. The default limit is 100.

x – the maximum number of address book 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.

ENABLE_SERVICE_PACKAGE [YES | NO] 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.

- YES – the IP Deskphone downloads the service package.
- NO – the IP Deskphone does not download the service package.

CONFERENCE_URI1 This parameter contains the conference Uniform Resource Identifier (URI); for example CONFERENCE_URI1 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.

ADHOC_ENABLED [YES | NO] The default value is NO. If a service package is used then this is provided by the service package.

- YES – the call server supports ad hoc conferencing.
- NO – the call server does not support ad hoc conferencing.

MAX_ADHOC_PORTS1 [0–4]

This parameter indicates the maximum number of users supported for ad hoc conferencing on the server. This value must be the same as the value configured on the server. When ENABLE_SERVICE_PACKAGE is enabled, the preceding parameters are ignored. 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 will be no subscription alive for this NOTIFY, it is treated as an out of dialog NOTIFY. The IP Deskphones sends a 200 OK for the NOTIFY to the proxy for the acceptance of the event.

Receiving a NOTIFY with the event header set to check-sync, the IP Deskphone sends out a 200 OK, and the user is prompted for the update process.

- 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_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.

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. Y 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)

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.
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_SOUNDS_ENABLE [YES | NO]	This parameter allows the user to act on WAV files using the file manager. If the value is configured as N, the IP Deskphone cannot perform any actions on WAV files, such as delete or copy 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 Y, 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 – to 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 – to 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.

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 – to 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 – to 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.

ENABLE_LIGHT [YES |NO]

This parameter enables or disables the on the IP Deskphone to illuminate when a user picks up the handset. When the handset is returned to the IP Deskphone the light goes out. The default is NO.

- YES – enables the light on the IP Deskphone to illuminate.
- NO – disables the light on the IP Deskphone (default).

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

MAX_ALLOWEDADDRESSES [x]

This parameter limits the size of the list of user and domain addresses stored for auto-answered authorization. The default value is 100.

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 modified.
- NO – the Port Mirroring prompt in the Advanced Diag Tools dialog is 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 147.
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 147.
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 147.

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 147.
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 [DSN]	This parameter is the network domain (DSN) of the user to be added to the INVITE message of outgoing calls. 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.
MAX_APPEARANCES [x]	This parameter determines the maximum number of call appearances that a user can have. The maximum is 10. The default is 2. DoD requirement is a maximum of 2. x – number of call appearances between 1 and 10.
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).

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.

LOCAL_CFWD_ENABLE [YES | NO] This parameter enables or disables SIP-based call forwarding for IP Office support. The default value is YES.

- YES – enables SIP-based call forwarding (default).
- NO – disables SIP-based call forwarding.

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 does not process or use the value defined in NAT_TTL [x]. The IP Deskphones always pings 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 IPs 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 servers IPs 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 120 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.
- NO – disables VQMoN.

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	LISTENING_R_WARN = 70 (default if not configured and unknown type) LISTENING_R_EXCE = 60

vqmonVocoderTypeUnknown	

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 0 resets it to default based on far end VOCODER.

xx – is an INTEGER value used as 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 0 resets it to default based on far end VOCODER.

xx – is an INTEGER value used as 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 0 resets the threshold to default.

xx – is an INTEGER value scaled by 256 that is used as 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 0 resets the threshold to default.

xx – is an INTEGER value scaled by 256 that is used as 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 alert report based on jitter detection
- NO – disables the sending of 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 0 resets the threshold to default.

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 0 resets the threshold to default.

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 0 resets the threshold to default.

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 0 resets the threshold to default.

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.

Both session report enable and session report interval 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.

ADMIN_UI_ENABLE [YES | NO]

This parameter configures the availability of the local administration UI on the IP Deskphone. The default value is YES.

- YES – local administration UI is configured
- NO – local administration UI is not configured

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 recovery command

RECOVERY_LEVEL [x]

This parameter controls the phone recovery if the phone hits any Major or Critical error. Following values are used for setting the recovery level on the phone:

- 0 - Phone never recovers from any error
- 1 - Phone recovers from Major error
- 2 - Phone recovers from Major and Critical errors

Default is 255, which is equivalent to the recovery level of 2.

IP Deskphone configuration commands summary

AUTOLOGIN_ID_KEY [xx]

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.

xx – an ASCII string that corresponds to the User ID, where xx = 00 to the maximum number of keys supported on the IP Deskphone.

Note:

To provision AUTOLOGIN_ID_KEY [xx], the IP Deskphone must be rebooted after the IP Deskphone configuration file is updated.

AUTOLOGIN_PASSWD_KEY [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 in the device configuration file, the IP Deskphone does not log on.

Note:

To provision AUTOLOGIN_PASSWD_KEY [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 CS 1000 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 [xx] This parameter specifies the authentication name to be used for a specific key.

Create the Dialing Plan file on the provisioning server

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.

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 for 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 163 for information on the handling of Emergency calls by the IP Deskphone with SIP software.

An example of a dialing plan is provided below.

```
/* ---------------------------------------- */
/* A simple dial plan                       */
/* ---------------------------------------- */
$n="yourcompany.com"
$t=300
$s=0

%%

/* DIGITMAP: Operator call */

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

/* DIGITMAP: Help Desk */

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

/* DIGITMAP: Emergency call */

(911)|(911)#                    && sip:$$@$n;user=phone      && t=100|Emergency

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

([^0496]x{3})|([^0496]x{3})#    && sip:$$@$n;user=phone      &&

/* DIGITMAP: Public local call, access code 9 */

(9[^1]x{9})|(9[^1]x{9})#        && 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 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
```

Figure 5: Sample dialing plan

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 Figure 5: Sample dialing plan on page 83, 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.

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 matches within parentheses or the "matches" if parentheses is not specified
/* comments line */	comments

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
*6[179#]	Matches *61, *67, *69, or *6#
x{10}	Ten digits (0-9)
011x{7,15}	011 followed by seven to fifteen digits
91(x{10})	matches 91 followed by 10 digits (does not include 91) Ex: 911234567890 $$=1234567890

Figure 9: DRegex rules

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 with SIP Software. 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 to the provisioning server on page 24. 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 DHCP server requires special configuration in Full DHCP mode. The IP Deskphone with SIP Software obtains Device Settings parameters from specially-configured DHCP servers.

The IP Deskphone with SIP Software requests the following Device Settings parameters from the DHCP server:

- IP address configuration for the IP Deskphone
- subnet mask for the IP Deskphone IP address
- default gateway for the IP Deskphone subnet
- DNS server
- Provisioning Server

It is also possible to obtain the DNS IP automatically without any special configuration of the DHCP server. This means that there is no need to configure the Avaya-specific Vendor Class Identifier (Option 60) on the DHCP server. However, the provisioning server address needs to be manually defined within the Device Settings menu.

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 Avaya-SIP-Deskphone-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 Avaya-SIP-Deskphone-A, where A identifies the version number of the information format of the IP Deskphone.

The Class Identifier Avaya-SIP-Deskphone-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**

Requested Device Settings parameters

SIP IP Deskphone-aware DHCP server can automatically configure SIP IP Deskphones by requesting a list of configuration parameters. The IP Deskphone uses DHCP to request and receive the information.

The following table lists the Device Settings parameters requested by the IP Deskphone in the Parameter Request List option (Option Code 55) in the DHCPDISCOVER and DHCPREQUEST messages. The DHCPOFFER and the DHCPACK reply messages from the DHCP server must contain the options in the following table.

Table 6: DHCP options

Parameter requested by the IP Deskphone	Description	DHCP server option
Subnet mask	This is the subnet mask of the IP Deskphone.	1
Router and gateways	IP address of the default gateway of the IP Deskphone.	3
DNS server	DNS Server address; only the first one from the list is used.	6
Broadcast address	This is the Broadcast address of the subnet. The IP Deskphone automatically calculates the Broadcast address if it is not provided.	28
DNS domain	Implementation varies according to DHCP server.	15

Parameter requested by the IP Deskphone	Description	DHCP server option
Lease time	Implementation varies according to DHCP server.	51
Renewal time	Implementation varies according to DHCP server.	58
Rebinding interval	Implementation varies according to DHCP server.	59
Provisioning server	Used for delivering the provisioning server IP address. This parameter can contain either IP address or a URL to the provisioning server or folder.	66

DHCP VLAN Auto Discovery

Configuring a server for Voice VLAN Discovery is optional. This configuration is required only when you are configuring the VLAN Auto Discovery in the Device Settings menu on the IP Deskphone.

VLAN Auto Discovery configuration is useful in a network with separate Data VLAN for traffic (commonly used for PC-to-PC communication) and Voice VLAN for VoIP traffic with different priorities.

The VLAN Auto Discovery is a two-step process:

1. DISCOVER is sent to the DHCP server for available Voice VLAN IDs. The DHCP server sends an OFFER with the available Voice VLAN IDs. If the Data VLAN ID has been manually provisioned in the Device Settings of the IP Deskphone, DHCP DISCOVER is tagged with the Data VLAN ID; otherwise, it is untagged.
2. DISCOVER is sent to the DHCP server for all of the DHCP required parameters. However, this DISCOVER is tagged with the Voice VLAN obtained in step 1.

DHCP VLAN Auto Discovery requires a Avaya-SIP-Deskphone-aware DHCP server. All DHCP requests carry the Vendor Class Identifier, Avaya-SIP-Deskphone-A, to allow the DHCP server to identify that the requests are coming from an IP Deskphone with SIP Software.

DHCP Auto Discovery returns Voice VLAN IDs. The DHCP protocol provides no standard option for VLAN ID requests. Separate DHCP vendor-specific entry is needed for DHCP VLAN Auto Discovery to convey the VLAN information to the IP Deskphone. DHCP VLAN Auto Discovery uses one of the reserved for site-specific use DHCP options for VLAN list retrieval. At least one of the following Avaya site-specific options must be returned by the DHCP server as part of each DHCPOFFER and DHCPACK message for the IP Deskphone to accept these messages as valid; 43, 128, 131, 144, 157, 188, 191, 205, 219, 223, 232, 247, 251.

After multiple VLAN IDs are returned from the DHCP server, the IP Deskphone tries to connect to each of the VLANs, following the order in which VLAN IDs are specified in the DHCP option.

The format of the field for DHCP VLAN Auto Discovery is: Type, length, and data, described in the following sections.

Type (1 octet)

To avoid the possibility of option types already being used by different vendors, there are fourteen options types supported by the IP Deskphone. They are: 128, 131, 144, 157, 188, 191, 205, 219, 223, 232, 247, 251, 247, and 251. Select one value from the type byte list for the DHCPOFFER response. Avaya recommends using 232, 247, or 251. DHCP option numbers less than 224 are reclaimed by the IETF (RFC3942). Future changes in the DHCP protocol can force the IP Deskphone to stop sending these option requests. Currently, IP Deskphone with SIP Software does support the remaining listed options to maintain backward compatibility.

Length (1 octet)

The Length value is variable. Count only the number of octets in the data field.

Data (variable number of octets)

ASCII based format: VLAN-A:XXX+YYY+ZZZ. where, VLAN– A: uniquely identifies this as the Avaya DHCP VLAN discovery request. Each VLAN ID is followed by a plus (+) sign if there are more VLAN IDs or a period (.) to terminate the string.

There are a maximum of 10 VLAN IDs that can be configured in the current version.

Once IP Deskphone with SIP Software receives the DHCP offer containing the site-specific Voice VLAN option, the next DHCPDISCOVERY message is tagged with the Voice VLAN ID.

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.

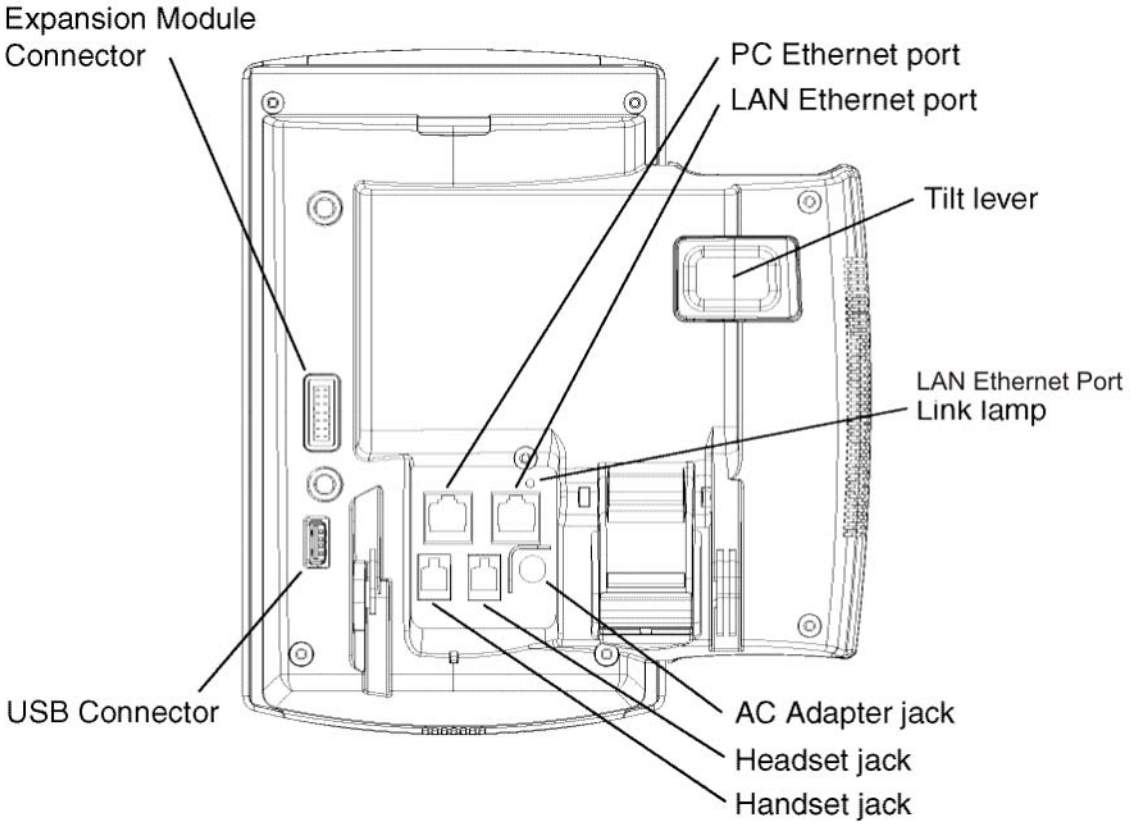


Figure 10: IP Deskphone connections

Chapter 9: Upgrade and convert the IP Deskphone software

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

n 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 101. 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 98.

To convert the firmware on the IP Deskphone from SIP to UNIStim, see the section Convert SIP Software to UNIStim Software on page 102.

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 the provisioning server

To download the SIP Software, perform the following procedure.

Downloading SIP Software for the IP Deskphone

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya Web site with a valid Avaya User ID and Password.

   The Support page appears.
3. Enter the IP Deskphone type in the TheInSite Knowledge Base box.
4. Press the red arrow at the end of the TheInSite Knowledge Base box to obtain the Search Results.
5. From the Search Results, select and download the appropriate version of the SIP Software for the IP Deskphone, for example, SIP Avaya 1165E IP Deskphone Release SIP1165e03.02.16.00.bin.
6. Place the selected software on the provisioning server.

Modify the SIP provisioning file

Use the following procedure to modify the SIP provisioning file, which exists 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 SIP1165e03.02.16.00).
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.
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, System, 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 42).

   Any of these actions causes the IP Deskphone to contact the provisioning server and attempt to read the Provisioning file. A Soft Reset (**Srvcs, 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 C23 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 101.

   If the number is lower than 0625C39, go to the section Upgrade UNIStim software to the minimum required UNIStim software on page 98 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 7: Local Tools menu

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

   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 8: 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

Key	Action
Left	Closes menu
Select key (center of cluster)	Selects current menu item

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

2. Select **2. Local Diagnostics** in the Local Tools menu by pressing the key in the Navigation key cluster or by pressing the number 2.
3. Select **IP Set and DHCP Information** by pressing the **Select** key in the Navigation key cluster or by pressing the number .
4. Use the down arrow in the Navigation key cluster to scroll down the menu to Software Version.
5. 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 Phone (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 101.

If the number is lower than 0625C39, see Upgrade UNIStim software to the minimum required UNIStim software on page 98 and follow the instructions to upgrade an IP Phone 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. The 11xxe.cfg provisioning file is a clear text file. Create the provisioning file as shown in the next table.

   Table 9: 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.
   b. Log on to the Avaya Web site with a valid Avaya User ID and Password.

      The **Support** page appears.
   c. Enter the IP Deskphone type in the **The In Site Knowledge Base** box.
   d. Press the red arrow at the end of the **The In Site Knowledge Base** box to obtain the Search Results.
   e. From the Search Results, select the appropriate version of the SIP software for the IP Deskphone, for example, Avaya 1165E IP Deskphone Release 0625C23
   f. Place the selected software 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 TFTP server address.

   This can be the provisioning server as defined in the chapter Configure the provisioning server on page 23.
5. Select the **Apply&Reset** 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 chapterDiagnostics and troubleshooting on page 281 in the section 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

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 10: Local Tools menu

1. Preferences
2. Local Diagnostics
3. Device Settings
4. Lock Menu

2. Select **3. Device Settings** from the Local Tools menu.

   The Device Settings 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 Configure the provisioning server on page 23.

6. Select the **Apply&Reset** 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 281.

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 complete, and, if necessary, the procedure to upgrade the UNIStim software is complete, 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 C23 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 too http://www.avaya.com/support.
2. Log on to the Avaya Web site with a valid Avaya User ID and Password.

   The Support page appears.
3. Enter IP Deskphone type in the **TheInSite Knowledge Base** box.
4. Press the red arrow at the end of the TheInSite Knowledge Base box to obtain the Search Results.
5. From the Search Results, select the appropriate version of the SIP Software for the Avaya 1165 IP Deskphone; for example, Avaya 1165E IP Deskphone Release SIP1165e03.02.16.00.bin.
6. Place the selected software 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 11: Sample 11xxe.cfg configuration file

   ```
   [FW]
   DOWNLOAD_MODE AUTO
   VERSION 06C25D26.bin
   FILENAME 11xxe.img
   ```

3. Configure the IP Deskphone Device Settings TFTP IP address to the IP address where your TFTP server is running.

   After you are finished the configuration, the IP Deskphone reboots and sends a request to the TFTP server.
4. Select the **Apply&Reset** 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 containing the following information:

   [FW]

   DOWNLOAD_MODE FORCED

   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 Deskphones

The IP Deskphones support the following provisioning modes:

- Manual provisioning
- Automatic provisioning

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, Trivial File Transfer Protocol (TFTP), and HyperText Transport Protocol (HTTP) provisioning

You can store common provisioning parameters in a managed central server, such as a DHCP or TFTP or HTTP 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.

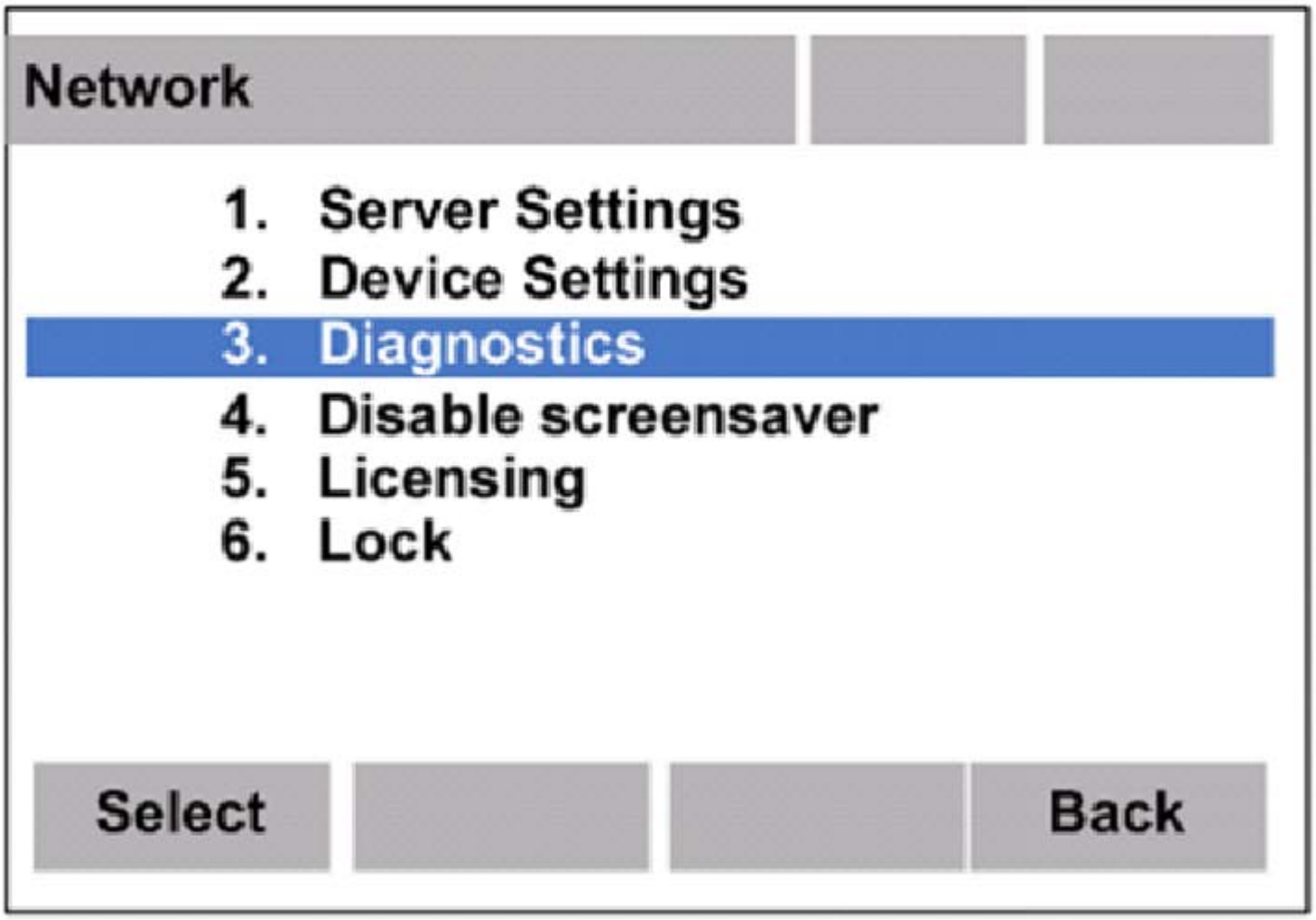
Configuration

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

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

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 check 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

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

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 12: 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.
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 parameters list in order of appearance.

```
Enable 802.1x (EAP) []
ID 1 []
ID 2 []
Password
Enable 802.1ab (LLDP)[]
Enable IPv6 []
DHCP []
Phone IP []
Net Mask []
Gateway []
DNS IP1 []
CA Server []
Domain Name []
Hostname []
Ntwk Port Speed []
Ntwk Port Duplex []
Enable Voice 802.1Q []
Voice VLAN []
VLAN Filter []
Voice Control pBits []
Voice Media pBits []
DSCP []
Avaya Auto QoS []
Enable PC Port []
PC Port Speed []
```

```
Data VLAN []
Data Priority bits []
PC-Port Untag all []
Cached IP []
Ignore GARP []
Provisioning []
PVQMon IP []
NAT Traversal []
STUN S1 IP []
STUN S2 IP []
Media Security []
SIP UDP Port []
SIP TCP Port []
SIP TLS Port []
Connection Timers []
Keep-Alive []
Register Retry []
Register Max Retry []
Login Notify []
Enable Bluetooth (1120E/1140/1165E only) [ ]
SSH-SFTP []
Enable SSH []
UserID [ ]
Password []
Enable SFTP []
Enable FIPS []
```

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 13: 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.

Key	Description
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.
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 14: 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.
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.

Config option	Options or input	Description
		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.
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.

Config option	Options or input	Description
	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.
	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.

Config option	Options or input	Description
	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.
	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.

Config option	Options or input	Description
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 15 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	
	Failure	
	Both	

Config option	Options or input	Description
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.

Chapter 11: Features

This section describes the features that are supported on the IP Deskphone.

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 77).
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 77).
    b. Configure PVQMon IP in Device Settings (see Manual provisioning parameters on page 110)
3. Configure the remainder of the VQMon parameters in the device configuration file (see VQMon configuration commands on page 77). 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 15: Glossary of RTCP XR metrics on page 120. 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 indicating that there is an exceeded value at regular intervals. 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 15: 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.

Metric	Description
MIU	Media Information Unit. MIU is a concept from VQMon. An MIU can be any size down to a 10 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 with SIP Software 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 Phones with SIP Software do not negotiate or exchange messages with the device defined using PUBLISH_IP options.

Session interval report

The IP Deskphone with SIP Software 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 with SIP Software send session interval reports more frequently, then a threshold violation has occurred.

Alert interval report

When an IP Deskphone with SIP Software detects that a voice quality metric has exceeded a threshold, the IP Deskphone with SIP Software 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 Deskphone with SIP Software stops 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.

The Multiuser feature for CS 1000 requires that PROMPT_ENABLE_YES is configured to YES in the device configuration file. This prompts the end user to enter an authentication ID that is different from the login ID.

An example of configuring SIP IP Deskphones to register with multiple users to 1 TN for Communication Server (CS) 1000 is provided below.

Important:

It is mandatory that you include the @domain.com in the LOGINID.

```
AUTOLOGIN_ENABLE USE_AUTOLOGIN_ID
PROMPT_AUTHNAME_ENABLE YES
AUTOLOGIN_ID_KEY01 2257@avaya.com
AUTOLOGIN_AUTHID_KEY01 johnsmith1234
AUTOLOGIN_PASSWD_KEY01 123456

AUTOLOGIN_ID_KEY02 2222@avaya.com
AUTOLOGIN_AUTHID_KEY02 johnsmith1234
AUTOLOGIN_PASSWD_KEY02 123456
```

Initial logon

To logon 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.

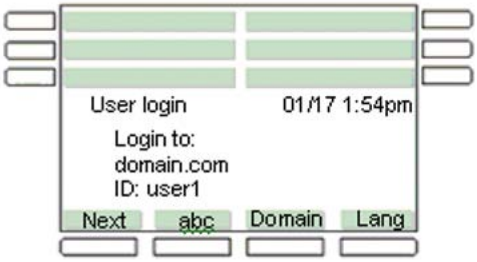


Figure 11: Primary logon screen

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), the IP Deskphone uses the configurations of the primary account. The IP Phone 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.

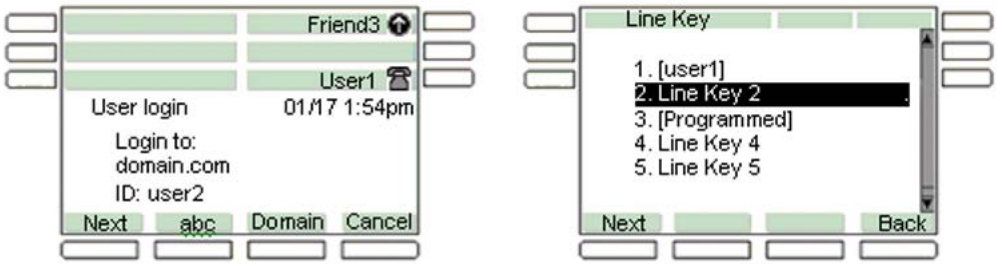


Figure 12: Example of secondary logon screens

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 `login in progress` 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

If you are logged on when the IP Deskphone is switched off, the IP Phone automatically logs you 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, one after the other, when you restart the IP Deskphone.

If the automatic logon feature is disabled in the device configuration file, automatic logon does not occur.

You can provision the IP Deskphone with user credentials to automatically logon multiple accounts on the initial startup. See Primary account logout on page 125.

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.

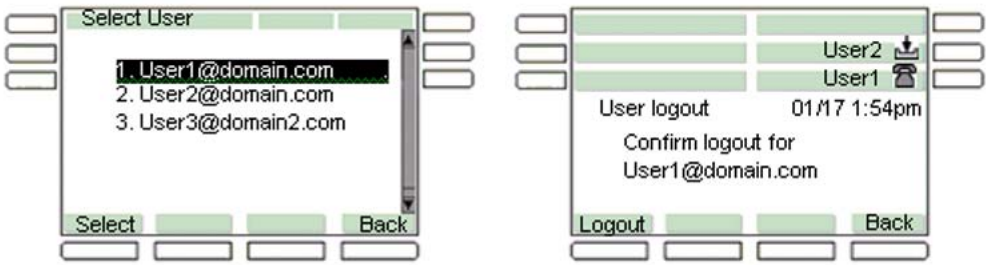


Figure 13: Example of log off screens

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 logon 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.

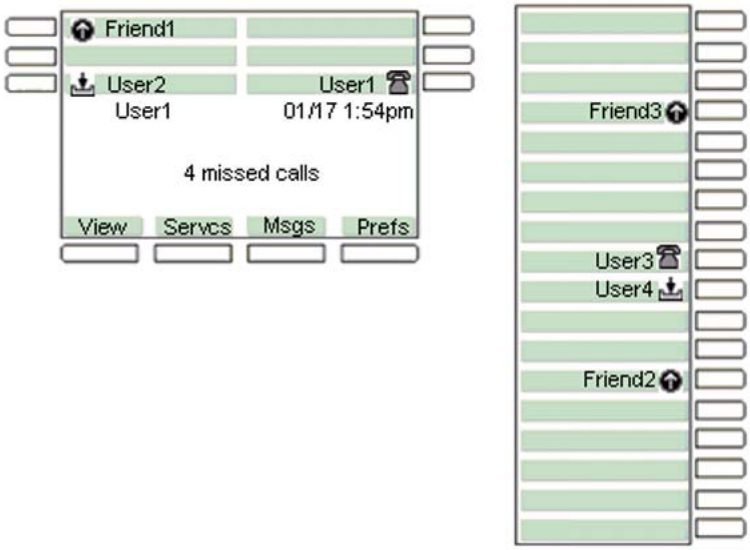


Figure 14: IP Deskphone with Expansion Module and multiple accounts

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 127.

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 136.

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.

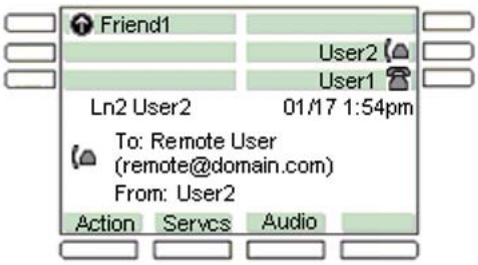


Figure 15: Example of the IP Deskphone with one call

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

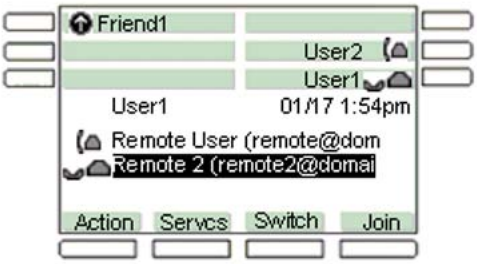


Figure 16: Example of the IP Deskphone with multiple calls

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 133.

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.

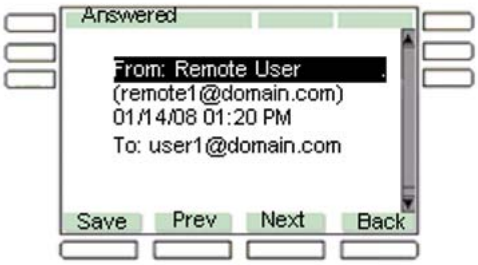


Figure 17: Example of the Inbox call details

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 Context-sensitive 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

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 local 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.

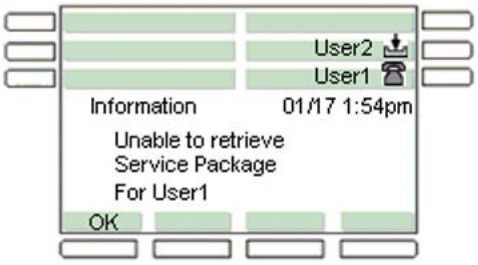


Figure 18: Example of an account notification

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. See Configuration files on page 137.

Configuration files

You can configure the parameter, MAX_LOGINS in the device configuration file. The number that you configure determines the maximum number of user accounts that you can log on 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 key. The default is unlimited. 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 it is not possible to restrict the IP Deskphone to 0 logons.

The number of concurrent logons can never exceed 24, regardless of the value of MAX_LOGINS.

The parameter SELECT_LAST_INCOMING determines which call is selected when there are multiple calls ringing (or active). The default value is 0. If the value is 0, the first selected call is left static as new calls come in or are dropped. . If the value is changed to 1 then the selected call in the call list jumps to the most recent ringing call when it is added to the list.

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.

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

The Multiple Appearance Directory Number (MADN) allows a Directory Number (DN) to appear on more than one IP Deskphone with SIP Software on a Communication Server 1000 system.

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.

With the MADN SCA feature configured on multiple phones of different registered SIP users, the IP Deskphones share one single DN. An incoming call to this DN causes all the IP Deskphones in the group to ring.

Any other user in the group can answer the incoming call by accessing the line key with SCA provisioned.

Any user with the MADN SCA feature can put a call on hold. Any other user in the group can pickup 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 the line key icons, see the applicable IP Deskphone User Guide.

For more information about the line key icons, see the applicable User Guide.

The MADN SCA feature for CS 1000 requires that PROMPT_ENABLE_YES is configured 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 authentication ID is used as the user ID in the CS 1000 and the login prompt on the IP Deskphone corresponds to the SCA group on the CS 1000.

An example of CS 1000 configuration is provided below.

```
TN 108 1 0 6
DATE
PAGE
DES
DES 1M011
TN 108 1 00 06 VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU johnsmith1234 (AUTOLOGIN_AUTHID_KEY0x)
NDID 3430
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
```

```
CFG_ZONE 00001
CUR_ZONE 00001
MRT
ERL
ECL 0
FDN
TGAR 1
LDN NO
NCOS 3
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SCPW 123456 (AUTOLOGIN_PASSWD_KEY0x)
CLS CTD FBD WTA LPR MTD FND HTD ADD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDD
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD FITD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
AHA DDGA NAMA
DRDD EXR0
USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD MSNV FRA
PKCH MWTD DVLD CROD CROD
CPND_LANG ENG
RCO 0
HUNT
PLEV 02
PUID
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 MCR 2257 0 (AUTOLOGIN_ID_KEY0x)
CLS CTD FBD WTA LPR MTD FND HTD ADD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDD
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD FITD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
AHA DDGA NAMA
DRDD EXR0
USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD MSNV FRA
PKCH MWTD DVLD CROD CROD CPND_LANG ENG
RCO 0
HUNT
PLEV 02
PUID
DANI NO
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
```

```
MLNG ENG
DNDR 0
KEY 00 MCR 2257 0 (AUTOLOGIN_ID_KEY0x)
CPND
CPND_LANG ROMAN
NAME John, Smith
XPLN 24
DISPLAY_FMT FIRST,LAST
01 SCR 2222 0 (AUTOLOGIN_ID_KEY0x)
CPND
CPND_LANG ROMAN
NAME EMS, Alpha Trials
XPLN 24
DISPLAY_FMT FIRST,LAST
02 HOT U 2005374 MARP 0
03 MCR 5549 0
CPND
CPND_LANG ROMAN
NAME Smith, John,
XPLN 24
DISPLAY_FMT FIRST,LAST
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 4
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31
DATE 29 JUN 2010
```

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 Phone to the Media Application Server (MAS) 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 24 for an example of the IMAGES section of the 11xxeSIP.cfg.

Image file size

Individual images cannot exceed 512 MB 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 16: 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 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.

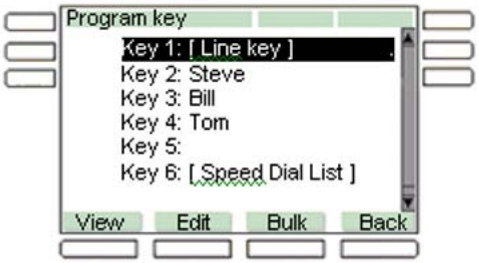


Figure 19: Main feature key programming screen showing Speed Dial List provisioned on key 6

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.

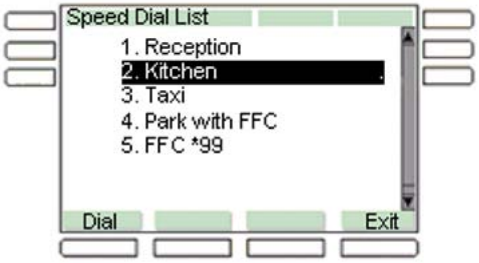


Figure 20: Example of a Speed Dial List

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 17: 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.

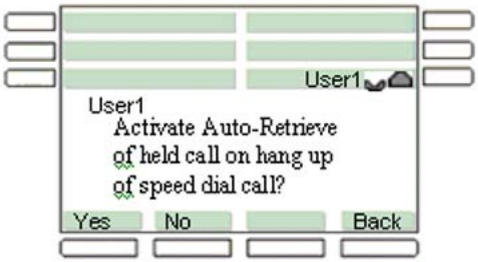


Figure 21: Speed Dial Key creation — last step

The following table describes the function of the context-sensitive soft keys for the Auto Retrieve screen.

Table 18: Context-sensitive soft keys for the Auto Retrieve screen

Context-sensitive soft key	Action
Yes	Enables the Speed Dial Auto Retrieve behavior.

Context-sensitive soft key	Action
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 that must be loaded through provisioning.

```
speedDialList.txt [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 type=spdial
```

Roaming profiles

Roaming profiles enable the user to obtain the same settings when they are log 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@macadamian.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 42.

Address book file

The Address book file represents each contact [contact] and each group [group] (name only). A contact provides attributes to specify nickname, SIP address, group and whether it is a friend. An example of the syntax is provided below:

```
[version] id=12345  [contact]
nickname=lpg address=lpg@macadamian.com group=macadamian 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 [key] sections, each describing a single key. Each key has the following mandatory attributes:

- 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.

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, presense 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. 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.

Note:

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
```

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 the key is not shown. The key appears only when an Expansion Module is attached.

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
- DEFAUT_SPEEDDIAL_LIST
- DEFAUT_CUSTOMKEYS_FILE

For more information about the device configuration file, see Feature configuration commands on page 42.

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 enable.

If the login banner is configured a 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 22: Login Banner

The following table describes the function of the context-sensitive soft key for the Login Banner screen.

Table 19: 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 20: 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 21: Outside actions on content

Key or action	Result
Inbox	No action.
Outbox	No action.
Directory (Address book)	No action.

Key or action	Result
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.
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, 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) is an alternate presence monitoring mechanism for the IP Deskphone that allows presence functionality on proxies supporting BLF, such as SCS proxy. The IP Deskphone subscribes to receive presence information for watched users through notifications. The BLF mechanism allows the user to subscribe to the proxy and receive the presence state list for all the users it is configured to watch. The provisioning of the proxy configures the watch lists for users.

The proxy involved supports BLF and has a mechanism for setting the lists of watchers and presentees. The UI is not available to a user to enable or disable this feature. If the IP Deskphone is provisioned for this feature, it makes use of it.

If enabled, and the proxy provides notifications to the user, the IP Deskphone uses the notifications to update any speed dial keys that receive presence information in the BLF notifications.

This feature is provisioned using BLF_ENABLE and BLF_RESOURCE_LIST_URI. Once this feature is activated, properly provisioned, and connected to the server that supports this feature, the BLF feature can be used. It is used whenever a speed dial key is provisioned on the IP Deskphone. An icon is assigned to the speed dial key; the status of the user is reflected in the display icon assigned to the speed dial key.

Figure 23: Call States and corresponding Presence icons

Universal Serial Bus Device support

The Avaya 1110 Series IP Deskphones provides 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 and USB memory stick are supported. 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 Deskphone starts 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 22: 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]	—

Commands	Parameters	Remarks
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.

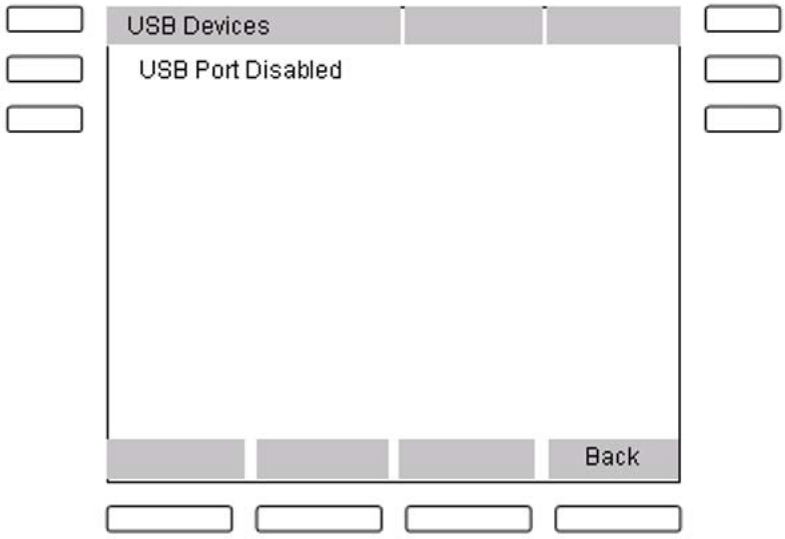


Figure 24: USB Devices information screen — USB Port disabled

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 provided below.

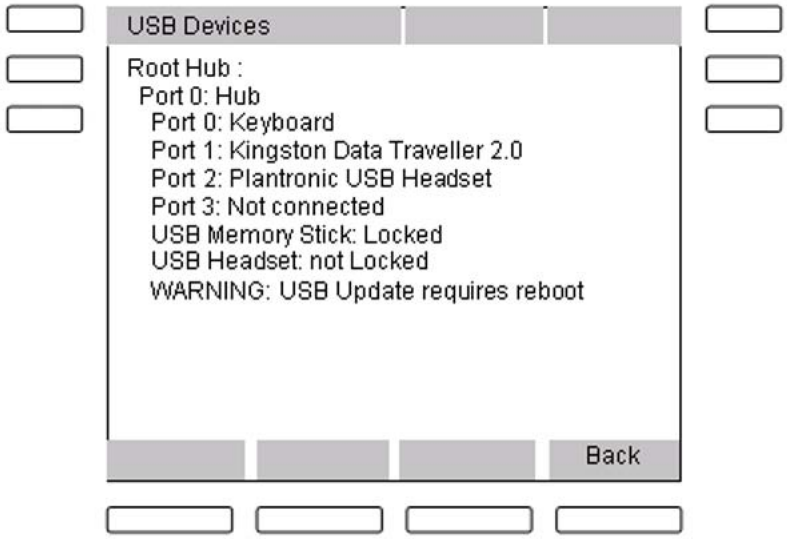


Figure 25: Sample USB Devices information menu

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 26: USB Locks screen

The following table describes the options that are listed on the USB Locks screen.

Table 23: 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.
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.

USB Locks options	Description
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 24: 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 27: Warning screen on page 159.
Back	Discards the changes, dismisses the USB Locks menu and returns you to the previous screen.

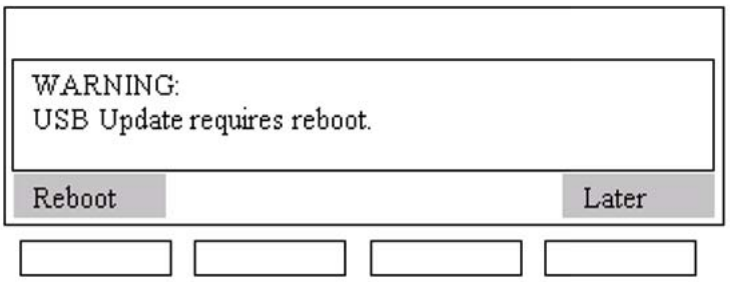


Figure 27: Warning screen

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 to a Hotline Phone. From a Hotline Phone, you can automatically make a call 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 25: 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 26: 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

Parameter name	Description	Default value
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
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.

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 27: 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 165.
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 28: Voice-VLAN and Data VLAN on page 171).

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.

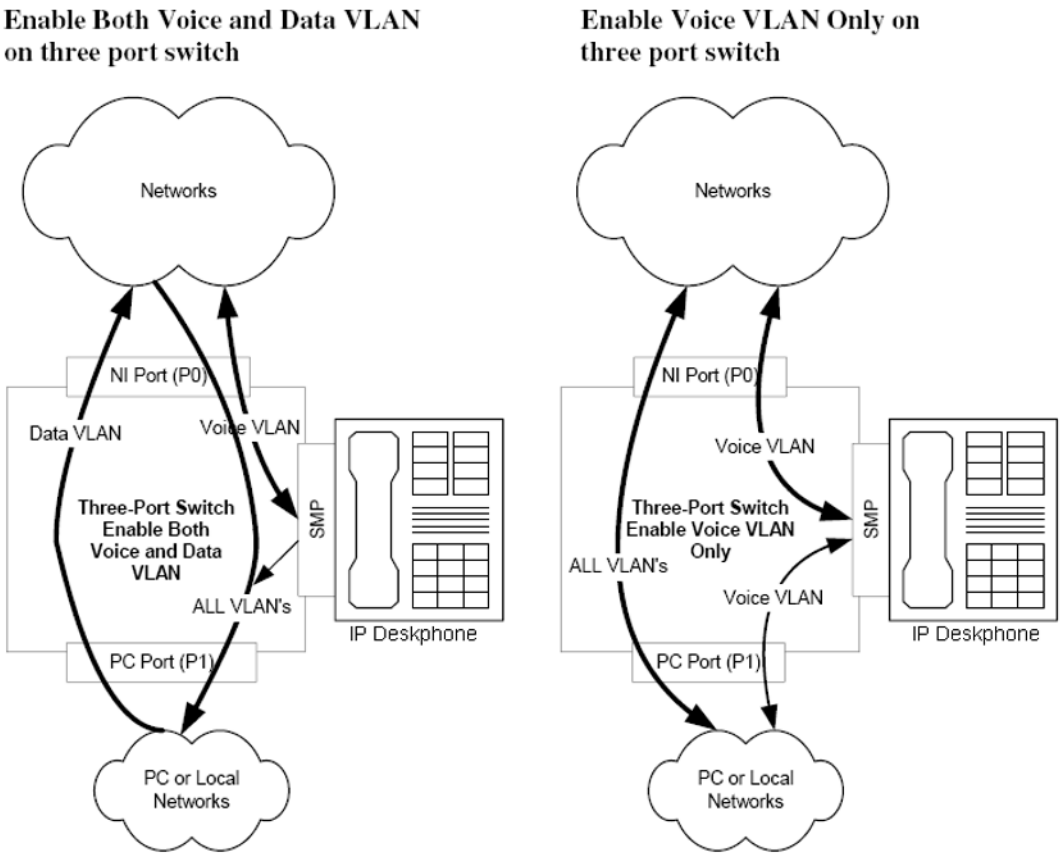


Figure 28: Voice-VLAN and Data VLAN

Table 28: 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	Tagging the incoming frame untagged and forwarding it to network port. Replacing the incoming frame tagged with VLAN

Ports	Voice VLAN enabled	Data VLAN enabled	Both Voice and Data VLAN enabled
		VLAN other than Data-VLAN and forwarding it to network port. Sending all kinds of frames.	other than 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 106 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 240
- EAP-PEAP on page 241
- EAP-TLS on page 240

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 29: 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 = 2001, 2002, 2004, 2007, 1110, 1120E, 1140E, 1150E, 1165E Software = software version. “0604D97” is an example only.
System Capabilities	Length = 4 System capabilities = 0x24 [Telephone + Bridge] Enabled capabilities = 0x24 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.

TLV	Fields
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 mode0x0800 - 100BASE-TX half duplex mode 0x0400 - 100BASE-TX full duplex mode0x0002 - 1000BASE-TX half duplex mode0x0001 - 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 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 = 2 for 2001/2002/2004/1110 IP Deskphones Power Class = 3 for 2007/1120E/1140E/1150E/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

TLV	Fields
	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 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:
	2001 NTDU90 = 4 2002 NTDU91 = 4.5 2004 NTDU92 = 4.5 2007 NTDU96 = 10 1110 NTYS02 = 51210 NTYS181220 NTYS191230 NTYS201120E NTYS03 = 8 1140E NTYS05 = 8 1150E = 7.6 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:
	2001: Code 01 2002: Code 01 2004: Code 01 2007: Code 01 2033: Code 03 1210: Code 04 1220: Code 04 1230: Code 04 1110: Code 01 1120: Code 01 1140: Code 01 1150: Code 02 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: 2001, 2002, 2004, 2007, 1110, 1210, 1220, 1230, 1120E, 1140E, 1150E , 1165E.

PC Client Softphone interworking

The interworking feature allows the user to access the functionality of the SIP Avaya 1110 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.

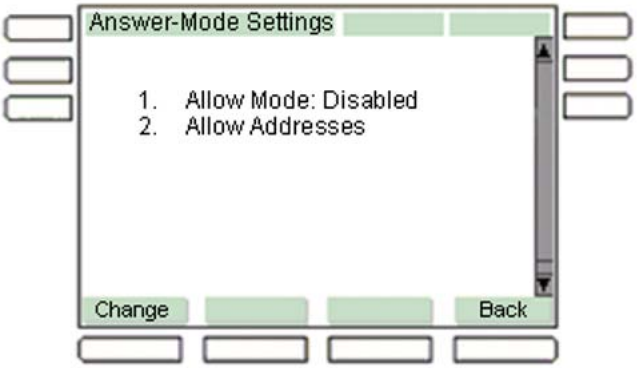


Figure 29: Answer-Mode Settings screen

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.

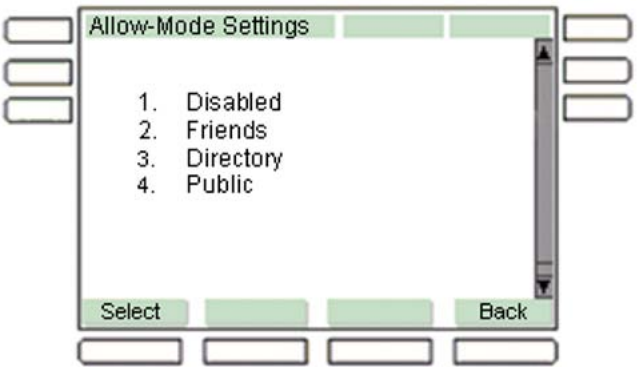


Figure 30: Allow-Mode Settings screen

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.

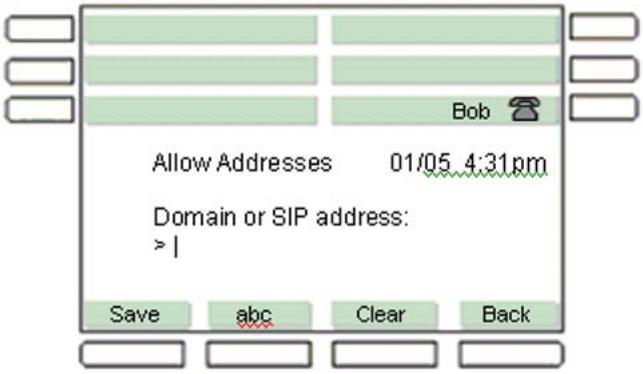


Figure 31: Allow Addresses screen — first entry

The following screen is an example of the Allow Address screen if one (or more) domain or SIP address is in the system.

Figure 32: 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 178), 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.

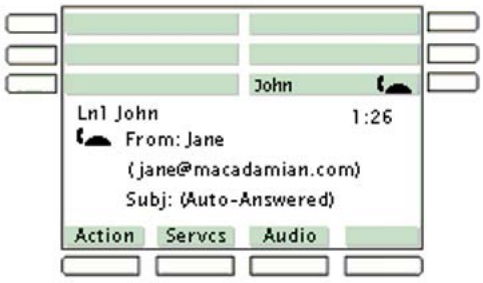


Figure 33: Example of a Notification screen indicating an Auto-Answered call

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-AS 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

.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-Application Sever (ARTS-AS).

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 or receiving calls from the 911 Emergency operator. 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.
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-AS 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 [DSN]	The network domain (DSN) 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.	2
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

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 section specifies the behavior of the following security features:

- SIP over TLS
- Connection persistence
- SRTP
- SFTP
- SSH

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 Deskphone SSH or SFTP.	None	Non-null string Maximum: 49 characters

Parameter	Description	Default value	Boundaries
Password	The password that must be entered when connecting to the IP Deskphone through SSH, SFTP.	None	Non-null string Maximum: 49 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:
  - `Error: User ID size: 4-12` – appears if a valid user ID is not provided.
  - `Error: Password size: 4-12` – appears if a valid password is not provided.
  - `Error: User ID size: 4-12 Error: Password size: 4-12` – 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=tcp>
  ```

  Important:

  The transport parameter is not TLS. Some older implementations of servers or clients that supported TLS may still continue to use TLS. The presence of TLS indicates that the server or client prefers TLS to be used for communication.

  SIP Software Release 3.2 adds transport=tcp to the contact header when using TCP or TLS.

- VIA header – contains the transport protocol used to send a request. For example, Via: SIP3.2/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 30: Provisioning parameters summary

Parameter	Purpose	Default	Allowed
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	Configures the TCP and TLS ports used when connecting to the SIP domain.	TCP: 5060 TLS: 5061	Integer

Parameter	Purpose	Default	Allowed
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 REGISTER_RETRY_TIME REGISTER_RETRY_MAX TIME	Configuration values that affect connection persistent.	<add link to table.	See Managing connection persistence on page 202.
SRTP_ENABLED SRTP_MODE	SRTP configuration values.	NoBE-2MLines	BE-2MLines BE-CapNeg 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	OffSuccessFailureBoth

Parameter	Purpose	Default	Allowed
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. 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_PASSW ORD	Indicate whether the Admin Password is hashed or not.	NO	YES, NO
ENALBE_LOCAL_ADMIN_ UI	Configure the availability of the local administration UI on the IP Deskphone.	YES	YES, NO

Parameter	Purpose	Default	Allowed
HASH_ALGORITHM	Hash algorithm.	SHA1	SHA1, MD5
MKI_ENABLE	Use Master Key Identifier (MKI) or not.	NO	YES, NO
ADMIN_UI_ENABLE	Configure the availability of the local administration User Interface on the IP Deskphone.	YES	YES, NO
SECURE_UI_ENABLE	Configure 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_EXPI RY	The date that the configured ADMIN_PWD is no longer valid, and a new password must be downloaded from the provisioning server.	Empty	Timestamp

Note:

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:

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:

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 31: 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: 65535Disabled: 0
SIP TCP Port	The listening port on the IP Deskphone for incoming TCP requests.	5060	Min: 1024 Max: 65535Disabled: 0
SIP TLS Port	The listening port on the IP Deskphone for incoming TLS requests.	0	Min: 1024 Max: 65535Disabled: 0

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 disabled (configured as zero), and the incoming UDP and TCP listening ports must be disabled (configured as zero).

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.

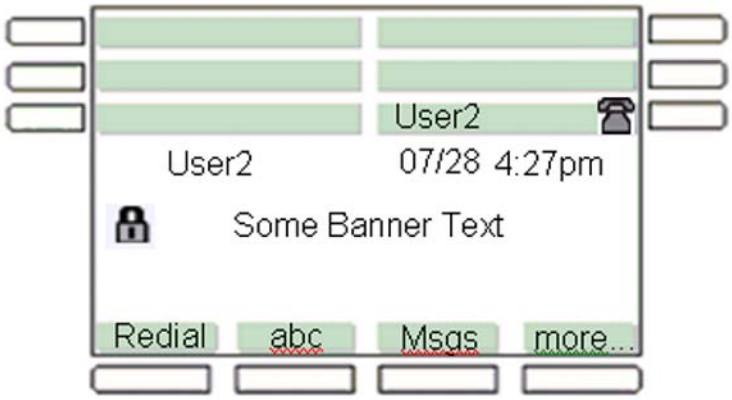


Figure 34: Security icon enabled

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 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 32: 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 + TCP + TLS	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.
IP Deskphon	The IP Deskphone only has TLS configured for	The IP Deskphone registers using SIP over	If the IP Deskphone is unable to contact the

Configuration	Description	Expected result	Possible results
e: TLS only Server: UDP + TCP + TLS	sending requests to the server. The IP Deskphone must have a device certificate installed if the server is configured for mutual authentication.	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.	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.

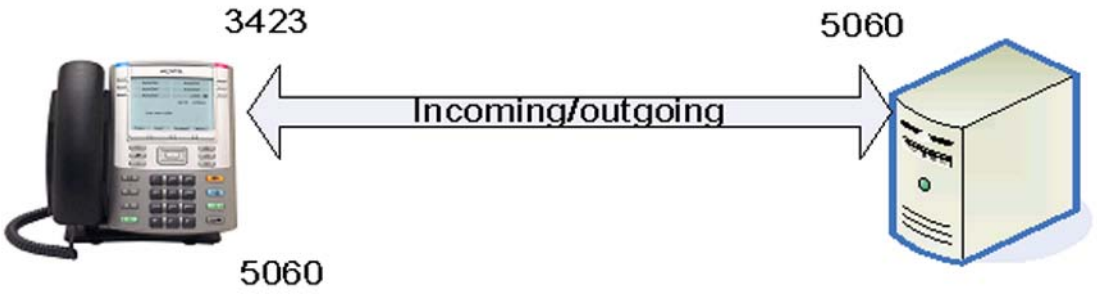


Figure 35: Incoming/Outgoing with connection reuse

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.

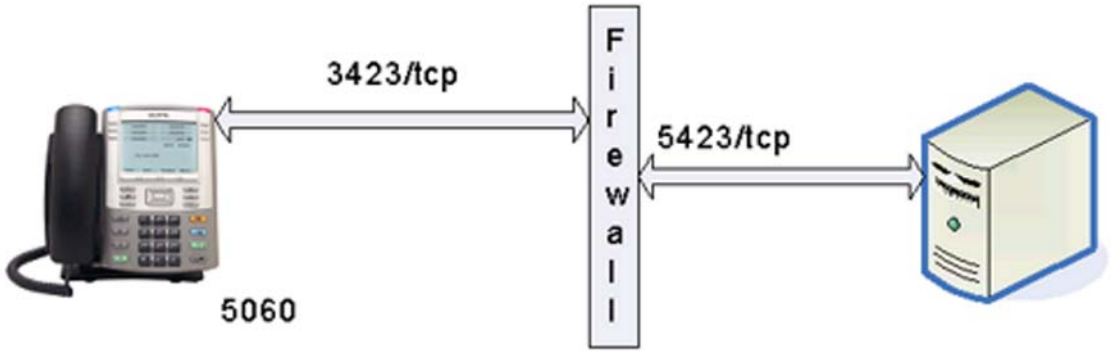


Figure 36: Connection reuse and a firewall

Table 33: 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: 15 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	1800	Min: 600 Max: 1800

Parameter name	Description	Default value	Boundaries
	registration retry attempt. This value, measured in seconds, is the maximum value that the IP Deskphone waits in between retry attempts		

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.

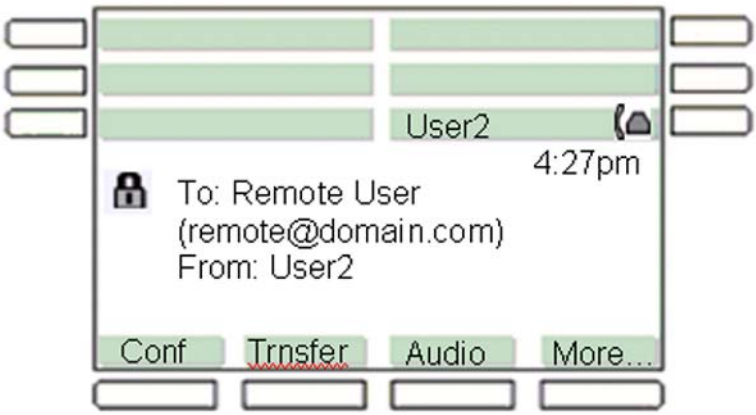
Table 34: SRTP properties

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

Parameter	AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_32
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 35: 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.

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.

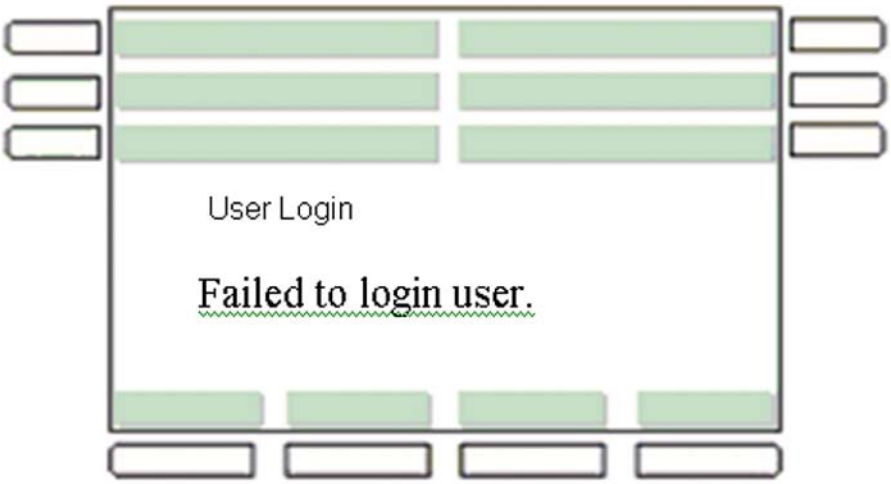


Figure 37: New login failure notification

The following notification appears on the display screen when the user successfully logs on.

Figure 38: Basic login notification

The following notification appears on the display screen when the user successfully logs on when Login Notify with Time is enabled.

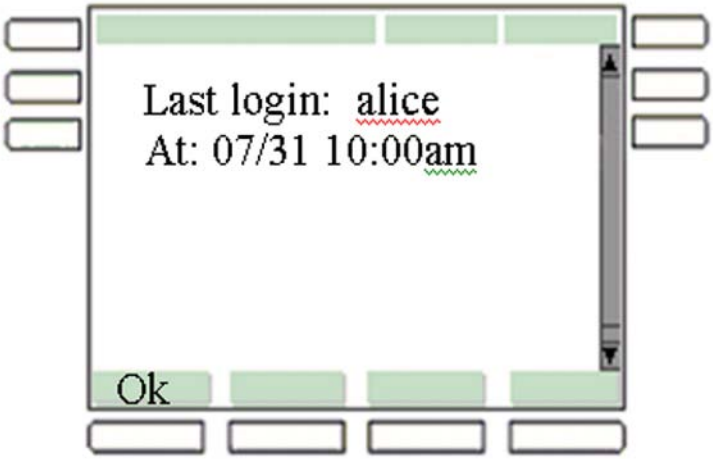


Figure 39: Basic login and time notification

The following notification appears on the display screen to notify the user of the last unsuccessful log on attempt made.

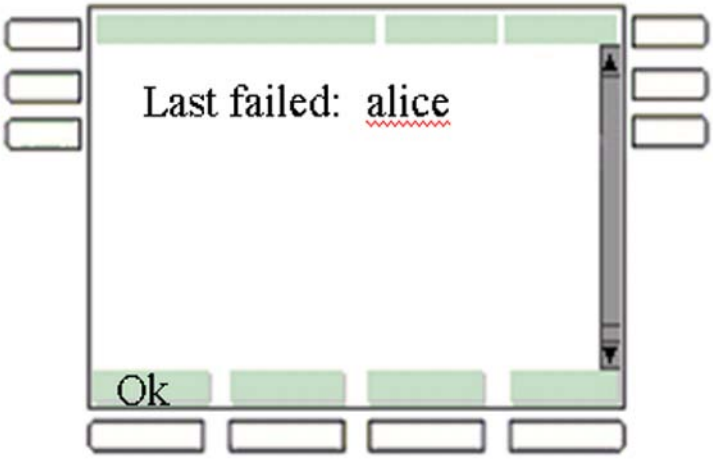


Figure 40: Login failure notification

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.

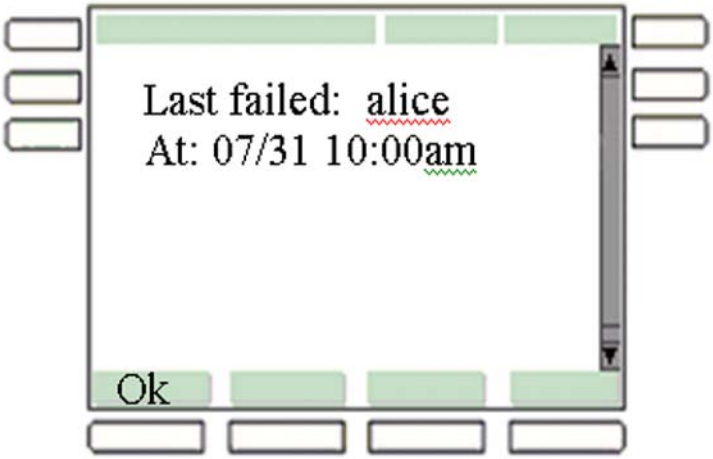


Figure 41: Login failure with time notification

The following notification appears on the display screen to notify the user the last successful and unsuccessful log on attempts made.

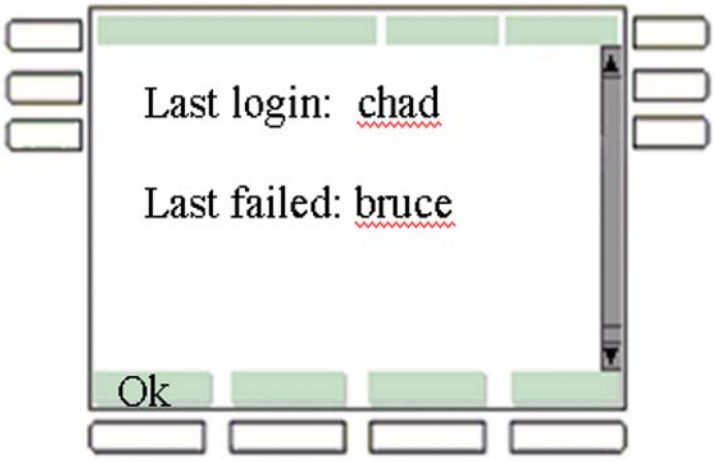


Figure 42: Login and login failure notification

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.

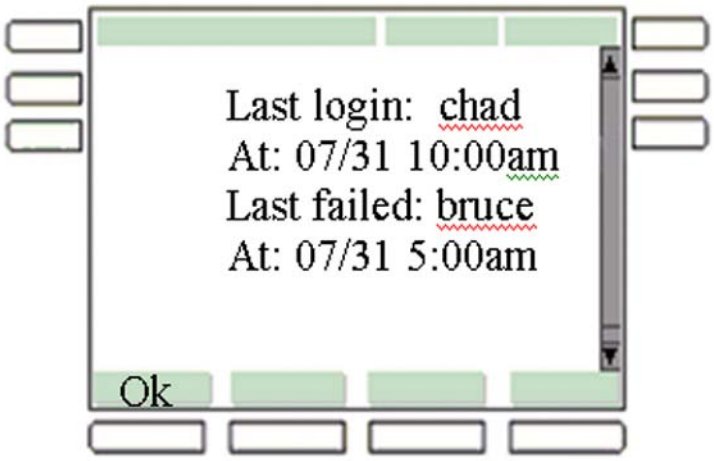


Figure 43: Login and login failure with time notification

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.

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 36: Audio codecs supported by IP Deskphone

Codecs	Description
G.722	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.

Table 37: 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)	ptime (milisec)	Channels
G.711 a-law	8	PCMA	8000		20	1
G.711 u-law	0	PCMU	8000		20	1
G.711 a-law	8	PCMA	8000		30	1
G.711 u-law	0	PCMU	8000		30	1
G.729A + 40ms ptime	18	G729	8000		20	1
G.729B	18		8000	8	20	1
G.722	9	G722	8000	48	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.

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 38: Audio codecs supported by IP Deskphone

Codecs	Description
G.722	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

Codecs	Description
	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.

Table 39: 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)	ptime (milisec)	Channels
G.711 a-law	8	PCMA	8000		20	1
G.711 u-law	0	PCMU	8000		20	1
G.711 a-law	8	PCMA	8000		30	1
G.711 u-law	0	PCMU	8000		30	1
G.729A + 40ms ptime	18	G729	8000		20	1
G.729B	18		8000	8	20	1
G.722	9	G722	8000	48	20	1
G.723.1	4	G723	8000	5.3 6.3	30	1

Codec	Payload type	SDP encoding name	Clock rate (HZ)	Bit rate (kbps)	ptime (milisec)	Channels
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 Device Configuration

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 40: Sample Device Configuration entries

```
AUDIO_CODEC CodecID text_description
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 G729 and G723 codecx, 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, which disables the codec entry.

If you remove all codecs from the allowed list, the IP Deskphone resets to the default list of codecs.

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 new 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 all together and without specifying codec through the new 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.

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 41: Examples of the ordered lists of Codecs

Supported by IP-set	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

Chapter 15: Certificate-based authentication

Certificates 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 and provisioning servers.

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

Certificate based authentication is provided on the IP Deskphone by installing trusted root certificates, device certificates, and Certificate Trust Lists (CTL). Device Certificates are installed by importing a password protected PKCS#12 file. A PKCS#12 file contains both private and public key pair of the certificate.

CTL is a predefined list of trusted server certificates which the IP Deskphone views as trusted endpoints. It is used 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, as well.

The administrator is able to define the Security policy on the IP Deskphone using Security Policy file. 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.

After the certificates are installed, they can be used by SIP, HTTP, and EAP applications running on the IP Deskphone to provide secure connections with the corresponding servers, which results in SIP-TLS, HTTP, and EAP-TLS connections.

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 uses 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.

HTTPS is used to securely download provisioning files from a provisioning server. These files include configuration file, such as 11xxeSIP.cfg and also other configuration and resource files specified by 11xxeSIP.cfg.

In order for the IP Deskphone to perform certificate based authentication, the following components needs to be installed on the IP Deskphone:

- Trusted root certificates
- Device certificate
- CTL
- Security policy

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 AUTOPROTOCOL HTTPSFILENAME 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 Desklphone, 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.

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. Currently, SIP Software 3.2 supports installation of only one device certificate.

The following sections describe the process used to install a device certificate on the IP Deskphone.

- 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 PKCS#12 file 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 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: _ - . ! @ $ % & + : ^.

Installing a device certificate using PKCS12

Use the following procedure to install a device certificate using a PKCS#12 file.

Installing a device certificate using PKCS12

1. Add a [DEV_CERT] section to 11xxeSIP.cfg to enable the IP Deskphone to import a PKCS#12 file.

   An example of the [DEV_CERT] section is as follows:

   ```
   [DEV_CERT]
   FILENAME "*.p12"    # must include "*" symbol to be substituted with
   MAC                              # address or it will be rejected.VERSION
   <n>PROFILE 1                 # profile indexPURPOSE -1             #
   bitflag with all purposes it can be used for
                                # (default is -1 = ALL)
   ```

   - FILENAME attribute points to the PKCS#12 file name. The file name must include the * symbol which is 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.
   - 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).
   - VERSION attribute determines if the file should be downloaded by comparing this VERSION with the VERSION stored in the corresponding device certificate profile.

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 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.

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

The IP Deskphone uses the Certified Trust List (CTL) method to verify the various network elements, such as proxy servers and provisioning servers.

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 Certificate Administration option in 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 [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**.

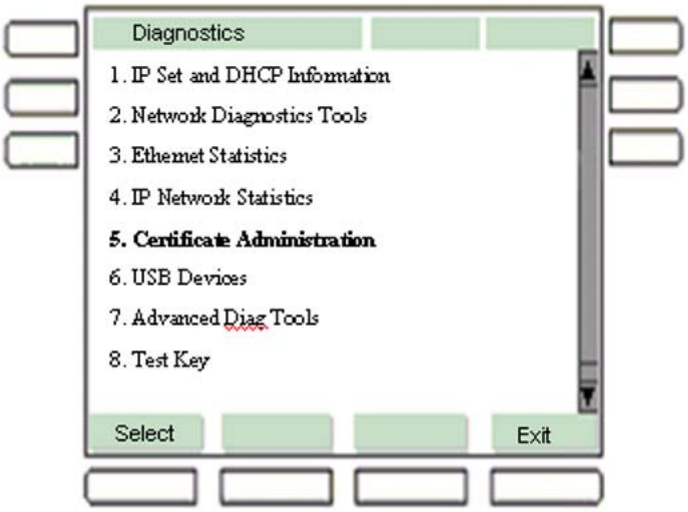


Figure 44: Diagnostics main menu

Certificates Administration main menu

The certificates administration screen displays the following options:

- Trusted Certificates
- Device Certificates
- CTL

To access the Certificates Administration screen from the Network screen, select **Device Settings** > **Diagnostics** > **Certificate Administration**.

Figure 45: Certificates administration main menu

The following table describes the function of the context-sensitive soft keys for the Certificates Administration screen.

Table 42: 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:

CRL is not supported.

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:

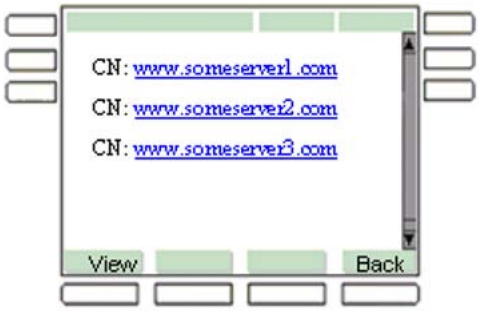


Figure 46: Trusted Certificates screen

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 43: 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 47: 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 Phone displays a warning confirmation screen.

The following table describes the function of the context-sensitive soft keys for the Trusted Certificates Details screen.

Table 44: 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 48: 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 45: 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:

Context-sensitive soft key	Action
	• 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 49: 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 50: CTL certificate screen

The following table describes the function of the context-sensitive soft keys for the CTL screen.

Table 46: 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 51: CTL Certificate details screen

You can use the PDT shell command to view an installed CTL.

The following is an example 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 52: Example of command output

Important:
The CTL file size must not exceed 20 Kbytes.

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 NOSECURITY_LOG_UI_ENABLE NOKEY_SIZE
1024KEY_ALGORITHM KEY_ALG_RSATLS_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

You can install a Security Policy file on the phone by using the configuration file 11xxeSIP.cfg.

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.

```
-> securitypolicyCUST_CERT_ACCEPT =
VAL_MANUAL_ASIGN_SIP_CONFIG_FILES = NOCERT_EXPIRE =
DELETE_CERTSEC_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.

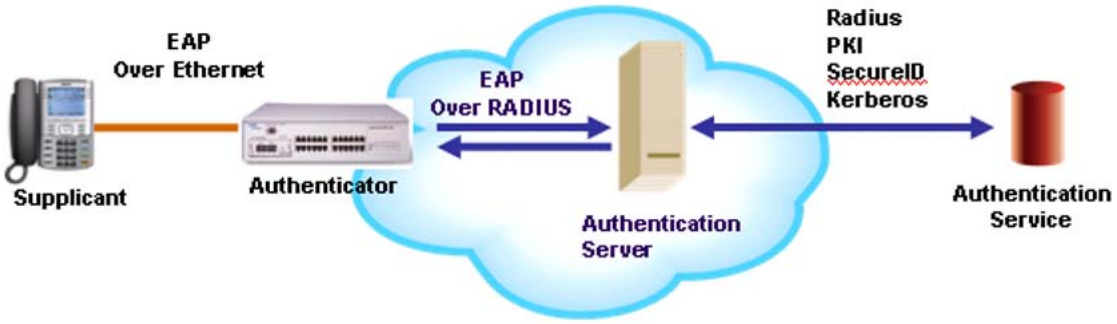


Figure 53: 802.1x and EAP network architecture

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 54: 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 47: 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. For more information, see Trusted Root certificate on page 220 .

The device certificate can be installed using the PKCS 12 download method. For more information, see Installing a device certificate using PKCS12 on page 222

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 220.

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/dot1x/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.

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 222.

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

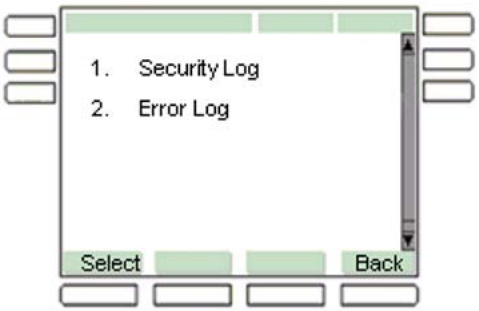


Figure 55: Logs main menu

When the user selects a log file, the screen displays each log item on a full screen, as shown in the following figure:

Figure 56: Log item screen

The following table describes the function of the context-sensitive soft keys for the log item screen.

Table 48: 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
0x1031EAP_INVALID_ROOT_CERTIFICATE 0x1032EAP_TLS_AUTH_FAILURE
0x1033EAP_PEAP_AUTH_FAILURE 0x1034
```

The following is a list of certificate-related events and failures logged in the Security Log.

```
SLC_AVAYA_CERTIFICATE_IMPORTED
0x0006SLC_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 0x000CSLC_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
0x1002SLC_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 238.

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 243.

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 244.

Creating a signing certificate

You can create a signing certificate using OpenSSL.

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
  - o Validity fields
  - o 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 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. 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 creates 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 creates 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.
2. Click **Self-Service**
3. Select **Keycode Retrieval System**
4. Select **GLOBAL LOGIN** from the list for the login location that you would like to use for access to the Keycode Retrieval System.
5. Select **IP CLIENTS** from the list for the product whose keycodes you would like to access.
6. When registration is validated, go to http://support.avaya.com/css/appmanager/public/support and log in to KRS.
7. To view the KRS User Guide, select **Product family > Documentation > Forms and User Guides > KRS IP Clients User Guide_v2.ppt**.

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)—Executes on the IP Phone and calls the server locally.
- License Client—Resides in the IP Phone 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).

The following figure demonstrates a high-level view of the licensing framework interactions and components.

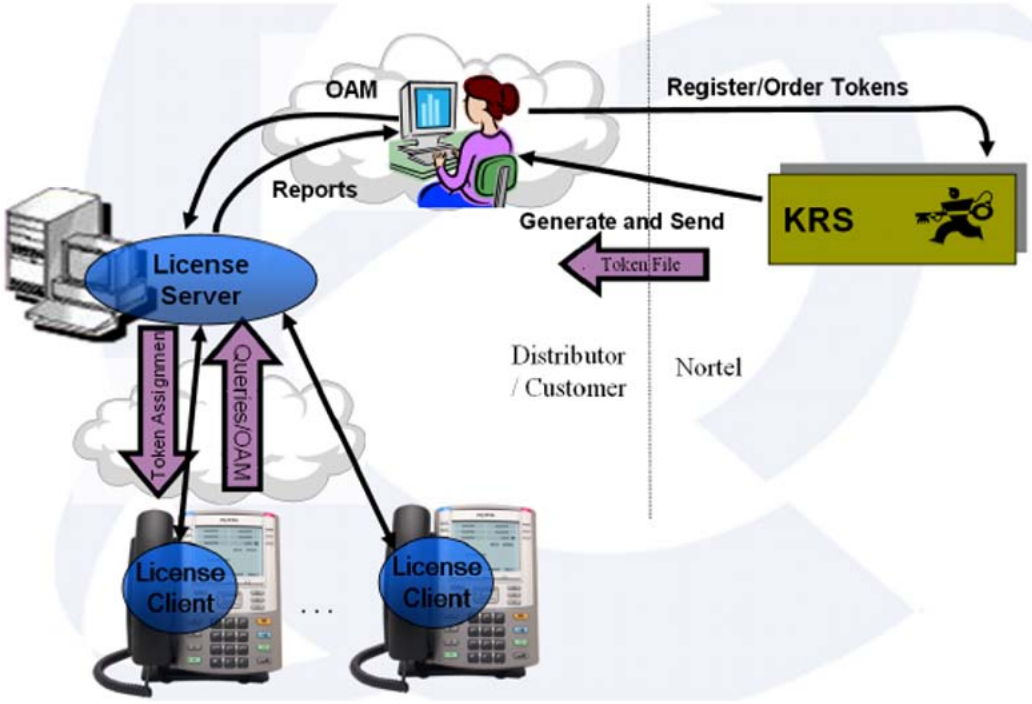


Figure 57: Licensing framework interactions and components

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 a 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).
- The license file is keyed for the IP Deskphone so that the license is only valid on a specific IP Phone.

- 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

Use the following procedure to download the license file from the provisioning or TFTP server.

Downloading a 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 24.
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, 1165eSIP.cfg, 1220eSIP.cfg, or 1230eSIP.cfg.

   The [LICENSING] section specifies a wild card filename which uses the IP Deskphone MAC address as the filename with the cfg prefix and suffix.

   For example:

   ```
   [FW]
   DOWNLOAD_MODE AUTO
   VERSION 3.00.xx.yy
   PROTOCOL TFTP
   FILENAME SIP 1140_e03.02.xx.yy.bin
   PROMPT NO
   [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 iptokenMAC.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.

You can download the node-locked license file from the provisioning or TFTP server by performing the following actions:

Any new license file on the provisioning server overwrites the current file on the IP Deskphone. After the IP Deskphone retrieves the configuration during start up, the IP Deskphone

downloads the license file, renames the license file as `ipclient.lic` , and saves the licensing file in the IP Deskphone Security File System (SFS).

[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 49: 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 FORCED VERSION 0625C4E FILENAME 11xxes.bin
PROTOCOL TFTP SERVER_IP 47.11.183.165 SECURITY_MODE 0 [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. Licensing Info**. Enter admin password (if prompted).

Figure 58: 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 gets an additional token. This means that the Enhanced Feature Set is available when the IP Deskphone connects to an Avaya Server.

Access Licensed Features list

Licensed Features screen can be accessed through the IP Deskphone using **Prefs > Network > Licensing** and selecting 2. Features.

Figure 59: Licensing menu

The Licensable Features list displays.

Figure 60: Licensable Features

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 61: 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 62: 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
- Licensed expired
- Released

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 63: 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 the extra line Tokens Required: 1. This line is displayed only when the IP Deskphone connects to an Avaya Server.

Figure 64: 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
- Licensed expired
- Released

Invalid or no license file

The following figure is an example of an invalid or no license file.

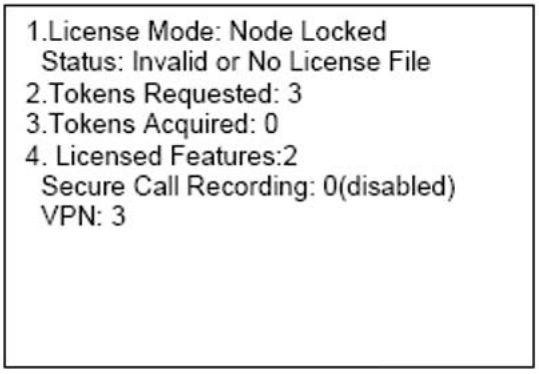


Figure 65: License information — Invalid or no license file

Evaluation period

When the IP Deskphone arrives from the fac tory, 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. ; Once the evaluation period expires, there is no way to reset it.

The following figure is an example of the IP Deskphone in a 15 days evaluation period.

Figure 66: IP Deskphone in a 15 day 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 67: 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.

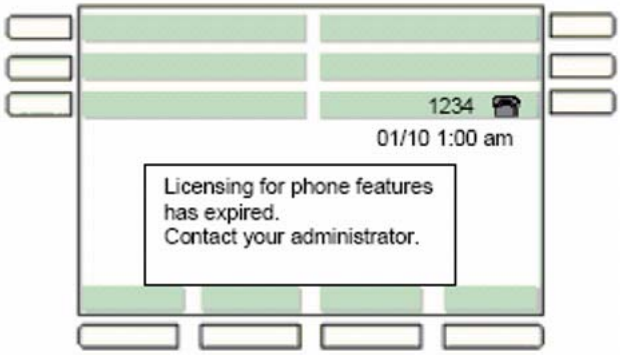


Figure 68: License expiry warning

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.

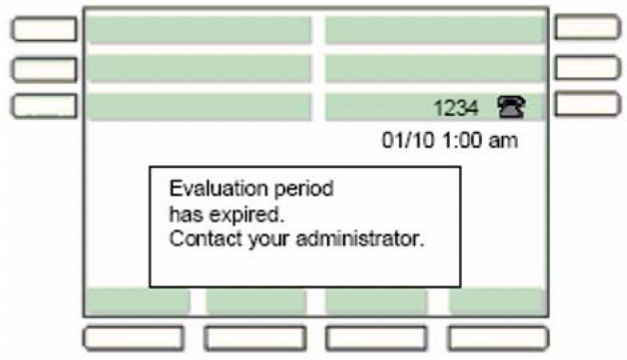


Figure 69: Evaluation period expiry warning

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.

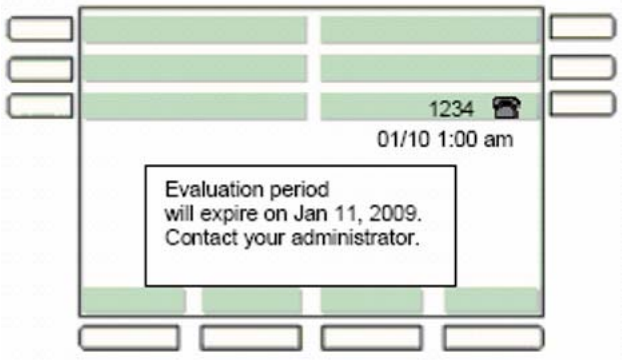


Figure 70: Evaluation threshold warning

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.

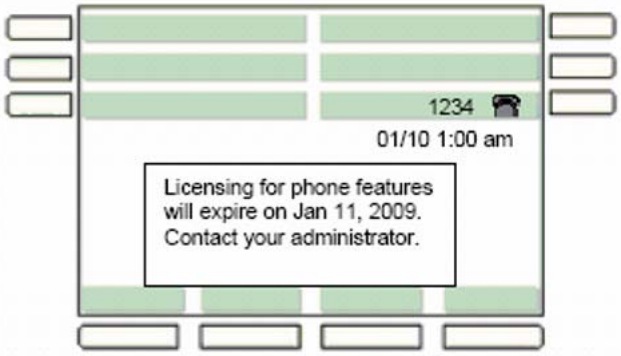


Figure 71: License expiry threshold warning

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, CS 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
- Broadsoft Broadworks SCA

The following advanced features are available with two tokens or if the IP Deskphone is registered to a recognized Avaya server (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.

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 50: 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 51: 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 Phone IP address, DNS Server address, Provisioning Server address, and SIP Server addresses.

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 Phone IP address, DNS Server address, and SIP Server address.

Maximum 1 Phone IP, 2 SIP Server IPs, and 1 Provisioning Server IP are supported. The first 2 SIP Server IPs 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 SIP proxy IPv4–mapped address, the IP Deskphone registers with its IPv4 address. If the DHCPv6 server is configured with SIP proxy IPv4-

mapped and IPv6 addresses, the DHCPv6 client calls the destination address selection algorithm and select 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.nortelexample.com, sip2.nortelexample.com,
sip3.nortelexample.com, sip4.nortelexample.com, sip5.nortelexample.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 52: 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

Method	Supported?	Comments
		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

3xx Response	Send	Receive	Comments
			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.
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.

4xx Response	Send	Receive	Comments
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.
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

4xx Response	Send	Receive	Comments
			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

Header field	Supported?
Accept-Encoding	Yes
Accept-Language	Yes
Alert-Info	Yes
Allow	Yes
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

Header field	Supported?
Priority	Yes
Privacy	Yes
Proxy-Authenticate	Yes
Proxy-Require	Yes
RAck	Yes
Reason	Yes
Record-Route	Yes
Refer-To	Yes
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

Subscription type	Supported	Avaya Call Server specific
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 on page 281
- Local diagnostic tools on page 283
- How to access the Diagnostics menu on page 284
- IP Set and DHCP information on page 285
- Network Diagnostics tools on page 287
- Ethernet Statistics on page 289
- IP Network Statistics on page 292
- USB Devices on page 293
- Advanced Diag Tools on page 294
- Test key on page 295
- Logging System on page 298
- Problem Determination Tool (PDT) on page 300
- Diagnostic Logs on page 309

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 Telnet session using the IP address of the IP Deskphone (for login and password, contact Avaya).

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.

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 setting 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. An audible beep indicates a field entry must be made before advancement to the next parameter.
-

Software Download Failure

If you are having trouble downloading software, review the following.

- Is the TFTP IP address correct within the IP Deskphone Device Settings menu?
- 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 Configure the provisioning server on page 23. 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 select **Srvcs, System, Erase User Data** 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 UNIStim 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, 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.

Table 53: Diagnostics menu options on page 283, describes the Diagnostics menu options.

Table 53: 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

Diagnostics option	Description
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.
Advanced Diag Tools	Provides information for setting up the following configuration parameters: • Auto Recovery (enable/disable) • SSH (enable/disable) • Port Mirroring (enable/disable) • 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 72: 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:

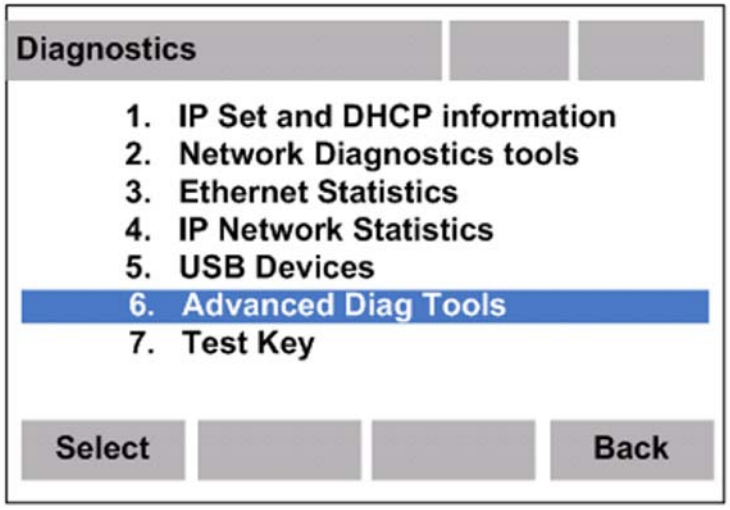


Figure 73: Diagnostics menu screen

The following table describes the function of the Navigation keys for the Diagnostics screen.

Table 54: 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:

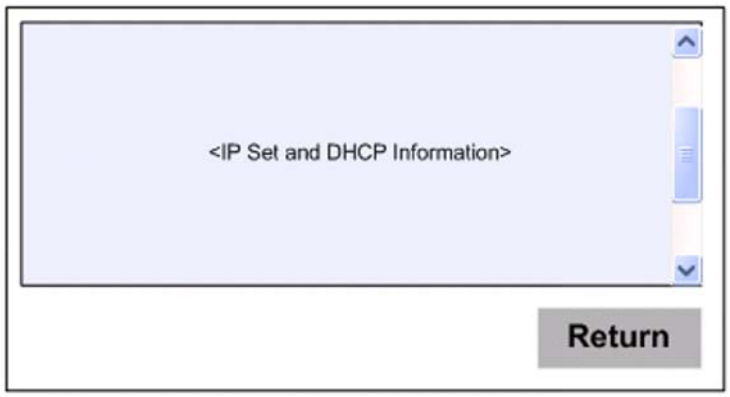


Figure 74: IP Set and DHCP information screen

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 55: 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 56: Navigation

Key	Action
Return	Press the Return context-sensitive soft key to cancel this screen and return to the Diagnostics menu.

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 75: 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 57: 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 58: 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:

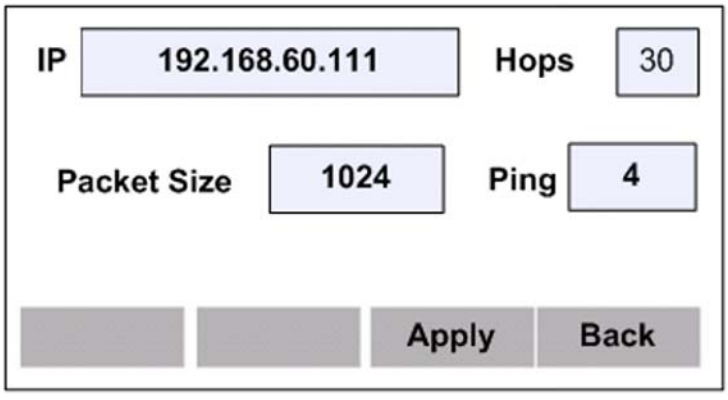


Figure 76: Network Diagnostics tools (Config) screen

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 59: 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 60: 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 screen from the Diagnostics menu, choose **Ethernet Statistics**.

The following screen appears:

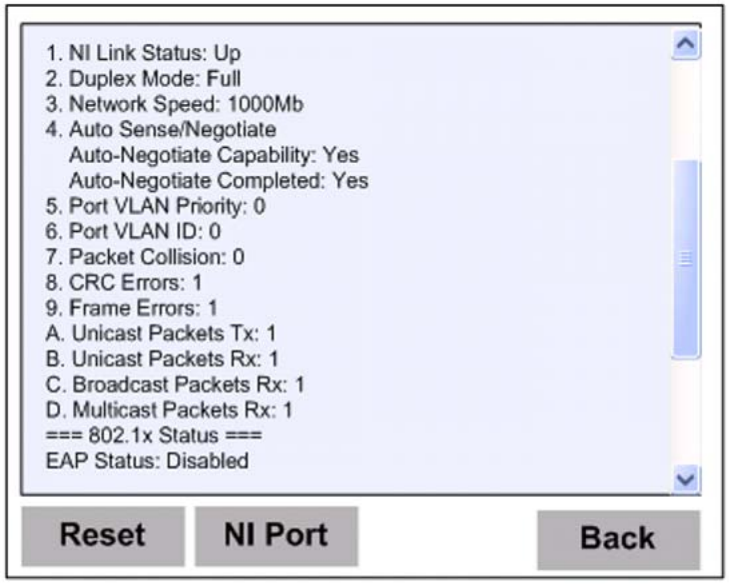


Figure 77: Ethernet Statistics (NI Port) screen

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 61: 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 62: 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:

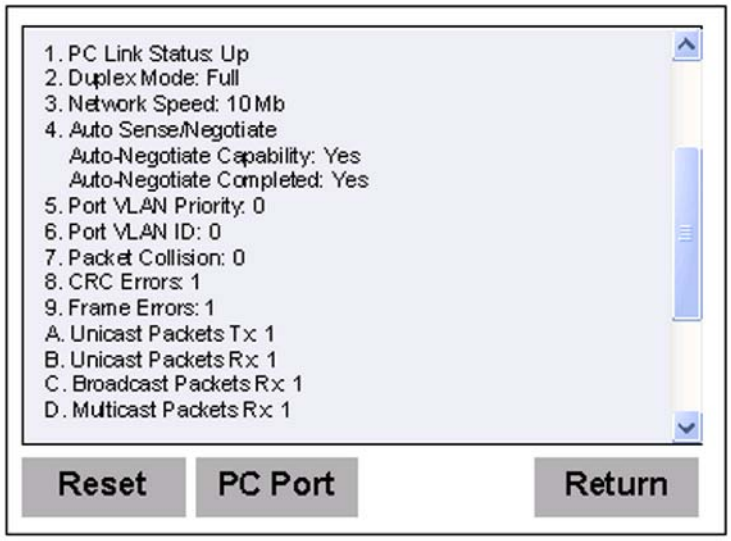


Figure 78: Ethernet Statistics (PC Port) screen

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 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 63: 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 64: 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:

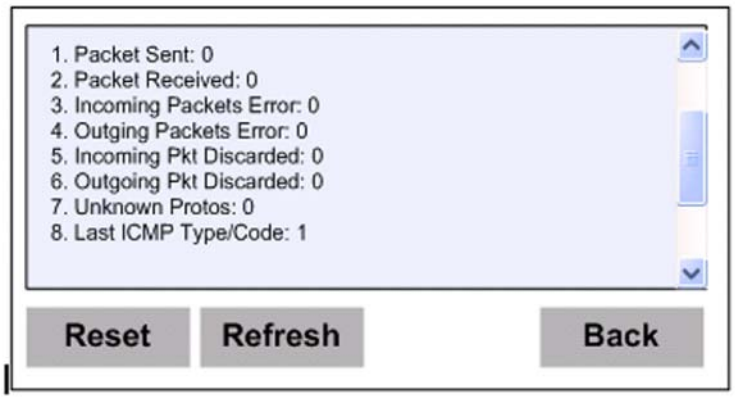


Figure 79: IP Network Statistics screen

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 65: 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 66: 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:

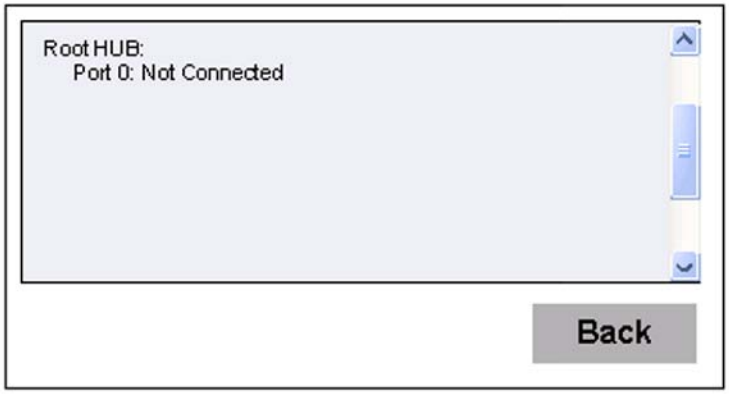


Figure 80: USB Devices screen

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 67: 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 68: 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

To access the Advanced Diag Tools screen from the Diagnostics menu, choose **Advanced Diag Tools**.

The following screen appears:

Figure 81: Advanced Diag Tools screen

The following table describes the function of the context-sensitive soft keys for the Advanced Diag Tools screen.

Table 69: 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 70: Navigation

Key	Action
Up and down arrows	Use the up and down arrows to scroll through a list of statistics information.

Key	Action
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 Port Mirroring field behavior depends on the device configuration flag defined by the administrator. A device configuration file parameter manages the PC Port Mirroring option:

PORT_MIRROR_ENABLE [YES | No]

The command determines whether or not the option can be managed:

- If PORT_MIRROR_ENABLE is Yes, then you can activate or deactivate the option. The Port Mirroring prompt in the Advanced Diag Tools menu is enabled and can be modified.
- If PORT_MIRROR_ENABLE is No, then you cannot manage the option. The Port Mirroring prompt in the Advanced Diag Tools menu is disabled (dimmed); Port Mirroring is disabled.

The default value for the PORT_MIRROR_ENABLE is No. This means that PC Port Mirroring is not active.

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:

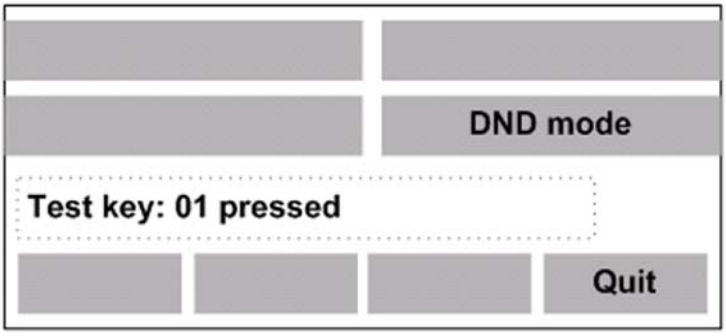


Figure 82: Test key screen

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 71: 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 72: 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 73: 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... 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:

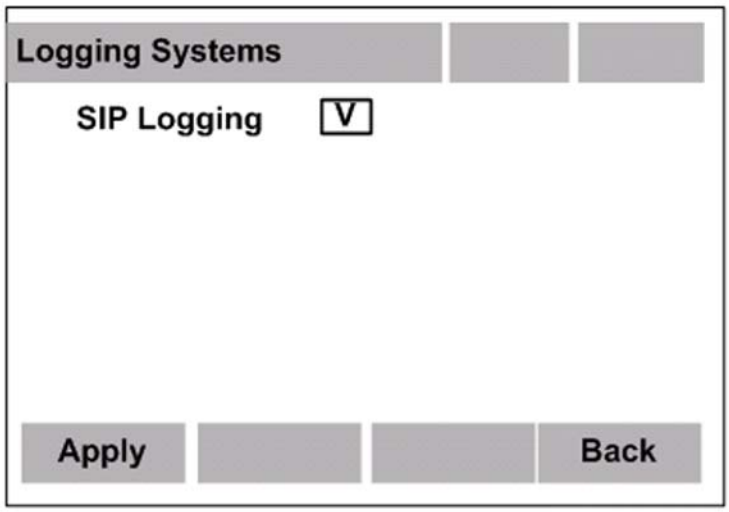


Figure 83: Logging Systems screen

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 74: 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 75: 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.

The 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 Telnet session. Access is restricted by admin ID and password.

The PDT supports the following set of commands:

Table 76: List of PDT commands

Command	Description
prtlog >prtlog<mngr_dest>	• Prints a content of the ECR-log file. • 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
l	Prints all task information
ti <taskName | task id>	Print task information

Command	Description
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 • 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:

Command	Description
	• 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 297.
routePrint	Displays GW IPv6 addresses.
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.

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 77: 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**********
 *** SIPdomainl 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 78: Alarms, logs and diagnostics configuration commands

Component	Flag	Description
PC Port Mirroring parameter which can be modified in the Advanced Diag Tools dialog. See 2.2.1.6	PORT_MIRROR_ENABLE	Determines whether the option can be managed or not. • 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 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 manage the option. • The values are YES and NO. The default value is NO (disabled).
Memory Monitor. See 2.2.4	MEMCHECK_PERIOD	Determines the time period in seconds when the Memory

Component	Flag	Description
		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
tSl811Int  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-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
```

Figure 91: Example of the SIP-log file (continued)

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 182.

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 178.

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 client to non secure client, 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`

Index

Numerics

802.1ab Link Layer Discovery Protocol (LLDP) 173
802.1x (EAP) authorization 173
802.1x (EAP) device ID 173
802.1x (EAP) password 173

A

Animated screensaver 6, 143
Automatic provisioning at a preconfigured time 23
Automatic provisioning at power-up 23
Avaya 1165E IP Deskphone with SIP Software illustration 15
Avaya IP Deskphones parts list 21

B

background 143

C

Call Origination Busy 182
certificate requirements 193
Certified Trust List 226
Checking the UNIStim software version on an IP Deskphone in use 96
Checking the UNIStim version on a new IP Deskphone 96
Communication Server 1000 and MADN 138
Communication Server 2000 140
Communication Server 2100 140
Configuration file 24
Configuring the provisioning server 23
Configuring the TFTP server 98
connection persistence 189
Connection persistence 189
Connections on the IP Deskphone 93
Convert SIP FW to UNIStim FW 102
Converting UNIStim software to SIP Software 101
Converting UNIStim software to SIP Software using TFTP 101
Create the device configuration file on the provisioning server 30
Creating the SIP provisioning file on the provisioning server 24
CTL 226
Custom banner problem 281
Customer service 7

D

Default error handling 275
Device configuration commands, details 35
Device configuration commands, list 30
Device configuration file example 30
Dialing function description 84
Dialing plan 84
Dialing plan declarations section sample 84
Dialing plan digit map section sample 84
Dialing plan file on the provisioning server 82
Dialing plan sample 82
dialing plan variable definitions sample 84
Downloadable WAV files 86
Downloading SIP Software from the Avaya Web site 101
Downloading the SIP Software to the provisioning server 24, 95
Downloading UNIStim software through TFTP on bootup 98
DRegex 85
DRegex rules 85

E

Emergency call location information 165
Emergency service dialing plan configuration 165
Emergency Services 163, 164

F

Feature configuration commands 42

G

Getting help from a distributor or reseller 7
Getting product training 7
Getting technical documentation 7
Getting technical support from Avaya 7

I

Identify the current version of UNIStim Software 96
Images 142
Installation overview 17
Installing the IP Deskphone 93
IP Deskphone diagnostics 281
IP Deskphone Getting Started Card 16
IP Deskphone restrictions 187

L

Licensable features 254
Local Diagnostic Tools 283

M

MADN 5, 137, 140
Mandatory keywords in the provisioning file 24
Media security 5
MLPP 182
Multi-Level Precedence and Preemption 182
Multiple Appearance Directory Number 5, 137, 140

N

NAT configuration commands 75
NAT firewall traversal 168
Network requirements 21

O

Optional keywords in the provisioning file 24

P

Port functions on the three-port switch when VLAN is enabled 170
Precedence 182
Preemption 182
Preinstallation checklist 21
Proactive Voice Quality Monitoring (PVQMon or VQMon) 119
Provisioning error displayed 281
Provisioning file example 24
Provisioning file supported sections 24
Provisioning server 23
Provisioning updates 23
PVQMon or VQMon Server set-up 120

Q

QoS and ToS commands 71

R

Re-authorization 182

S

screensaver 142
Screensaver 6
SDP and Call Hold 278
Secure file transfer 190
Secure Real-time Transfer Protocol 204
Secure Real-time Transport Protocol 5
Secure Shell Handler 5
Security 5
Security features 6
Security Policy file 108, 237
Server and network configuration commands 36
Server unreachable after power up 281
Service package restrictions 187
Session description protocol usage 278
SFTP 189
Signing certificate 246
SIP DTMF Digit transport 279
SIP header fields 275
SIP messages supported 269
SIP methods 269
SIP over TLS 189
SIP overview 15
SIP responses 270
SIP responses - 1xx Response 270
SIP responses - 2xx Response 271
SIP responses - 3xx Response 271
SIP responses - 4xx Response 272
SIP responses - 5xx Response 274
SIP responses - 6xx Response 275
SIP security authentication 279
Slideshow 142
Software conversion failure 281
Software download failure 281
Speakerphone exclusive to 911 Emergency 182
SRTP 5, 189
SSH 5, 189, 190
Support instant messaging 280
Supported subscriptions 279
System commands 80

T

TCP operation overview 191
Three-port switch and VLAN functionality 170
TLS 5
TLS operation overview 191
Tone configuration commands 74
Transport layer protocols 278
Transport Level Security 5

U

Upgrade and convert the IP Deskphone software. 95
Upgrade the SIP Software 95
Upgrade the UNIStim software version 98
Upgrade to the minimum UNIStim Software 96
USB headsets 159

V

Vertical services (MADN) 141
Voice-VLAN and Data VLAN 170
VQMon - how it works 120
VQMon configuration commands 77
VQMon set-up 119