avaya.com

Product Bulletin

Bulletin Number: P-2010-0016-Global
Date: 28 February 2010

UNIStim Software Release 4.1 for IP Deskphones

Revision History		
Date	**Revision #**	**Summary of Changes**
28 February 2010	Original bulletin	This is the original publication

Introduction

Avaya is pleased to announce the availability of UNIStim software release 4.1 for IP Deskphones. UNIStim software release 4.1 makes available the following software versions for the following IP Deskphones:

UNIStim Software Release 4.1	
IP Deskphone	**Software**
2007 IP Deskphone	0621C7D
1110 IP Deskphone	0623C7J
1120E IP Deskphone	0624C7J
1140E IP Deskphone	0625C7J
1150E IP Deskphone	0627C7J
1165E IP Deskphone	0626C7J
1210 IP Deskphone	062AC7J
1220 IP Deskphone	062AC7J
1230 IP Deskphone	062AC7J

Avaya recommends an upgrade to this release of software for all applicable IP Deskphones and Call Servers at the earliest convenience. This release is being provided as a no charge update to all customers, although some of the functionality delivered in UNIStim software release 4.1 can only be activated with a purchased license.

UNIStim software release 4.1 for IP Deskphones is available for download from the “Software Download” link under “Support and Training” on the Nortel website located at: http://support.nortel.com. The software is available by phone model under “Phones, Clients and Accessories”. **These software loads have not been introduced as the default loads for the IP Deskphones shipped from Avaya.**

UNIStim software release 4.1 for IP Deskphones delivers enhancements to Avaya’s IP Telephony Solution and delivers general quality improvements. The enhancements available include:

- UNIStim 4.0 functionality delivered onto the 1165E IP Deskphone
- Quality improvements to Secure Signaling using DTLS
- Adjustable open-microphone warning tone during Zone Paging
- UNIStim VPN client interoperability extended to include Avaya VPN Gateways

Enhancements

UNIStim 4.0 functionality delivered onto the 1165E IP Deskphone (applies to the 1165E IP Deskphone only)

UNIStim software release 4.1 delivers the complete UNIStim 4.0 software functionality onto the 1165E IP Deskphone. When UNIStim software release 4.0 availability was announced in November 2009, no 1165E IP Deskphone load was included in the suite of software loads. The UNIStim software release 4.1 load for the 1165E IP Deskphone – specifically software load 0626C7J – finally delivers the UNIStim 4.0 functionality onto the 1165E IP Deskphone.

The functionality delivered with UNIStim software release 4.0 that is also now available on the 1165E IP Deskphone includes:

- UNIStim VPN Client (UVC)
- Feature and Application Licensing
- Secure Signaling using DTLS
- Secure Call Recording (SCR)
- Design for Operability (DfO)
- Enhancements to Certificate Support

For a brief description of the functionality delivered with UNIStim software release 4.0, please refer to the Product Bulletin P-2009-0143-Global, UNIStim Software Release 4.0 for IP Phones.

For complete details on the functionality delivered with UNIStim software release 4.0, or more specifically, details on the delivery of this functionality onto the 1165E IP Deskphone, please refer to the IP Phones Fundamentals NN43001-368 or the IP Phone 1165E User Guide NN43101-102.

Quality improvements to Secure Signaling using DTLS (applies to all the IP Deskphones)

UNIStim software release 4.0 first delivered the capability to encrypt the signaling communication between the IP Deskphone and the call server using standards-based Datagram Transport Layer Security (DTLS). DTLS guarantees a secure connection between the IP Deskphone and the call server ensuring the integrity and confidentiality of call control.

But numerous DTLS quality improvements have been delivered in UNIStim software release 4.1. For this reason, Avaya strongly recommends an upgrade to UNIStim software release 4.1 in all environments where one wishes to use DTLS.

At the time of this writing, the only Avaya call platform also supporting DTLS is the Communication Server 1000. Support for DTLS was also introduced with Communication Server 1000 release 6.0.

Support for DTLS was planned with Communication Server 1000 release 6.0. But at the time of this writing, a quality issue persists preventing the delivery of the secure signaling using DTLS feature with release 6.0 of Communication Server 1000. Since the quality of the DTLS feature is not at an acceptable level, support for DTLS is being delayed on the Communication Server 1000 until the quality concern can be addressed. Correction to the quality concern will be delivered with a Communication Server 1000 signaling Service Update (SU). The delivery of the SU is expected shortly. Updates will be provided as more details become available.

Until support for secure signaling using DTLS can be delivered, to secure the signaling between the IP Deskphone and the Communication Server 1000, one has to deploy the Secure Multimedia Controller (SMC) 2450.

Adjustable open-microphone warning tone during Zone Paging (applies to the 2007, 1120E, 1140E, 1150E and 1165E IP Deskphones)

One of the applications supported by the Nortel Application Gateway is “Zone Paging”. In an environment in which “Zone Paging” is enabled, an IP Deskphone end user can initiate a page from his or her phone. When a page is initiated in handsfree mode the IP Deskphone’s microphone becomes active. For security reasons, in order to notify the end user that the phone’s microphone is active, a periodic warning tone, also known as an “alternate tone” is generated by the phone.

In some environments this periodic warning tone can be disruptive. In UNIStim software prior to release 4.1 the periodic warning tone volume could not be adjusted. But with UNIStim software release 4.1, the periodic warning tone volume can be adjusted to suit the needs of different environments.

UNIStim software release 4.1 introduces a new parameter to the Info Block to allow the periodic warning tone volume to be adjusted. The new Info-Block parameter allowing the periodic warning tone volume to be auto-provisioned is provided in the table below. Please refer to Appendix B for the complete list of parameters supported within the Info block.

Periodic Warning Tone Provisioning Parameter		
xatv	‘0’ no tone ‘1’ -36dB ‘2’ -26dB ‘3’ -20dB ‘4’ -16dB ‘5’ -13dB ‘6’ -9dB ‘7’ -6dB ‘8’ 0dB	Alternate tone volume

If the periodic warning tone volume value is set to 0, representing “no tone”, then no tone is generated by the phone. Instead the handsfree indicator LED flashes while the microphone is active.

Feature Advisement

Manual configuration of the periodic warning tone volume is not supported.

If a secure connection to the Application Gateway is provisioned, the periodic warning tone is not generated by the phone and thus the volume control parameter is ignored.

UNIStim VPN Client interoperability (applies to the 1120E, 1140E, 1150E and 1165E IP Deskphones)

UNIStim software release 4.0 introduced an integrated VPN Client inside the 1100 Series IP Deskphones. The UNIStim VPN Client (UVC) is supported on all the 1100 Series IP Deskphones phones except the 1110 IP Deskphone. The UVC allows the IP Deskphone to be deployed remotely and maintain a connection back to the corporate network by establishing a Virtual Private Network (VPN) tunnel. The UVC feature can be used by telecommuters or remote workers to maintain a corporate phone connection from their remote location.

The UVC within the IP Deskphone is the client end of the tunnel. The corporate end of the tunnel is terminated by an enterprise VPN router or gateway. UNIStim software release 4.0 introduced interoperability with the Avaya (formally Nortel) VPN Router (NVR) family running software release 8.00 or greater.

UNIStim software release 4.1 expands the interoperability of the UVC to also include the Avaya (formally Nortel) VPN Gateway (NVG) family running software release 8.0.1 or greater.

Product Advisements

The following is a list of advisements associated with UNIStim software release 4.1. Some advisements remain from previous releases of software, whereas other advisements reflect new or changed behavior introduced with UNIStim software release 4.1. Advisements that are new to UNIStim software release 4.1 or have changed since previous releases of UNIStim software are prefixed with “NEW”.

NEW – Slight change to the contrast level on the icons on the 1100 Series Expansion Module when the Module is attached to an 1165E IP Deskphone (applies to the 1165E IP Deskphone only)

After upgrading to firmware 0626C7J on the 1165E IP Deskphone, if an 1100 Series Expansion Module is attached, the user will notice slight changes to the contrast levels on icons on the Expansion Module. The changes were necessary to improve the display quality during low contrast settings.

1110 IP Deskphone may experience a double reboot when upgrading software (applies to the 1110 IP Deskphone only)

If the 1110 IP Deskphone is upgraded (or downgraded) to (from) UNIStim software release 4.1 while Asian font files are installed in the phone, a double reboot may occur during the upgrade (or downgrade) procedure. After the second reboot, the phone will be fully operational and will maintain its selected language choice. This advisory is simply to provide notification that the upgrade (or downgrade) procedure may now be lengthened due to the double reboot.

IP Deskphone may appear locked when downloading large font files over the VPN (applies to the 1120E, 1140E, 1150E and 1165E IP Deskphones)

It has been discovered that when using the VPN feature on home based phones, that the phone may appear locked when downloading large files (such as font files) to the phone. This issue is due to Internet delay and the fact that the phone’s TFTP client is inefficient to transfer large files across the Internet. Unfortunately the IP Deskphone does not have a progress indication to inform the user that the download is still in progress and in fact the phone is not locked.

Users are advised to wait should the phone be downloading font files over the Internet. As a additional measure, one can also look to the back of the phone at the link activity LED to confirm network activity is still occurring and in fact that the phone is not locked.

The DOWNLOAD_MODE cannot be FORCED for license keycode files (applies to the 1100 Series IP Deskphones)

An issue was discovered with the DOWNLOAD_MODE command in the [LICENSING] section of the phone’s configuration file. Unfortunately, only the AUTO option can be used at this time to download license keycode files into the phone. Support for the FORCED option in DOWNLOAD_MODE is being fixed and will be delivered in a future build of UNIStim software.

A USB Hub cannot be used to simultaneously connect a mouse and a keyboard to the USB port of the 2007 IP Deskphone (applies to the 2007 IP Deskphone only)

The USB port on the 2007 IP Deskphone will not support the connection of both a mouse and a keyboard connected via a USB hub. The USB port on the 2007 IP Deskphone is restricted to supported either a USB mouse or a USB keyboard, but not both simultaneously.

A 2-step upgrade may be required to load UNIStim software release 4.1 on the 2007 IP Deskphone (applies to the 2007 IP Deskphone only)

Due to changes in the memory structure of the 2007 IP Deskphone, a 2-step upgrade may be required to load UNIStim software release 4.1 onto the 2007 IP Deskphone if the upgrade is performed with TFTP. If the 2007 IP Deskphone is currently running UNIStim software release 3.2 (0621C6M) or greater then one will be able to upgrade using TFTP directly to UNIStim software release 4.1. But if the 2007 IP Deskphone is running any software prior to UNIStim software release 3.2 and the upgrade is performed with TFTP, then the phone must first be upgraded to UNIStim software release 3.2 before subsequently upgrading to UNIStim software 4.1. The 2-step up upgrade is not required if the upgrade is performed from the call server using UFTP.

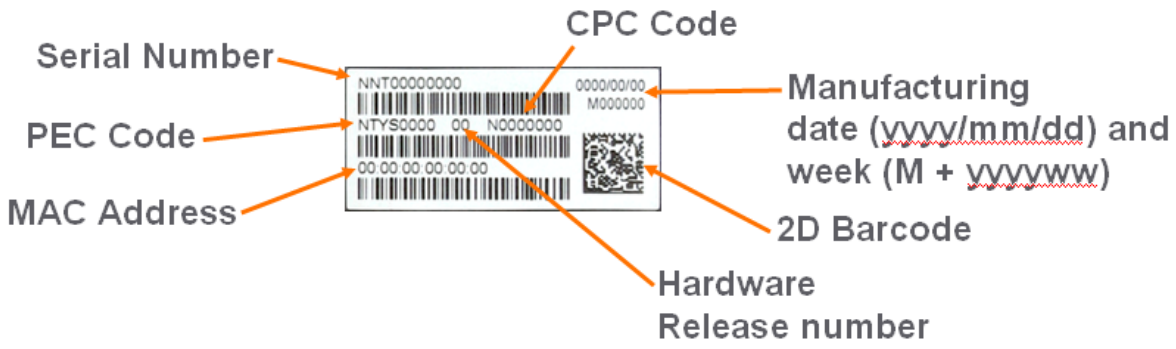
Minimum allowable software on the 1150E IP Deskphone with new hardware changes (applies to the new hardware 1150E IP Deskphone only)

Hardware changes in recent 1150E IP Deskphones impose a restriction on the minimum allowable software version on these phones. The new hardware phone will absolutely accept an upgrade to UNIStim software release 4.1. But the new hardware 1150E IP Deskphone will NOT accept a downgrade to any software version previous to UNIStim software release 3.4 (0627C6T). Any attempt to download a software version previous to UNIStim software release 3.4 will result in the phone responding with a denial of software downgrade response.

The minimum allowable software is dependant on the phone's PEC and hardware release number and is provided in the table below:

Minimum Allowable Software			
PEC	**Hardware Release**	**Description**	**Minimum Software**
NTYS06AAE6	07	1150E IP Deskphone Graphite with Icon Keycaps (RoHS)	UNIStim 3.4 (0627C6T)
NTYS06ABE6	07	1150E IP Deskphone Graphite with English keycaps (RoHS)	UNIStim 3.4 (0627C6T)

The below Figure 1 provides an explanation of where to identify the PEC and Hardware Release Number on the white product label (located on the back of the IP Deskphone).



If UFTP software download is used within the Communication Server 1000 environment, Avaya recommends that the software image for the 1150E IP Deskphone on the signaling server be upgraded minimally to UNIStim software release 3.4.

Communication Server 1000 release 5.0, and greater, will interpret denial of software downgrade responses from the new hardware phones. However, Communication Server 1000 prior to release 5.0 requires patch MPLR23154 to interpret correctly the phone's denial of software downgrade responses. Failure to install the patch introduces the risk that the call server may continuously try and downgrade the software thereby denying service to the phone. MPLR23154 is available at VO status on the Nortel ESPL website and is deployed only by contacting your Technical Support Representative

If TFTP software download is used, and the TFTP server is not upgraded to UNIStim software release 3.4 or greater, the TFTP server will continuously try and downgrade the software in the phone. The new hardware phone will prevent the downgrade resulting in the phone being denied service.

In a Communication Server 1000 environment containing SRG and SRG50 branch office systems, two SRG Smart Updates (SU) exist to allow the SRG and SRG50 platforms respectively to interpret denial of software downgrade responses from the new hardware phones. Failure to install the SU introduces the risk that the call server may continuously try and downgrade the software thereby denying service to the phone.

For SRG 200 and SRG 400 release 1.5, the denial of software downgrade support is included in BCM.R400.SU.System.024 and later.

For SRG50 release 3.0, the denial of software downgrade support is included in BCM050.R300.SU.System-197 and later. This SU is not available for SRG50 release 2.0

If the above SRG SU are not installed then the "umsUpgradeAll" Main Office system command should not to be executed when the branch office sites has the new hardware 1150E IP Deskphone and the IP Deskphone software at the Main Office precedes UNIStim software release 3.4.

For complete details on the minimal allowable software for the new hardware changes in the 1150E IP Deskphone please refer to Clarify Bulletin 2010009988 Rev3, Minimum IP Phone Software Requirement for IP Phone 1150E.

Minimum allowable software on the new hardware 1120E IP Deskphone and new hardware 1140E IP Deskphone (applies to the new hardware 1120E IP Deskphone and the new hardware 1140E IP Deskphone)

Hardware changes in recent 1120E IP Deskphones and 1140E IP Deskphones impose a restriction on the minimum allowable software version on these phones. The new hardware phones will absolutely accept an upgrade to UNIStim software release 4.1. But the new hardware 1120E IP Deskphone and new hardware 1140E IP Deskphone will NOT accept a downgrade to any software version previous to either UNIStim software release 3.1 or UNIStim software release 3.4 respectively depending on the level of hardware changes. Any attempt to download a software version previous to minimum allowable software will result in the phone responding with a denial of software downgrade response.

The minimum allowable software is dependant on the phone's PEC and hardware release number and is provided in the table below:

Minimum Allowable Software			
PEC	**Hardware Release**	**Description**	**Minimum Software**
NTYS03ADE6	01	1120E IP Deskphone Graphite with Icon Keycaps (RoHS)	UNIStim 3.1 (0624C6J)
NTYS03BDE6	01	1120E IP Deskphone Graphite with English keycaps (RoHS)	UNIStim 3.1 (0624C6J)
NTYS03BDGS	01	1120E IP Deskphone GSA (RoHS)	UNIStim 3.1 (0624C6J)
NTYS05ACE6	50	1140E IP Deskphone Graphite with Icon Keycaps (RoHS)	UNIStim 3.1 (0625C6J)
NTYS05BCE6	50	1140E IP Deskphone Graphite with English keycaps (RoHS)	UNIStim 3.1 (0625C6J)
NTYS05BCGS	01	1140E IP Deskphone GSA (RoHS)	UNIStim 3.1 (0625C6J)
NTYS03AEE6	01	1120E IP Deskphone Graphite with Icon Keycaps (RoHS)	UNIStim 3.4 (0624C6T)
NTYS03BEE6	01	1120E IP Deskphone Graphite with English keycaps (RoHS)	UNIStim 3.4 (0624C6T)
NTYS03BEGS	01	1120E IP Deskphone GSA (RoHS)	UNIStim 3.4 (0624C6T)
NTYS05AEE6	01	1140E IP Deskphone Graphite with Icon Keycaps (RoHS)	UNIStim 3.4 (0625C6T)
NTYS05BEE6	01	1140E IP Deskphone Graphite with English keycaps (RoHS)	UNIStim 3.4 (0625C6T)
NTYS05BEGS	01	1140E IP Deskphone GSA (RoHS)	UNIStim 3.4 (0625C6T)

Recall that Figure 1 presented in the previous section above provides an explanation of where to identify the PEC and Hardware Release Number on the white product label (located on the back of the IP Deskphone).

If UFTP software download is used within the Communication Server 1000 environment, Avaya recommends that the software image for the 1120E IP Deskphone and 1140E IP Deskphone on the signaling server be upgraded to the minimum allowable software for the respective PEC and Hardware Release.

Communication Server 1000 release 5.0, and greater, will interpret denial of software downgrade responses from the new hardware phones. However, Communication Server 1000 prior to release 5.0 requires patch MPLR23154 to interpret correctly the phones denial of software downgrade responses. Failure to install the patch introduces the risk that the call server may continuously try and

downgrade the software thereby denying service to the phone. MPLR23154 is available at VO status on the Nortel ESPL website and is deployed only by contacting your Technical Support Representative

If TFTP software download is used, and the TFTP server is not upgraded to the minimum allowable software, or greater, the TFTP server will continuously try and downgrade the software in the phone. The new hardware phone will prevent the downgrade resulting in the phone being denied service.

In a Communication Server 1000 environment containing SRG and SRG50 branch office systems, two SRG Smart Updates (SU) exist to allow the SRG and SRG50 platforms respectively to interpret denial of software downgrade responses from the new hardware phones. Failure to install the patches introduces the risk that the call server may continuously try and downgrade the software thereby denying service to the phone.

For SRG 200 and SRG 400 release 1.5, the denial of software downgrade support is included in BCM.R400.SU.System.024 and later.

For SRG50 release 3.0, the denial of software downgrade support is included in BCM050.R300.SU.System-197 and later. This SU is not available for SRG50 release 2.0

If the above SRG patches are not installed then the "umsUpgradeAll" Main Office system command should not to be executed when the branch office sites has the new hardware 1120E IP Deskphone or the new hardware 1140E IP Deskphone and the IP Deskphone software at the Main Office precedes UNIStim software release 3.1.

For complete details on the minimal allowable software for the new hardware changes in the 1120E IP Deskphone and 1140E IP Deskphone please refer to Clarify Bulletin 2009009363 Rev2, New Minimum Firmware Requirement for 1120E IP Deskphone and 1140E and Clarify Bulletin 2009009916 Rev1, New Product Codes for 1120E IP Deskphone and 1140E.

EAP-MD5 and Microsoft Windows Server 2008 (applies to all the IP Deskphones)

If access control is enabled on the IP Deskphone and MD5 is chosen as the EAP mode, realize that EAP-MD5 is not available by default in the Microsoft Windows Server 2008 NPS[1] but can be turned on. Please refer to Microsoft support for more details on enabling EAP-MD5. In addition, minimally, Service Pack 2 is required on the Windows Server 2008 NPS to support the IP Deskphones using MD5 access control.

PC Port resets during software upgrade (applies to the 2007 IP Deskphone only)

The PC port on the IP Deskphones temporarily resets during software upgrades and during phone resets due to configuration changes. As a result, traffic to and from the network and a PC connected to the IP Deskphone's PC port will be disrupted during these periods.

Minimal firmware required on the Algo 4900 USB ATA (applies to the 1120E, 1140E, 1150E and 1165E IP Deskphones)

The Algo 4900 USB ATA must have firmware version v1.00.32v or greater before connecting the adapter to the IP Deskphone. A Windows based configuration tool to upgrade the ATA firmware version can be found at the Algo web site:

http://www.algosolutions.com/products/usbATA/fw-download.html

Also note that the Algo 4900 USB ATA is classified as a high power USB device and must be connected to an 1120E, 1140E and 1150E IP Deskphone through a powered USB hub. If it is connected to the phone directly, it will cause the phone to completely shut off service to the USB port.

[1] In Windows Server 2008, IAS has been replaced with Network Policy Server (NPS)

The 1165E IP Deskphone can support the Algo 4900 USB ATA connected directly as long as the 1165E IP Deskphone is locally powered with an AC adapter. If the 1165E IP Deskphone is obtaining it power from the network via Power over Ethernet (POE) then the Algo 4900 USB ATA must be connected to through a powered USB hub

Constant humming sound may be heard in Avaya (formerly Nortel) USB Headset Adapter (applies to the 1120E, 1140E, 1150E and 1165E IP Deskphones)

A constant humming noise is sometime heard through the headset when either the Enhanced USB Headset Adapter or the Mobile USB Headset Adapter is connected to the 1120E, 1140E, 1150E or 1165E IP Deskphone.

The humming noise heard within the headset can be corrected by upgrading the Headset Adapter firmware to version 2.00.98 or greater.

The USB Headset Adapter firmware version 2.00.98 is available for download from the "Software Download" link under "Support and Training" on the Nortel website located at: http://support.nortel.com. The firmware is available for the 1120E, 1140E, 1150E and 1165E IP Deskphone models under "Phones, Clients and Accessories" as file Adapter3v2.0098.zip.

To load the version 2.00.98 firmware onto the USB Headset Adapter perform the following procedure:

1) Download the firmware file Adapter3v2.0098.zip from the Nortel Technical Support web site
2) Load the file Adapter3v2.0098.zip onto a PC
3) Uncompress (unzip) the file to obtain Adapter3v2.0098.exe.
4) Connect the USB Headset Adapter to the PC
5) Start the Adapter3v2.0098.exe application to load the firmware onto the device.

IP Deskphone's performance will be diminished during broadcast storms (applies to all the IP Deskphones)

By default, network traffic to the IP Deskphone will be accepted based on the packet's destination MAC address. The phone will therefore accept, in addition to all unicast packets sent to the phones MAC address, all broadcast and multicast packets as well. If the network environment results in a high amount of broadcast or multicast traffic, the IP Deskphone's performance may be impacted.

If "Voice 802.1Q" is enabled on the phone, the phone can then be provisioned to filter some or all of the broadcast or multicast traffic. If "VLAN Filter" is enabled, packets will be accepted by the phone based on the packet's destination MAC address as well as the packet's VLAN tag. Untagged packets and packets with a VLAN tag different from the Voice VLAN ID will be prevented from reaching the phone. This will protect the voice application from excessive traffic sent to the broadcast address or to the multicast addresses. But please be aware, if VLAN filtering is enabled on the phone, one must ensure that voice packets are tagged with the appropriate VLAN ID as they exit the network switch, else the packets will be dropped by the filter.

Change in behavior of entering an asterisk (*) to manually provision the "Provision" parameter in the network configuration menu (applies to the 2007, 1120E, 1140E and 1150E IP Deskphones)

In UNIStim software prior to release 3.2 (0621C6M, 0624C6O, 0625C6O and 0627C6O on the 2007, 1120E, 1140E, and 1150E IP Deskphones respectively) the asterisk (*) key could not be used to input the dot (.) for defining an IP address in the "Provision" parameter in the network configuration menu. Since the "Provision" parameter in the network configuration menu can accept both a URL as well as an IP address the entry is a text based field causing the asterisk key to be accepted as an actual asterisk. But since this is different from other parameters that accept only an IP address where the asterisk key is used to represent the dot the inconsistent behavior of this field can be confusing.

With UNIStim software release 3.2 and greater, the typing of the asterisk key in the "Provision" parameter in the network configuration menu has slightly changed. Now, if the asterisk key is pressed twice relatively quickly it will input the dot. Pressing the asterisk key once will still input the asterisk character consistent with previous behavior.

Throughput may be slow for large file transfers on conversions from GigE to 100Mbit (applies to the 1120E, 1140E, 1150E and 1165E IP Deskphones)

In networks in which a PC is connected to the IP Deskphone's PC port and the PC's NIC speed is 100Mbit but the network speed is at GigE, large file transfers to the PC can take quite a long time. This is an issue with large file transfers only. Due to the speed mismatch between the phone's two ports the buffers in the phone can overflow resulting in retransmissions.

Although the IP Deskphones support Ethernet flow control (802.3x), the support is only implemented on the phone's PC port, not on the phone's network port. Ethernet flow control is a mechanism were the IP Deskphone can request a brief "pause" from the transmitting Ethernet device if the IP Deskphone buffers are about to overflow.

Ethernet flow control cannot be implemented on the phone's network port, since it impacts the phone's voice quality. As a result, in environments were the network is GigE but the PC NIC is only 100Mbit, large file transfers from the network to the PC can take quite a long time.

On the other hand, since Ethernet flow control is implemented on the phone's PC port, in environments were the PC NIC is GigE but the network is only 100Mbits, large file transfers should be well managed by the phone's Ethernet flow control mechanism.

Receiving a LLDP MED Network Policy TLV from the network infrastructure will cause the IP Deskphone to ignore any DSCP value received from the Communication Server 1000 Element Manager and the Info Block (applies to all the IP Deskphones)

Because of the precedence order, in auto-provisioning mode (i.e. the value has not been overridden manually) if the IP Deskphone receives a LLDP MED Network Policy TLV from the network infrastructure, the phone will provision its DSCP from the LLDP MED Network Policy TLV and not from the Call Server or Info Block. When the phone receives a Network Policy TLV from the network infrastructure, it sets its voice VLAN, L2 Priority and DSCP to the value specified in the VLAN ID field, L2 Priority field and DSCP Value field respectively. Thus, if the Network Policy TLV is received, any QoS values also received from the Call Server (i.e. Telephony Manager and/or Element Manager) or Info Block it will be ignored.

Special Note: The feature "DSCP provisioning precedence override" available in UNIStim software release 3.3 and greater provides a work-around to this advisory.

IP Deskphone's default for Auto VLAN changed to "Enabled". And Auto VLAN now supports a No VLAN option (applies to the 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230 IP Deskphones)

In software loads prior to UNIStim software release 2.2 for 2007, 1100 Series and 1200 Series IP Deskphones, one had to manually provision whether the phone was to be installed in an 802.1Q VLAN environment or not. The default configuration for the phone was assuming that the phone was not being deployed into an environment supporting a Voice VLAN. The default source for VLAN assignment was "no VLAN".

For the phones to be deployed into a voice VLAN environment, the phone had to be manually provisioned with either a Voice VLAN ID, or manually provisioned to accept and Auto VLAN assignment.

With UNIStim software commencing with release 2.2 and continuing with present UNIStim software the default configuration for the phone now has Auto VLAN assignment via DHCP enabled. But realizing that not all phones will be deployed in an 802.1Q VLAN environment, the Auto VLAN assignment support has also been updated to support both an 802.1Q VLAN environment and an environment without 802.1Q VLANs.

With Auto VLAN enabled, if VLAN information is provided within the DHCP option type VLAN-A, the phone will use the VLAN information to provision a voice VLAN. However, if no VLAN-A option type is provided by DHCP, the phone will assume that no VLAN is to be provisioned.

Although the default configuration for voice VLAN has changed, the new default configuration will not be applied to field upgrades. A limitation of the new functionality is that it could only apply to new phones being shipped from the factory with UNIStim software release 2.2 or greater. The default configuration of “Auto” will not be applied to field upgrades. Upgrading software does not change any pre-established values already in the phones.

But as mentioned above, to allow phones already deployed in the field to change the source of their VLAN information, with UNIStim software release 3.2 a new parameter called “vvsource” has been added to the Info Block to allow VLAN source to be auto-provisioned.

Important Note: While these changes provide greater flexibility, the change might impact the deployment of new phones into an existing deployment.

Manually provisioned link speed and duplex mode restored to “Auto” after software upgrade (applies to the 2007, 1120E, 1140E and 1150E IP Deskphones)

In UNIStim software release 1.3 (0621C3N, 0623C3F, 0624C3F, 0625C3F and 0627C3F for 2007, 1110, 1120E, 1140E and 1150E IP Deskphones respectively) greater low level network control available through the phones configuration menus was introduced. The greater control included allowing the link speed and the duplex mode on the IP Deskphones to be provisioned independently for both the network port and the PC port

By delivering this greater network control, the software unfortunately had to reset link speed and duplex mode back to “Auto” after an upgrade. Regrettably, preservation of the forced manual override could not be maintained during the upgrade.

What this means, is that if the IP Deskphone is running software prior to UNIStim software release 1.3 and if the link speed was manually provisioned to force the link to 10Mbit Full Duplex or 100MBit Full Duplex, after upgrading the software to UNIStim software release 1.3 or greater (including the current UNIStim software), the link speed and duplex mode is reset to “Auto” representing Auto-negotiation. With the phone now configured for Auto-negotiation a duplex mode mis-match will occur if the other end of the link is still provisioned to force the link to 10Mbit Full Duplex or 100MBit Full Duplex.

But, since UNIStim software release 3.1 for IP Deskphones, the means to provision the network port speed and the network port duplex mode has been available in the Info-Block. If a duplex mis-match occurs as a result of the software upgrade, the speed and duplex mode can forced, by provisioning them via the Info Block. This is possible because the auto-negotiation will pick the correct speed but the wrong duplex mode. Since the speed is correct, but the duplex mode is wrong, transmission can occur, albeit of poor quality. The duplex mismatch will impact the time taken for the phone to receive the Info Block, but re-transmission mechanisms built into the transmission protocols should allow the Info Block to eventually be received by the phone thus correcting the resetting of link speed and duplex mode to “Auto”.

Proportional spacing may not be optimal (applies to the 2007, 1110, 1120E, 1140E, 1150E and 1210 IP Deskphones)

The 2007, 1110, 1120E, 1140E, 1150E and 1210 IP Deskphones support graphical fonts. The supported fonts include hinting – or ‘intelligence’ – to the font outline, making the font more readable by preventing the letters in the font from becoming distorted and difficult to identify. But in some rare instances, the hinting may impact the proportional spacing resulting in characters appearing too close or too far apart.

Some models of Plantronics Bluetooth headset may unexpectedly become unpaired (applies to the 1140E, 1150E and 1165E IP Deskphones)

An issue was uncovered with certain Plantronics Bluetooth headsets (including the formerly validated Plantronics Voyager 510/510S) in which the headset may unexpectedly become unpaired. If the unpair occurs during an active call, all audio will be lost to and from the headset. In such a situation the call will remain active and the user is recommended to switch to handset or handsfree.

Due to the severity of this issue, Avaya does not recommend the use of the Plantronics Voyager 510/510S headset. For a complete list of wired and wireless headsets that Avaya has confirmed provide acceptable audio quality when used in conjunction with Avaya IP Deskphones please refer to the Product Bulletin P-2006-0084-Global-Rev7, Headsets for Nortel IP Phones.

2-step upgrade may be required (applies to the 1120E and 1140E IP Deskphones)

One important note when upgrading the 1120E IP Deskphone and 1140E IP Deskphone to UNIStim software release 4.1 from any load previous to 0624C1B or 0625C1B respectively is that a 2-step upgrade **will** be required. The 1120E IP Deskphone and 1140E cannot be upgraded directly to the newly released software if they are currently running software previous to 0624C1B and 0625C1B respectively. Instead, the phones must first be upgraded to 0624C1B and 0625C1B or newer (recommend 0624C3G and 0625C3G). Once the phones are running at least 0624C1B and 0625C1B software, they will accept being upgraded to UNIStim software release 4.1 respectively.

2-step upgrade may be required to load Asian fonts (applies to the 2007 IP Deskphone only)

Adding Asian languages to a 2007 IP Deskphone running UNIStim software release 1.3 (0621C3N) or earlier requires a 2 step process since the configuration file format has changed to support the new font downloads.

1) One must first upgrade the 2007 IP Deskphone software to using TFPT with the former configuration files ("BasicConfig" folder) – or upgrade the software from the call server.

2) Once the 2007 IP Deskphone is running the new software one must update the TFTP server to the new configuration files ("AsianConfig" folder) to download the Asian font files.

Running SRTP PSK with Communication Server 1000 release 5.0 requires a patch (applies to the 2007 and 1100 Series IP Deskphones)

In association with Communication Server 1000 release 5.0, UNIStim software since release 2.0 delivered media stream protection using SRTP UNIStim Keys (USK). However, running SRTP using PreShared Keys (PSK) is still a valid option in the IP Deskphones. But, if one wishes to run SRTP PSK with Communication Server release 5.0, patch MPLR24632 is required on the Communication Server 1000[2]. The Communication Server 1000 patch is located in the Meridian PEP library at the www.nortel.com/support web site.

Current release of SRTP PSK is not backward compatible with older version of SRTP PSK (applies to the 2007, 1110, 1120E, 1140E and 1150E IP Deskphones)

As stated above, running SRTP using PreShared Keys (PSK) is still a valid option in the IP Deskphones. But one important note when upgrading the IP Deskphones to the current releases of software is to realize that the current releases of SRTP PSK is not compatible with older versions of SRTP PSK. The minimum software releases for which the current release of SRTP PSK is backward compatible is UNIStim software release 1.3 (0621C3N, 0623C3G, 0624C3G, 0625C3G and 0627C3G for the 2007, 1110, 1120E, 1140E and 1150E IP Deskphone respectively).

Backlight Interaction with USB devices (applies to the 2007, 1120E, 1140E and 1150E IP Deskphones)

Some USB devices (i.e. Mice or Keyboards) send regular coordinate update messages to the phone even when the device is not being used. This can cause the sleep mode for the backlight to not be properly invoked.

Certain USB mice do not work with the 2007 IP Deskphone (applies to the 2007 IP Deskphone only)

It has been discovered that certain USB Mice do not work with the 2007 IP Deskphone. If the mouse does not transit information in the "Production", "Vendor" and "Manufacturing" fields of the USB communication exchange, the mouse will not be recognized by the 2007 IP Deskphone. Note that failure to send the above mentioned information is in violation of the USB communication exchange standard. Most leading brands of mice do send the required information.

[2] The patch is not required on Communication Server 1000 Release 5.5

Contrast adjustments: Local & TPS contrast adjustments are not synchronized (applies to the 1110, 1120E, 1140E and 1150E IP Deskphones)

The 1100 Series IP Deskphones' graphical display contrast control can be adjusted either locally (on the phone) or through the call server (TPS) control. The Communication Server 1000 does not yet synchronize its contrast setting with the local control. This means if the local control is used exclusively, then whenever the phone has a power cycle, the contrast setting provided by the Communication Server 1000 is restored and the user may need to adjust contrast again.

The local contrast control on the 1110, 1120E, 1140E and 1150E IP Deskphones is accessed by a "double press" of the Services key and selecting "1. Preferences", then "1. Display Settings" in the menu. The contrast control from the Communication Server is accessed with a "single press" of the Services key, then selecting "Telephone Options", then "Contrast Adjustment".

Volume adjustments are not persistent across phone resets (applies to all the IP Deskphones)

Even though the speech volume and ringer volume is controlled by the IP Deskphone, the user selected preferences are stored by the Communication Server 1000. Prior to release 5.0 of the Communication Server 1000, the server did not save the user selected preferences across a phone reboot. Thus, if the phone rebooted, for whatever reason, the speech volume and ringer volume would be reset to their default values. Upgrading to release 5.0 or greater of the Communication Server 1000 corrects this issue.

Power disruption during software upgrade will corrupt the upgrade (applies to all the IP Deskphones)

During a software upgrade, if a power disruption is experienced by the phone, the software upgrade will fail. In some instances a power disruption during an upgrade may also corrupt the existing software on the phone. If this corruption should occur, the phone will fail over into its boot code known as "BootC". BootC will automatically try to restore the phone's software from the image on a call server. But for the 2007, the 1100 Series and the 1200 Series IP Deskphones, if the phone's software was obtained from a TFTP server instead, in order to restore, or upgrade, the software from BootC a manual TFTP download from BootC must be performed. The Manual TFTP Download from BootC Procedure is documented in the IP Phones Fundamentals NN43001-368. **Regardless, caution should be exercised to avoid power disruptions during software upgrades.**

Quality Improvements

In addition to delivering the enhancements listed above, the UNIStim software release 4.1 for IP Deskphones also continues to improve the overall quality of the IP Deskphone software through the delivery of ongoing resolution of CRs and closed cases. Numerous quality improvements have been delivered, and 7 customer cases have been closed in UNIStim 4.1.

UNIStim software release 4.1 for IP Deskphones close the following cases:

Closed Cases	
Case #	**Description**
090330-09018	IP Deskphone ARP table may become full
091009-31321	Noise may be heard when switching to secure (SRTP) call
090818-00084	Cannot control the beep volume with Application Gateway (AG) zone paging
091117-54529	IP Deskphone fails to register if too many DHCP offers are provided
091201-61674	GEM icons are too bright when attached to an 1165E IP Deskphone
100125-87603	IP Deskphone does not send EAP LOGOFF when an attached PC is unplugged
090904-10920	2007 IP Deskphone TFT - Digits being dialed flicker on the display

IP Deskphone Compatibility

UNIStim software release 4.1 for IP Deskphones is compatible with the following IP Deskphones:

IP Deskphone Compatibility		
PEC	**Description**	**Software File**
NTDU96xxxxxx	2007 IP Deskphone	0621C7D.bin
NTYS02xxxxxx	1110 IP Deskphone	0623C7J.bin
NTYS03xxxxxx	1120E IP Deskphone	0624C7J.bin
NTYS05xxxxxx	1140E IP Deskphone	0625C7J.bin
NTYS06xxxxxx	1150E IP Deskphone	0627C7J.bin
NTYS07xxxxxx	1165E IP Deskphone	0626C7J.bin
NTYS18xxxxxx	1210 IP Deskphone	062AC7J.bin
NTYS19xxxxxx	1220 IP Deskphone	062AC7J.bin
NTYS20xxxxxx	1230 IP Deskphone	062AC7J.bin

Call Server Compatibility and Requirements

UNIStim software release 4.1 is compatible with the below Avaya Call Servers. Note that the 1200 Series IP Deskphones are only supported on Communication Server 1000 release 5.5 and greater, SRG 50 release 3.0, BCM 50 release 3.0, BCM 450 release 1.0, and Communication Server 2100 CICM 10.1 MR2.

Communication Server 1000

Communication Server 1000 Compatibility and Requirements	
Call Server Release	**Notes and Advisements**
CS 1000 6.0R - IP Line 6.00.18 - SS (Linux App) 6.00.018	Avaya recommends an upgrade to this UNIStim software release at the earliest opportunity. **Since the quality of the DTLS feature is not at an acceptable level at this time, support for DTLS is being delayed on the Communication Server 1000 until the quality concern can be addressed**.
CS 1000 5.5 J - IP Line 5.5.12 - SS 5.5.12	Avaya recommends an upgrade to this UNIStim software release at the earliest opportunity. The DTLS and SCR features are not supported on this platform.
CS1000 5.00W - IP Line 5.00.31 - SS 5.00.31	Avaya recommends an upgrade to this UNIStim software release at the earliest opportunity. The DTLS and SCR features are not supported on this platform The 1200 Series IP Deskphones are not supported on this platform.

Survivable Remote Gateway (SRG)

SRG Compatibility and Requirements	
Call Server Release	**Notes and Advisements**
SRG 50 3.0	Avaya recommends an upgrade to this UNIStim software release at the earliest opportunity. No SRG50 patches are required to support the Enhanced Software Download feature that allows the IP Deskphone software supported on the SRG50 to remain in synch with the Communication Server 1000 Main office. In addition, if the “Main” Communication Server 1000 is on release 4.5, or later, no patch is necessary on the Communication Server 1000 to upgrade the IP Deskphone. The 1150E and 1165E IP Deskphones are not supported on the SRG50 3.0.

SRG 50 2.0	Avaya recommends an upgrade to this UNIStim software release at the earliest opportunity. No SRG 50 patches are required to support the Enhanced Software Download feature that allows the IP Deskphone software supported on the SRG 50 to remain in synch with the Communication Server 1000 Main office. In addition, if the "Main" is Communication Server 1000 release 4.5, or later, no patch is necessary on the Communication Server 1000 to upgrade the IP Deskphone. The 1110, 1150E, 1165E and 1200 Series IP Deskphones are not supported on SRG 50 2.0.
SRG 200/400 1.5	Avaya recommends an upgrade to this UNIStim software release at the earliest opportunity. No SRG patches are required to support the Enhanced Software Download feature that allows the IP Deskphone software supported on the SRG 200/400 1.5 to remain in synch with the Communication Server 1000 Main office. In addition, if the "Main" is Communication Server 1000 release 4.5, or later, no patch is necessary on the Communication Server 1000 to upgrade the IP Deskphone. The 1110, 1150E, 1165E and 1200 Series IP Deskphones are not supported on SRG200/400 Rls1.5

Business Communications Manager (BCM)

BCM Compatibility and Requirements	
Call Server Release	**Notes and Advisements**
BCM 50 5.0	Upgrading the phone's software is dependent upon a BCM Smart Update (SU) that includes the UNIStim software. Although UNIStim software release 4.1 for IP Deskphones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The 1150E and 1165E IP Deskphones are not supported on BCM 50 5.0.
BCM 50 3.0	Upgrading the phone's software is dependent upon a BCM Smart Update (SU) that includes the UNIStim software. Although UNIStim software release 4.1 for IP Deskphones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The 1150E and 1165E IP Deskphones are not supported on BCM 50 3.0.

BCM450 5.0	Upgrading the phone's software is dependent upon a BCM Smart Update (SU) that includes the UNIStim software. Although UNIStim software release 4.1 for IP Deskphones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The 1150E and 1165E IP Deskphones are not supported on BCM 450 5.0.
BCM450 1.0	Upgrading the phone's software is dependent upon a BCM system update (SU) that includes the UNIStim software. Although UNIStim software release 4.1 for IP Deskphones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The 1150E and 1165E IP Deskphones are not supported on BCM 450 1.0.
BCM 200/400 4.0	Upgrading the phone's software is dependent upon a BCM Smart Update (SU) that includes the UNIStim software. Although UNIStim software release 4.1 for IP Deskphones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The 1110, 1150E, 1165E and 1200 Series IP Deskphones are not supported on BCM 200/400.

Communication Server 2100 Centrex IP Client Manager (CICM)

CICM Compatibility and Requirements	
Call Server Release	**Notes and Advisements**
CICM 10.1 MR2 (Succession)	Upgrading the phone's software is dependent upon CICM performing regression test activities on UNIStim software release 4.1 to verify its performance on this CICM product. The 1165E and 1210 IP Deskphones are not supported on CICM 10.1
CICM 10.0 (Succession)	Upgrading the phone's software is dependent upon CICM performing regression test activities on UNIStim software release 4.1 to verify its performance on this CICM product. The 1165E and 1200 Series IP Deskphones are not supported on CICM 10.0
CICM 9.0 (Succession)	Upgrading the phone's software is dependent upon CICM performing regression test activities on UNIStim software release 4.1 to verify its performance on this CICM product. The 1165E and 1200 Series IP Deskphones are not supported on CICM 9.0

IP Deskphone Software Upgrade Methods (Communication Server Dependent)

Upgrading the IP Deskphone software in a Communication Server 1000 environment

The 2007, 1100 Series and 1200 Series IP Deskphones supports remote software upgrades through both a TFTP process and the more automated UFTP process direct from the Communication Server 1000.

Note that the 1200 Series IP Deskphones are only supported on Communication Server 1000 release 5.5 or later. Therefore the software can be upgraded by either UFTP or TFTP.

Also note that the 1165E IP Deskphone is only supported on Communication Server 1000 release 5.0 or later. Therefore the software can be upgraded by either UFTP or TFTP.

For information on the TFTP software upgrade process for the Communication Server 1000, please refer to the IP Phones Fundamentals, NN43001-368.

For information on the UFTP software upgrade process for the Communication Server 1000, please refer to the IP Line Fundamentals, NN43100-500.

Upgrading the IP Deskphone software in a Survivable Remote Gateway (SRG) environment

For information on the software upgrade process for the SRG200/400, please refer to the Main Office Configuration Guide for SRG200/400 Rls1.5, 553-3001-207

For information on the software upgrade process for the SRG50, please refer to the Main Office Configuration Guide for SRG50 Rls 2.0, 553-3001-207.

Upgrading the IP Deskphone software in a Business Communication Manager (BCM) environment

Upgrading the IP Deskphone's software is dependent upon a BCM system patch that includes the UNIStim software. This is applicable to all BCM platforms. BCM system patches will be delivered initially as atomic patches that are individually installable. These patches will be rolled up into a monthly Smart Update (SU) which includes all atomic patch content since the previous SU.

Patches and SU are posted for partner access on the www.nortel.com/support web site under "Voice, Multimedia & Unified Communications" then under the respective BCM platform.

Upgrading the IP Deskphone software in a Communication Server 2100 (CICM) environment

Depending on the MR level, the UNIStim software will either be included in the installation files or will need to be transfer to the CICM Element Manager.

If the software is included in the installation files some manual administrator configuration will still be required. If the software is not included in the installation file the administrator can transfer these software loads to the CICM Element Manager, configure the terminal's "Recommended and Minimum software levels" and the Element Manager will propagate the software to the CICM. The user will be prompted to upgrade their software at their own convenience.

For details on using the CICM Element Manager to configure the recommended software and how to upgrade the IP Deskphones, refer to the CICM Administration and Security, NN10252-611.06.03 in the section titled "Downloading firmware to the CICM Element Manager".

System Compatibility and Requirements

System Compatibility and Requirements	
System	**Notes and Advisements**
Avaya (formerly Nortel) Contact Recording and Quality Monitoring (CRQM) 7.0	The Secure Call Recording feature in UNIStim software release 4.0 and greater interworks with Avaya (formerly Nortel) Contact Recording and Quality Monitoring release 7.0 For additional information on Avaya CRQM solution and its support for Secure Call Recording, please refer to the CRQM 7.0 Planning, Installation and Administration Guide, NN44480-300
Avaya (formerly Nortel) VPN Router (NVR) 8.00 or greater	The UNIStim VPN Client (UVC) feature in UNIStim software release 4.0 and greater interworks with Avaya (formerly Nortel) VPN Routers running release 8.00 and greater
Avaya (formerly Nortel) VPN Gateway (NVG) 8.0.1 or greater	The UNIStim VPN Client (UVC) feature in UNIStim software release 4.1 interworks with Avaya (formerly Nortel) VPN Gateways running release 8.0.1 and greater
Nortel Application Gateway 2000 6.3 and higher	This software release provide support to interwork with Nortel Application Gateway 2000 (AG2000) release 6.3 The Nortel Application Gateway solution delivers packaged applications on the IP Deskphones desktop extending the phone's capability beyond telephony features. For more information on the capabilities of the AG2000 please refer to the Product Bulletin P-2008-0005-Global. The AG2000 does not support the 1150E IP Deskphone.
Secure Multimedia Controller (SMC) 1.0	This software release continues to provide support to interwork with the Secure Multimedia Controller (SMC) 2450. The SMC 2450 is a purpose-built application firewall, delivering an integrated inside threat security solution to protect IP Deskphones and multimedia communication servers. The SMC 2450 creates a "Secure Multimedia Zone" around the converged infrastructure to protect against Denial of Service attacks and other security threats, while pre-configured policy settings simplify deployment and ensure the integrity and availability of the business critical converged, multimedia infrastructure. For more information on the capabilities available with the SMC 2450 please refer to the Product Bulletin P-2006-0131-Global, SMC 2450

Appendix A: Certificate Installation (applies to all the IP Deskphones)

Installing CA Root Certificate using the IP Deskphone's configuration file

The recommended means to install a Certificate Authority (CA) root certificate on an IP Deskphone is to use the phone's configuration file (e.g. 1140e.cfg). An example of the modified configuration file is shown below where cacert.pem contains the PEM format CA root certificate

[USER_KEYS]
DOWNLOAD_MODE AUTO
PROTOCOL TFTP
VERSION 1
FILENAME cacert.pem

When the phone boots and connects to the TFTP server, the phone will download the certificate. The installer will then be prompted to accept the fingerprint of the initial certificate file. Once accepted, the certificate is saved and the phone will be ready to use the CA root certificate. Installations of all subsequent root certificates are authenticated by an attached signature. There will be no prompt to accept a fingerprint after the first certificate is installed[3].

Installing CA Root Certificate and Device Certificates using SCEP

In UNIStim software release 3.0 support for Simple Certificate Enrollment Protocol (SCEP) was introduced to allow the IP Deskphone to request both a CA root certificate and then a device certificate to be loaded into the IP Deskphone.

To successfully install certificates using SCEP, the following phone parameters must be configured (either manually or using auto-provisioning):

- CA Server - the URL of the SCEP interface of the CA Server. As an example, for a Microsoft CA server this would be: http://www.<<ca_url.com>>/certsrv/mscep/mscep.dll
- Domain Name - the domain to which the phone will belong. (e.g. acme.com)
- Hostname - the name assigned to the phone. For some authentication servers (i.e. Microsoft IAS), this must match a username that can be authenticated in the server. If left blank, the hostname will be automatically filled with NTIPPxxxxxx where the final 6 characters are the last 6 hex characters from the phone's MAC address.

When the phone boots with the above configuration, a CA root certificate will be requested from the CA Server. Once the CA root certificate is received, the prompt "CA Fingerprint" will be displayed on the phone's screen. The installer must press the "Accept" softkey to install the CA root certificate. Once accepted, the certificate will be saved on the phone and the prompt will never appear again.

After the CA root certificate is installed, a Device certificate must be installed. Depending on the CA Server configuration, the user may be prompted to enter a challenge password.[4] If no challenge password is required, the installer must simply select the OK softkey.

Once the challenge password is entered (or the OK softkey is pressed), the phone will then request a device certificate and "Waiting for Approval…" will be displayed on the phone's screen. Depending on the CA Server configuration, it may be necessary for the installer to manually approve the certificate request using the CA Server.

[3] All subsequent certificates must be signed

[4] For the Microsoft CA Server, MSCEP installation allows the option of configuring a challenge password. If configured, the user must access http://www.<<ca_url>>/certsrv/mscep/mscep.dll with a web browser to obtain a temporary password. For the EJBCA CA Server, the password (if any) defined for the End Entity for each phone must be entered.

After the certificate is approved (automatically or manually), the “Waiting for Approval…” prompt will be removed.

Once approved, the phone is ready to use the device certificate[5].

As of UNIStim software release 4.0 the IP Deskphone’s support for SCEP was enhanced to:

- allow certificates installed using SCEP to be associated with a specific device certificate profile (DCP)
- allow the definition of the number of days prior to expiry when the phone should attempt to renew the device certificate automatically (default is 90 days)
- eliminate the need to be prompted for the CA fingerprint during renewal (although the user is still prompted for the CA password)
- automatically repeat the prompt for certificate renewal on an hourly basis, if the password prompt times out
- provide more control over the attributes of the requested device certificate
- provide the ability to force a device certificate to be deleted
- allow the CA Server configuration to support a URL containing an FQDN hostname instead of only an IP address

For additional information on installing certificates into the IP Deskphone, please refer to the IP Phones Fundamentals NN43001-368.

Installing Device Certificates using PKCS#12

As of UNIStim software release 4.0, the IP Deskphone’s certificate support was enhanced to support PKCS#12 device certificates as well.

PKCS#12 is a standard which allows a device certificate and its private key to be encrypted for secure transmission. A PKCS#12 file is encrypted by a user-defined password when it is created. Then to extract the device certificate with its private key, the recipient must know the password[6]. After the PKCS#12 file is downloaded, the user is prompted to enter the password. If the prompt times out, the installation is aborted.

The advantage of using PKCS#12 rather than SCEP is that with PKCS#12 an administrator has full control over the device certificate attributes. The disadvantage of using PKCS#12 is that installed device certificates cannot be automatically renewed. It is up to the Administrator to keep track of when device certificates will expire. To update a device certificate that is about to expire, a new certificate must be generated as a PKCS#12 file and loaded onto the phone.

The PKCS#12 certificate is downloaded to the IP Deskphone via the IP Deskphone’s configuration file (1120e.cfg, 1140e.cfg, and 1150e.cfg). A new section called [DEV_CERT] must be added to the configuration file to specify the PKCS#12 file to be loaded.

[5] Both the Accept prompt and the CA Password prompt will time out after 30 seconds. If either times out, the installation of the device certificate is not completed and the phone will restart this process after waiting 1 hour. This process will repeat as long as the CA Server and Domain Name are defined and the device certificate is not successfully installed.

[6] It is assumed that the password has been provided by an out-of-band method (e.g. email).

The [DEV_CERT] section supports five command lines:

- DOWNLOAD_MODE (required command) - The DOWNLOAD_MODE can be either FORCED or AUTO. If FORCED, the VERSION command is ignored and the licenses files are always downloaded. If AUTO, the application looks at the VERSION and downloads the certificate files only if they are a newer version than what is currently stored on the phone.
- VERSION (optional command) - if this command is not present, version 0 is assumed). The VERSION command specifies the version of the certificates being downloaded. When certificates are written to the phone's memory, the value for the .cfg file's VERSION field (or "0" if VERSION is not in the file) becomes the new stored version value against which any future comparisons are made.
- FILENAME (required command) - the filename of the device certificate file to be downloaded. The individual device certificate file name is MAC.pfx or MAC.p12 where MAC is the phone's 12 characters MAC address to which the certificate is associated. The FILENAME command can either reference a specific certificate file (for which only the phone with that specific MAC address will load the file) or the FILENAME command can use the asterisk to represent all MAC addresses. If the asterisk is used, each individual phone will upon reading this command, substitute its own MAC address into the filename, thereby assuring that the phone only downloads its specific device certificate file.
- PROFILE (required command) - The PROFILE command specifies the index of the DCP where the device certificate is to be installed.
- PURPOSE (required command) - The PURPOSE command specifies which application(s) can use the PKCS#12 device certificate defined in the DCP. Supported values for PURPOSE are shown in the table below. To specify multiple purposes, simply add each application's value (for example to use the same certificate for both VPN and GXAS enter the value 24 (16 + 8). To indicate that the device certificate can be used by all applications enter the value of negative one (-1)[7].

PURPOSE command values		
Application	**Value**	**Note**
EAP-TLS	1	
SIP TLS	2	Not supported in UNIStim
HTTPS	4	Not supported in UNIStim
GXAS	8	
VPN	16	
DTLS	32	
SCR	64	
Licensing	128	

Below is an example of a DEV_CERT section in a configuration file. In this example, a PKCS#12 device certificate will be downloaded into DCP #2 and will be marked as being available for all applications. The version associated with the device certificate will be marked as 5. Finally, the "*" in the filename is substituted with the IP Deskphone's MAC address so that each phone will download its own unique device certificate (e.g. 001365ff7d69.pfx).

```
[DEV_CERT]
DOWNLOAD_MODE AUTO
VERSION 000005
FILENAME *.pfx
PROFILE 2
PURPOSE -1
```

[7] Please note that since negative one means that the device certificate can be used by all applications, it cannot be combined with other values.

Device Certificates Profiles (DCP)

As of UNIStim software release 4.0 for IP Deskphones support for Device Certificate Profiles (DCP) is available. A DCP provides the ability to support mixed SCEP and/or PKCS#12 device certificates installs by specifying the installation method for each certificate independent of each other. A DCP also allows arbitrary sharing of device certificates across one or more applications.

The number of DCP supported is dependant on the phone model. The number of profiles supported by phone model is shown in the table below:

DCP	
Model	**Number of DCP**
2007 IP Deskphone	3
1100 Series IP Deskphones (except the 1110 IP Deskphone)	6
1110 IP Deskphone	5
1200 Series IP Deskphones	5

One device certificate can be installed with each supported DCP. DCP provisioning parameters all include the prefix “dcp” and include a suffix with the DCP index (1 to max number of profiles). For example, “dcpsource1” is the Source (SCEP or PKCS#12) for DCP #1.

A DCP can only be configured using auto-provisioning. Each DCP can be configured for SCEP, PKCS#12 and configured as Active or Inactive. By default, DCP #1 is configured as active with SCEP whereas all remaining DCP area configured as inactive with PKCS#12. An inactive PKCS#12 DCP is automatically activated if a PKCS#12 device certificate is successful installed using the [DEV_CERT] configuration option.

Several new Info-Block parameters that have been created to allow the DCP to be auto-provisioned. Some of the new DCP parameters are common to both SCEP and PKCS#12 device certificate configuration, where as some of the new DCP parameters apply only to SCEP device certificate configuration. The new Info-Block parameters that have been created to allow the DCP to be auto-provisioned are provided in the two tables below. Please refer to Appendix B for the complete list of parameters supported within the Info Block.

The new Info-Block parameters that have been created to allow the DCP parameters common to both SCEP and PKCS#12 to be auto-provisioned are provided below.

Auto-Provisioning DCP Parameters		
dcpsource1	‘scep’ ‘pkcs12’	Method used to install device certificates
dcpactive1	‘n’ Inactive ‘y’ active	Profile is active or not
dcppurpose1[8]	Character string made up of: ‘a’ All applications ‘v’ VPN ‘d’ DTLS ‘s’ SCR ‘g’ GXAS ‘e’ EAP-TLS ‘l’ Licensing	Specifies which phone applications can use this device certificate Multiple values can be cascaded (e.g. ‘dsg’) but ‘a’ can only be used by itself

[8] Provisioning the dcppurpose# parameter on a DCP defined for a PKCS#12 certificate, will overwrite the initial purpose established at installation time by the PURPOSE command in the [DEV_CERT] section of the configuration file

The new Info-Block parameters that have been created to allow the DCP parameters that apply only to SCEP to be auto-provisioned are provided below. These SCP specific parameters provide control over SCEP device certificate renewal and deletion.

Auto-Provisioning SCP Parameters		
dcprenew1	Integer value, but also supports the following special values '-1' Never '0' Immediately	Number of days prior to certificate expiry that a certificate renewal is requested
dcpdelete1	'n' No action 'y' Delete	If set to 'y' forces the device certificate to be deleted
dcpautocn1	'0' Manual '1' Automatic	Automatically construct the Certificate Name using cadomain and cahost
dcpcaname1	Character string of 128 characters	CA name included in the SCEP request to identify requested CA (note that not all CA require the CA name)
dcphostnameoverride1	Character string of 128 characters	Override hostname (cahost) for this DCP only
dcpattrcn1	Character string of 128 characters	If "Auto CN" is disabled, this value is used instead of combining cadomain and cahost
dcpattrextkeyusage1	Character string made up of one of the following characters 'a' anyExtendedKeyUsage 'c' clientAuth 'i' ipsecIKE (RFC 4945) 'm' iKEIntermediate ' ' no Extended Key Usage	Define the Extended Key Usage attributes to be requested for the device certificate. The default is clientAuth.

Each of the parameters in the above two tables are replicated an additional 5 times for 1100 Series IP Deskphones (except the 1110 IP Deskphone), an additional 4 times for the 1110 IP Deskphone and the 1200 Series IP Deskphones, and an additional 2 times for the 2007 IP Deskphone. The additional parameters will have the same name as above except that the character "1" on the end will be replaced by the character 2, 3, etc. up to the maximum number of DCP supported.

Below are a couple of examples of provisioning DCP. The first example shows the configuration of DCP #1 for VPN using SCEP and the configuration of DCP#2 for DTLS and SCR using SCEP.

```
dcpsource1=scep;
dcpactive1=y;
dcppurpose1=v;
dcprenew1=60;
dcpsource2=scep;
dcpactive2=y;
dcppurpose2=ds;
```

This second example shows the configuration of DCP #1 for all applications using a PKCS#12 download device certificate.

```
dcpsource1=pkcs12;
dcpactive1=y;
dcppurpose1=a;
dcpactive2=n;
```

Appendix B: IP Deskphone Info Block (applies to all the IP Deskphones)

The list of all the parameters that can be provisioned via the Info-Block is provided in the table below. Note that not all parameters need be specified in the Info-Block. If the option is included, the parameter will be provisioned with the value specified. If the option is not included, the phone will retain its default value for the particular parameter, or the phone will retain the value that was previously provisioned for the parameter if the "stickiness" parameter is set.

Info Block Parameters		
Parameter	**Value**	**Description**
s1ip	Value from 0.0.0.0 to 255.255.255.255	Primary server IP address
p1	Value from 1 to 65535	Primary server port number
a1	Value from 0 to 255	Primary server action code
r1	Value from 0 to 255	Primary server retry count
s2ip	Value from 0.0.0.0 to 255.255.255.255	Secondary server IP address
p2	Value from 1 to 65535	Secondary server port number
a2	Value from 0 to 255	Secondary server action code
r2	Value from 0 to 255	Secondary server retry count
dhcp	'y' yes 'n' no	Enable DHCP
xip	Value from 0.0.0.0 to 255.255.255.255	XAS server IP address
xp	Value from 0 to 65535	XAS server port number
xa	Character string made up of the following character 'g' graphical XAS mode 'f' full screen XAS mode 's' secure XAS mode 'h' hidden Phone mode 'r' reduced Phone mode	XAS server action code (XAS Mode and Phone Mode) Note that there is no explicit character to select text-mode. Instead, the lack of specifying graphical 'g' implies the XAS mode is text. Also note that there is no explicit character to select Full phone mode. Instead, the lack of specifying either hidden 'h' or reduced 'r" implies the phone is to be provisioned for Full phone mode. Please be careful not to confuse Full Screen XAS mode 'f' with Full phone mode. Note that hidden Phone mode and reduced Phone mode are supported on the 2007 IP Deskphone only.
unid	Character string up to 32 characters	Unique network identification
menulock	'f' full lock 'p' partial lock 'u' unlock	Menu lock mode
vq	'y' yes 'n' no	Enable 802.1Q for voice [1]
vcp	Value from 0 to 8	802.1Q control p bit for voice stream. Provisioning this value to 8 tells the phone to use the value it receives from the LLDP Network Policy TLV or from the call server
vmp	Value from 0 to 8	802.1Q media p bit for voice stream. Provisioning this value to 8 tells the phone to use the value it receives from the LLDP Network Policy TLV or from the call server

vlanf	‘y’ yes ‘n’ no	Enable VLAN filter on voice stream
nis	‘a’ auto negotiation ‘10’ 10 Mbps ‘100’ 100 Mbps	Network port speed [1]
nid	‘a’ auto negotiation ‘f’ full duplex ‘h’ half duplex	Network port duplex [1]
pc	‘y’ yes ‘n’ no	Enable PC port
pcs	‘a’ auto negotiation ‘10’ 10 Mbps ‘100’ 100 Mbps	PC port speed
pcd	‘a’ auto negotiation ‘f’ full duplex ‘h’ half duplex	PC port duplex
dq	‘y’ yes ‘n’ no	Enable 802.1Q for PC port
dv	‘y’ yes ‘n’ no	Enable VLAN for data
dvid	Value from 1 to 4094	VLAN ID for data VLAN
dp	Value from 0 to 8	802.1Q p bit for data stream. Provisioning this value to 8 tells the phone to use the value it receives from the LLDP Network Policy TLV or from the call server
pcuntag	‘y’ yes ‘n’ no	Enable stripping of tags on packets forwarded to PC port
lldp	‘y’ yes ‘n’ no	Enable 802.1ab LLDP [1]
pk1	Character string of16 character representing 16 hexadecimal digits	S1 PK [2]
pk2	Character string of 16 character representing 16 hexadecimal digits	S2 PK [2]
st	‘y’ yes ‘n’ no	Enable stickiness (provisioning is persistent in the event a new info block is not received)
cachedip	‘y’ yes ‘n’ no	Enable cached IP
igarp	‘y’ yes ‘n’ no	Ignore GARP
srtp	‘y’ yes ‘n’ no	Enable SRTP-PSK
eap	‘dis’ disable ‘md5’ EAP-MD5 ‘peap’ PEAP/MD5 ‘tls’ EAP-TLS	Disable or choose an EAP authentication method [1] [2]
eapid1	Character string up to 32 characters	802.1x (EAP) device ID1 [1] [2]
eapid2	Character string up to 32 characters	802.1x (EAP) device ID2 [1] [2]
eappwd	Character string up to 32 characters	802.1x (EAP) password [1] [2]
ca	Character string up to 80 characters	Certificate Authority (CA) server
cahost	Character string up to 32 characters	Certificate Authority (CA) host name

cadomain	Character string up to 50 characters	Certificate Authority (CA) domain name
cdiff	Value from 0 to 255	Diffserv code points for control messages
mdiff	Value from 0 to 255	Diffserv code points for media messages
prov	Character string up to 50 characters	Provisioning server address or URL (if the string is prefixed with “http://” the phone will connect to a HTTP server, otherwise the phone will connect to a TFTP server)
dns	Character string up to 50 characters	Primary DNS server URL
dns2	Character string up to 50 characters	Secondary DNS server URL
ct	Value from 0 to 15 for 1100 Series IP Deskphones Value from 7 to 39 for 2007 IP Deskphone	Contrast value
br	Value from 0 to 15	Brightness value
blt	‘0’ 5 seconds ‘1’ 1 minute ‘2’ 5 minutes ‘3’ 10 minutes ‘4’ 15 minutes ‘5’ 30 minutes ‘6’ 1 hour ‘7’ 2 hours ‘8’ always on	Backlight timer
dim	‘y’ yes ‘n’ no	*As of UNIStim software release 3.4, the previously supported “dim” parameter is no longer supported since its functionality is superseded by the dimt parameter. The phone will still accept the dim parameter to prevent errors when reading existing provisioning files but the parameter will be ignored in favor of the new dimt parameter.*
dimt	‘0’ Off ‘1’ 5 seconds ‘2’ 1 minute ‘3’ 5 minutes ‘4’ 10 minutes ‘5’ 15 minutes ‘6’ 30 minutes ‘7’ 1 hour ‘8’ 2 hours	Phone inactivity timer to dim the screen (2007 IP Deskphone only)
sst	‘0’ Off ‘1’ 1 minute ‘2’ 5 minutes ‘3’ 10 minutes ‘4’ 15 minutes ‘5’ 30 minutes ‘6’ 1 hour ‘7’ 2 hours	Phone inactivity timer to initiate the slide show (2007 IP Deskphone only)
bt	‘y’ yes ‘n’ no	Enable Bluetooth (1140E IP Deskphone and 1150E only)
zone	Character string up to 8 characters	Zone ID

file	Character string up of the following character 'z' read zone file 't' read type file 'd' read device file	For system specific provisioning file specifies what other provisioning files to read
hd	Character string up of the following character 'w' wired 'b' Bluetooth 'n' none	Headset type
ar	'y' yes 'n' no	Enable Auto-recovery
arl	'cr' critical 'ma' major 'mi' minor	Auto-recovery level
ll	'cr' critical 'ma' major 'mi' minor	Log level
ssh	'y' yes 'n' no	Enable SSH
sshid	Character string between 4 and 12 characters	SSH user ID [2]
sshpwd	Character string between 4 and 12 characters	SSH password [2]
bold	'y' yes 'n' no	Enable bold on font display
menupwd	String between and 21 characters containing only numeric digits, asterisk (*) and hash (#) – i.e. only the dialpad symbols	Administrator password [2]
vvsource	'n' no VLAN 'a' auto VLAN via DHCP 'lv' auto VLAN via VLAN Name TLV 'lm' auto VLAN via Network Policy TLV	Source of VLAN information
srtpid	96 115 120	Payload type ID
ntqos	'y' yes 'n' no	Enable Nortel Automatic QoS
dscpovr	'y' yes 'n' no	DSCP Precedence Override
vpn	'y' enable 'n' disable	Enable the UNIStim VPN Client (UVC) within the phone
vpntype	'1' Nortel VPN	Only Nortel VPN devices are supported at this time

vpnmode	'aggressive' 'main'	Authentication mode
vpnauth	'psk' preshared key 'certificate' X.509 certificate	Authentication credential[9]
vpnxauth	'0' none '1' password	X Authentication type
vpnpskuser	Character string up to 64 characters	PreShared Key (PSK) User ID
vpnpskpwd	Character string up to 64 characters	PreShared Key (PSK) password
vpnxauthuser	Character string up to 64 characters	X Authentication User ID
vpnxauthpwd	Character string up to 64 characters	X Authentication password
vpns1	Character string up to 64 characters	IP address or FQDN[10] of the primary VPN server
vpns2	Character string up to 64 characters	IP address or FQDN of the secondary VPN server
vpndiffcpy	'y' copy DSCP from inner packet 'n' use vpndiff value	Source of DSCP value for the tunnel traffic. Determines if DSCP value is copied from inner packet to outer packet or if vpndiff is used.
vpndiff	0-255	If vpndiffcpy=n, then this value is used for the DSCP value for the tunnel traffic
vpnmotd	0-999	Message of the Day (MOTD) timer
dcpsource1	'scep' 'pkcs12'	Method used to install device certificates
dcpactive1	'n' Inactive 'y' Active	Profile is active or not
dcppurpose1	Character string made up of the following character 'a' All applications 'v' VPN 'd' DTLS 's' SCR 'g' GXAS 'e' EAP-TLS 'l' Licensing	Specifies which phone applications can use this device certificate Multiple values can be cascaded (e.g. 'dsg') but 'a' can only be used by itself
dcprenew1	Integer value, but also supports the following special values '-1' Never '0' Immediately	Number of days prior to certificate expiry that a certificate renewal is requested
dcpdelete1	'n' No action 'y' Delete	If set to 'y' forces the device certificate to be deleted
dcpautocn1	'0' Manual '1' Automatic	Automatically construct the Certificate Name using cadomain and cahost

[9] When 'certificate' is provisioned, both a CA root certificate and a device certificates must be installed in the phone. Please refer to *Appendix A: Certificate Installation* for details on installing a CA root certificate and a device certificate into the phone.

[10] If a FQDN is entered, the remote user's local network must have access to DNS to resolve the entered name. Typically in a home environment, this would be the service provider's DNS.

dcpcaname1	Character string of 128 characters	CA name included in the SCEP request to identify requested CA (note that not all CA require the CA name)
dcphostnameoverride1	Character string of 128 characters	Override hostname (cahost) for this DCP only
dcpattrcn1	Character string of 128 characters	If “Auto CN” is disabled, this value is used instead of combining cadomain and cahost
dcpattrextkeyusage1	Character string made up of one of the following characters ‘a’ anyExtendedKeyUsage ‘c’ clientAuth ‘i’ ipsecIKE (RFC 4945) ‘m’ iKEIntermediate ’ ’ no Extended Key Usage	Define the Extended Key Usage attributes to be requested for the device certificate. The default is clientAuth.
xatv	‘0’ no tone ‘1’ -36dB ‘2’ -26dB ‘3’ -20dB ‘4’ -16dB ‘5’ -13dB ‘6’ -9dB ‘7’ -6dB ‘8’ 0dB	Alternate tone volume
usb	‘y’ enabled ‘n’ disabled	UBS port enabled [3]
usbm	‘y’ enabled ‘n’ disabled	UBS mouse device enabled [3]
usbk	‘y’ enabled ‘n’ disabled	UBS keyboard device enabled [3]
usbh	‘y’ enabled ‘n’ disabled	UBS headset device enabled [3]
usbms	‘y’ enabled ‘n’ disabled	UBS memory stick (flash drive) device enabled [3]
th	‘0’ black theme ‘1’ metallic blue them ‘2’ blue theme ‘3’ orange theme ‘4’ green theme ‘5’ red theme ‘6’ purple theme	Theme [3]
utb	‘y’ use the selected theme background ‘n’ use the user selected image – if present	Use a user selected background picture [3]
fs	‘y’ enabled ‘n’ disabled	Font smoothing enabled [3]
of	‘y’ enabled ‘n’ disabled	Outlined font enabled [3]
si	‘y’ enabled ‘n’ disabled	Simple icons enabled [3]

[1]: Warning - changing this parameter could impact the network connectivity and may require manual correction

[2]: Warning – provisioning this parameter via TFTP, HTTP, or DHCP means that secure information is transferred in clear text

[3]: Applies to the 1165E IP Deskphone only

Appendix C: Auto-Provisioning the IP Deskphone with the Info Block via TFTP or HTTP (applies to all the IP Deskphones)

The IP Deskphones can receive the Info-Block inside one or more provisioning files that can be retrieved from a TFTP or HTTP server. Multiple provisioning files are supported by the phone:

- SYSTEM provisioning file – provides provisioning information to all IP Deskphones that support the auto-provisioning feature (e.g. system.prv)
- ZONE provisioning file – provides provisioning information to IP Deskphones that belong to a unique defined zone or group (e.g. headqrtr.prv)
- TYPE provisioning file – provides provisioning information to all the IP Deskphones of a particular model types (i.e. 1140E.prv)
- DEVICE provisioning file – provides provisioning information to a specific single device based on the device's MAC address (i.e. 001365FEF4D4.prv)

The provisioning files contain the provisioning Info Block only. The IP Deskphone continues to use the configuration file(s) for obtaining software and font file updates. The provisioning files are text-based file, which contains parameters that require provisioning.

The provisioning files can be downloaded via either TFTP server or a HTTP server. The address of the server is provisioned either manually, via DHCP option 66, or via .

An example of using hierarchal provisioning files (using system, zone and type provisioning files) is as per the following:

system.prv

```
# System level provisioning file
# Applies to all phones
file=zt;                      # read <zone>.prv and <type>.prv
zone=headqrtr;                # Zone id
unid=Main-tower;              # Unique network identification
menulock=p;                   # Menu lock mode
vq=y;                         # Enable 802.1Q for voice
vcp=3;                        # 802.1Q control p bit for voice
vmp=4;                        # 802.1Q media p bit for voice
pcs=a;                        # PC port speed
pcd=a;                        # PC port duplex
dq=y;                         # Enable 802.1Q for PC port
lldp=y;                       # Enable 802.1ab (LLDP)
st=y;                         # Enable stickiness
cachedip=n;                   # Enable cached IP
igarp=n;                      # Ignore GARP
eap=peap;                     # Enable 802.1x (EAP)
eapid1=DEV1024;               # 802.1x (EAP) device ID 1
eapid2=TOW2234;               # 802.1X (EAP) device ID 2
eappwd=D3c6v5;                # 802.1x (EAP) password
cdiff=13;                     # DiffServ code point for control
mdiff=12;                     # DiffServ code point for media
prov=47.11.232.115;           # Provisioning server IP address
dns=47.11.20.20;              # Primary DNS server IP address
dns2=47.11.20.21;             # Secondary DNS server IP address
ct=20;                        # Contrast value
br=18;                        # Brightness value
blt=1;                        # Backlight timer
dimt=3;                       # Set dim timer to 5 minutes
bold=y                        # Enable font display in bold
```

headqrtr.prv

```
# Zone level provisioning file
# Applies to all phones within the headquarters zone
s1ip=47.11.62.20;            # Primary server IP address
p1=4100;                     # Primary server port number
a1=1;                        # Primary server action code
r1=10;                       # Primary server retry count
s2ip=47.11.62.21;            # Secondary server IP address
p2=4100;                     # Secondary server port number
a2=1;                        # Secondary server action code
r2=10;                       # Secondary server retry count
xip=47.11.62.147;            # XAS server IP address
xp=5000;                     # XAS server port number
xa=g;                        # XAS server action code
```

1140E.prv

```
# Type level provisioning file specific to 1140E IP Deskphone
# Applies to all 1140E IP Deskphone within the network
bt=y;                        # Enable Bluetooth
```

For additional information on configuring the IP Deskphone with the Info Block and on auto-provisioning in general, please refer to the IP Phones Fundamentals NN43001-368.

Appendix D: Auto-Provisioning the IP Deskphone's Node and TN in a Communication Server 1000 Environment (applies to all the IP Deskphones)

Auto-provisioning on the 2007, the 1100 Series and the 1200 Series IP Deskphones also includes a centralized method of provisioning the Node and TN fields for these IP Deskphones when they are connected on a Communication Server 1000 system.

Prior to the availability of UNIStim software release 3.0 for IP Deskphones, if the Node and TN values in the phone were un-initialized, the only means to provision the Node and TN value was for the phone installer to manually enter these values at the phone when prompted to do so on the phone's display.

Ever since the delivery of UNIStim software release 3.0 for IP Deskphones the phones will now accept a list of Node and TN values associated to particular MAC addresses. The Node and TN value is assigned to an appropriate phone by the phone recognizing its own MAC address within the list of Node and TN values.

The IP Deskphone will accept the Node and TN information when contained in any of the existing .PRV files including:

- Device file (XXXXXXXXXXXX.PRV)
- Zone file (ZZZZZZZZ.PRV)
- Type file (TTTTT.PRV)
- System file (SYSTEM.PRV)

If the phone's MAC address is found in more than one valid association across the different .PRV files, the association that the phone ultimately accepts will be the one in the highest priority file. The precedence order of the .PRV files from highest priority to lowest is device, zone, type then system as shown above.

A format has been defined, which is similar to the existing auto-provisioning info block items, to provision the Node and TN values. The new Node and TN provision string has the following format:

reg =MACaddr, CallServerType, ConnectServer, NodeID, TN

The items can be separated by spaces or commas or any combination of them. The string is case insensitive, so uppercase, lowercase or mixed case is all acceptable.

MACaddr: Delimiters in the MAC address can be dashes, colons, spaces or any combination thereof. The following are examples of valid MAC address formats:

00-13-65-FE-F4-D4
00:13:65:FE:F4:D4
00 13 65 FE F4 D4
001365FEF4D4

CallServerType: Currently the implementation only supports the Communication Server 1000, thus the only supported CallServerType is CS1K.

ConnectServer: Only values S1 and S1S2 are supported at this time.

NodeID – The Node ID can be any number from 0 - 9999.

TN - The same format is used for the Terminal Number as would be entered via the TN prompt on the phone's display during registration. So two formats exist:

Large system TN: "LLL-SS-CC-UU" or “LLL SS CC UU”
Small system TN: “CC-UU” or “CC UU”

The TN must be in one of the formats shown above. The numbers in the TN can be separated by spaces, dashes or any combination thereof. The numbers can either have leading zeros to fill the field size, or not – e.g. LLL can be 096 or just 96.

Format errors resulting in no processing of the reg provisioning are silently discarded (no error message is provided).

The “reg” item(s) must be at the end of the file’s provisioning info data items. No other provisioning info items should come after it (them). This is required to optimize the speed of the parsing.

The following is an example of a valid Node and TN provision string that could be included in any of the .PRV files.

```
# Set Auto Node and TN
reg=00:1B:BA:F8:82:0D,CS1K,S1,123,096-1-22-01;
reg=00:1B:BA:F8:82:0E,CS1K,S1,123,096-1-22-02;
```

Appendix E: Auto-Provisioning the IP Deskphone with the Info Block via DHCP (applies to all the IP Deskphones)

The new Nortel specific option type ("Nortel-i2004-B") was introduced in UNIStim software release 2.2 for IP Deskphones. The Nortel-i2004-B specific option type expands the number of parameters that can be provisioned to include all those previously provisioned in the existing option type of Nortel-i2004-A, plus more.

In software loads prior to UNIStim software release 2.2 for the 2007 and 1100 Series IP Deskphones the IP Deskphones could obtain only limited provisioning parameters via Nortel specific DHCP options. The Nortel specific DHCP option types supported included:

- **Nortel-i2004-A** a unique identifier for provisioning Nortel call server information into the IP Deskphone
- **VLAN-A** a unique identifier for provisioning 802.1Q VLAN information into the IP Deskphone

With the introduction of the UNIStim software release 2.2 for the 2007 and 1100 Series IP Deskphones[11] a new Nortel specific option type was introduced ("Nortel-i2004-B"). The new Nortel-i2004-B specific option type expands the number of parameters that can be provisioned to include all those previously provisioned in the existing option type of Nortel-i2004-A, plus more. The existing option type of Nortel-i2004-A will continue to be supported for backward compatibility. In fact, the new software will accept both option types, although it is recommended to either remain with the existing option type or move to the new option type, but not both. In the event that the IP Deskphone receives both option types, values provisioned with the new option type of Nortel-i2004-B will have a higher priority than values provisioned with the old option type Nortel-i2004-A.

DHCP option type VLAN-A continues to be supported.

DHCP support for provisioning the IP Deskphones requires DHCP to send a class identifier option with the valid option type in each DHCP Offer and DHCP Acknowledgement.

The IP Deskphone supports both vendor specific sub-ops and site specific options. The new software now supports 42 Nortel specific DHCP options as listed below. Newly claimed options are in bold where as the reclassified[12] options are in italics.

- 21 DHCP vender specific options: *128, 131, 144, 157, 188, 191, 205, 219, 223,* **224, 227, 230**, 232, **235, 238, 241, 244,** 247, **249**, 251, and **254**
- 21 DHCP site specific options: 128, 131, 144, 157, 188, 191, 205, 219, 223, **224, 227, 230**, 232, **235, 238, 241, 244,** 247, **249**, 251, and **254**

The vendor specific field of the DHCP response is parsed to extract the provisioning information.

The format of the "Nortel-i2004-B" DHCP option type is:

Nortel-i2004-B,param1=value1;param2=value2;param3=value3; …

[11]The 1210, 1220 and 1230 IP Deskphones were introduced with UNIStim software release 2.2 and thus support Nortel-i2004-B from their initial release.

[12] RFC 3942 states that DHCP site-specific options 128 to 223 are hereby reclassified as publicly defined options. The IP Deskphone supports 9 vender specific options in this range and will continue to do so for backward compatibility. However, as suggested in RFC3942, the use of these options should be discouraged to avoid potential future collisions.

An example DHCP provisioning string is as per the following[13]:

```
Nortel-i2004-B,s1ip=47.11.62.20;p1=4100;a1=1;r1=255;s2ip=47.11.62.21;
p2=4100;a2=1;r2=2;xip=47.11.62.147;xp=5000;xa=g;
menulock=p;vq=y;vcp=3;vmp=4;vlanf=y;pc=y;pcs=a;pcd=a;
dq=y;dv=y;dvid=60;dp=5;pcuntag=y;
```

The list of all the parameters that can be provisioned via the Nortel-i2004-B options is provided in the Info Block table in Appendix B. Note that not all parameters need be specified in the option string. If the option is included, the parameter will be provisioned with the value specified. If the option is not included, the parameter will retain its default value, or the value that was previously provisioned for said parameter.

[13] Carriage returns have been added to the DHCP configuration string for readability only. A true DHCP configuration string would contain no such carriage returns

Appendix F: Provisioning Precedence Rule and Stickiness Control (applies to all the IP Deskphones)

The 2007, 1100 Series and 1200 Series IP Deskphones can obtain provisioning information from multiple sources when the parameter source is defined as AUTO from the Auto Provisioning page. The sources of automatic provisioning information include:

- LLDP when the phone is connected to an 802.1ab enabled network switch
- DHCP
- Provisioning file transferred via TFTP or HTTP
- Call server (and/or associated telephony manager) using UNIStim

It is assumed that each network provisioning parameter will be supplied by one and only one source. However, if the phone receives network configuration information from multiple sources a precedence rule is applied to determine the one source the phone selects for its provisioning information.

The precedence rule from highest priority to lowest priority for IP Deskphone provisioning is as follows:

- Manual provisioning
- Automatic provisioning using Link Layer Discovery Protocol (LLDP) from an 802.1ab enabled network switch
- Automatic provisioning using Info Block contained within provisioning files (and transferred via TFTP or HTTP). Provisioning files contain their own precedence order based on the file type:
    - Info Block carried by the Device-specific provisioning file
    - Info Block carried by the Zone-specific provisioning file
    - Info Block carried by the Type-specific provisioning file
    - Info Block carried by the System-specific provisioning file
- Automatic provisioning using Info Block contained within DHCP option strings (and transferred via DHCP Acknowledge message). DHCP provision contain its own precedence order based on the DHCP option
    - Info Block carried by the Nortel-i2004-B DHCP option
    - Former provisionable parameters carried by the Nortel-i2004-A DHCP option
    - (Note that VLAN-A option is still supported with both Nortel-i2004-B DHCP and Nortel-i2004-A DHCP options)
- Automatic provisioning from the call server (and/or associated telephony manager) using UNIStim
- Last automatic provisioned value
- Factory default

Automatic provisioning defines provisioning control for each parameter. One can either manually or automatically provision each parameter. Each provisioning parameter provides an attribute that specifies if the parameter was previously provisioned manually or automatically.

If the provisioning parameter is AUTO, the IP Deskphone can receive the value from automatic provisioning sources based on the precedence rule. If one manually changes the parameter, the attribute value is MANUAL. If the attribute is MANUAL, the provisioning information from automatic provisioning sources is ignored except for the standard DHCP parameters. If one enables DHCP, then the phone's IP address, the subnet mask, and the default gateway address, which the IP Deskphone obtains from the DHCP server, overwrites any manually configured value.

Provisioning information from a provisioning source with high priority will overwrite the provisioning information from a provisioning source with low priority. Manual provisioning always has the highest priority.

If one configure stickiness and the current provisioning source does not provide the provisioning information for the particular parameter, the last received provisioning value is used. The default value of the stickiness attribute is AUTO.

Appendix G: Manual Configuration Menu on the 1120E, 1140E, 1150E and 1165E IP Deskphones

The full-screen based configuration menu structure below presents the complete configuration menu now available on the 1120E, 1140E, 1150E and 1165E IP Deskphones:

EAP Mode: [Disable, MD5, PEAP, TLS]
ID 1:
ID 2:
Password:
Enable VPN: []
Protocol:
Mode:
Authentication:
PSK User ID:
PSK Password:
XAUTH Method:
XAUTH User ID:
XAUTH Password:
VPN Server 1: xxx.xxx.xxx.xxx
VPN Server 2: xxx.xxx.xxx.xxx
VPN DSCP:
VPN MOTD Timer:
Enable 802.1ab (LLDP): []
DHCP: [No, Yes]
Set IP: xxx.xxx.xxx.xxx
Net Mask: xxx.xxx.xxx.xxx
Gateway: xxx.xxx.xxx.xxx
DNS1 IP: xxx.xxx.xxx.xxx
DNS2 IP: xxx.xxx.xxx.xxx
Local DNS IP: xxx.xxx.xxx.xxx
CA Server:
Domain Name:
Hostname:
S1 IP: xxx.xxx.xxx.xxx
Port:
S1 Action:
Retry:
S1 PK: FFFFFFFFFFFFFFFF
S2 IP: xxx.xxx.xxx.xxx
Port:
S2 Action:
Retry:
S2 PK: FFFFFFFFFFFFFFFF
Ntwk Port Speed: [Auto, 10BT, 100BT]
Ntwk Port Duplex: [Auto, Force Full, Force Half]
XAS Mode: [Text Mode, Graphical, Secure Graphical] *This parameter is called "Graphical XAS" on the 1165E IP Deskphone.*

XAS IP: xxx.xxx.xxx.xxx
XAS Port:
Enable Voice 802.1Q: []
VoiceVLAN: [No VLAN, Auto, Enter VLAN ID]
The Auto option in the VoiceVLAN menu is only available if DHCP is provisioned to "Yes" above or if LLDP is enabled above
VLAN Filter : []
Ctrl Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]
Media Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]
Enable Nortel Auto Qos: []
DSCP Override: [] *This DSCP Override menu item is only presented if "Enable 802.1ab (LLDP)" is enabled above and "Control DSCP" or "Media DSCP" are not manually set below*
Control DSCP: xx
Media DSCP: xx
Enable PC Port: []
PC Port Speed: [Auto, 10BT, 100BT]
PC Port Duplex: [Auto, Force Full, Force Half]
Enable Data 802.1Q: []
DataVLAN: [No VLAN, Enter VLAN ID]
Data Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]
PC-Port Untag All: []
Enable Stickiness []
Cached IP: [] *This Cached IP menu item is only presented if DHCP is provisioned to "Yes".*
Ignore GARP: []
Enable SRTP PSK: []
SRTP PSK Payload ID: [96, 115, 120]
Provision: xxx.xxx.xxx.xxx
Provision Zone ID:
Enable Bluetooth: [Yes, No] *This Bluetooth menu item is on the 1140E IP Deskphone and 1150E only.*

The 1120E, 1140E, 1150E and 1165E IP Deskphones contain a password protection mechanism to lock out access to the Local Tools menu including the Network Configuration menu. If enabled, access to the Local Tools menu is password protected and the password is prompted by a pop up window. One must type the password from the dial pad and press the center of the navigation cluster (enter key) to enter the Network Configuration menu. The default password is 26567*738 (color*set), but this password can be changed by the system administrator.

When an incorrect password is entered, the Local Tools menu is not opened.

To thwart password guessing, only 3 incorrect password entries in a row are allowed. After the 3rd incorrect entry, the password entry is ignored for 5 minutes. During this period of time, the password prompt is displayed and the entered digits accepted; however, the phone will not process the incoming digits. The password prompt window simply closes and the behavior is identical to that of an incorrect password entry. The user will assume the incorrect password has been entered and try again. Thus even if the correct password is guessed during the 5 minute period, it will be ignored. This effectively reduces the guess entry rate to 3 guesses every 5 minutes.

Once the password has been entered, access to the Local Tools menu remains active for 5 minutes. During the 5 minutes, the menu can be freely navigated, exited and entered without being prompted again for the password. When the 5 minutes expires, the menu is closed. The password must be reentered to access the Local Tools menu.

Appendix H: Manual Configuration Menu on the 2007 IP Deskphone

The full-screen based configuration menu structure below presents the complete configuration menu now available on the 2007 IP Deskphone:

EAP Mode: [Disable, MD5, PEAP, TLS]
- **ID 1:**
- **ID 2:**
- **Password:**

Enable 802.1ab (LLDP): []
DHCP: [No, Yes]
- **Set IP: xxx.xxx.xxx.xxx**
- **Net Mask: xxx.xxx.xxx.xxx**
- **Gateway: xxx.xxx.xxx.xxx**

DNS1 IP: xxx.xxx.xxx.xxx
DNS2 IP: xxx.xxx.xxx.xxx
CA Server:
Domain Name:
Hostname:
S1 IP: xxx.xxx.xxx.xxx
Port:
S1 Action:
Retry:
S1 PK: FFFFFFFFFFFFFFFF
S2 IP: xxx.xxx.xxx.xxx
Port:
S2 Action:
Retry:
S2 PK: FFFFFFFFFFFFFFFF
Ntwk Port Speed: [Auto, 10BT, 100BT]
- **Ntwk Port Duplex: [Auto, Force Full, Force Half]**

Phone Mode [Hidden, Full, Reduced]
XAS Mode [Text Mode, Graphical, Full Screen, Secure Graphical, Secure Full Screen]
XAS IP: xxx.xxx.xxx.xxx
Port:
Enable Voice 802.1Q: []
- **VoiceVLAN: [No VLAN, Auto, Enter VLAN ID]**

The Auto option in the VoiceVLAN menu is only available if DHCP is provisioned to "Yes" above or if LLDP is enabled above, respectively.
- **VLAN Filter : []**
- **Ctrl Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]**
- **Media Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]**

Enable Nortel Auto QoS: []
DSCP Override: [] *This DSCP Override menu item is only presented if "Enable 802.1ab (LLDP)" is enabled above and "Control DSCP" or "Media DSCP" are not manually set below*
- **Control DSCP: xx**
- **Media DSCP: xx**

Enable PC Port: []
- **PC Port Speed: [Auto, 10BT, 100BT]**
- **PC Port Duplex: [Auto, Force Full, Force Half]**
- **Enable Data 802.1Q: []**
- **DataVLAN: [No VLAN, Enter VLAN ID]**
- **Data Priority Bits: [Auto, 0, 1, 2, 3, 4, 5, 6, 7]**
- **PC-Port Untag All: []**

Enable Stickiness []
Cached IP: [] *This Cached IP menu item is only presented if DHCP is provisioned to "Yes" above.*
Ignore GARP: []
Enable SRTP PSK: []
- **SRTP PSK Payload ID: [96, 115, 120]**

Provision: xxx.xxx.xxx.xxx
Provision Zone ID:

The 2007 IP Deskphone contains a password protection mechanism to lock out access to the Local Tools menu including the Network Configuration menu. If enabled, access to the Local Tools menu is password protected and the password is prompted by a pop up window. One must type the password from the dial pad and press the center of the navigation cluster (enter key) to enter the Network Configuration menu. The default password is 26567*738 (color*set), but this password can be changed by the system administrator.

When an incorrect password is entered, the Local Tools menu is not opened.

To thwart password guessing, only 3 incorrect password entries in a row are allowed. After the 3rd incorrect entry, the password entry is ignored for 5 minutes. During this period of time, the password prompt is displayed and the entered digits accepted; however, the phone will not process the incoming digits. The password prompt window simply closes and the behavior is identical to that of an incorrect password entry. The user will assume the incorrect password has been entered and try again. Thus even if the correct password is guessed during the 5 minute period, it will be ignored. This effectively reduces the guess entry rate to 3 guesses every 5 minutes.

Once the password has been entered, access to the Local Tools menu remains active for 5 minutes. During the 5 minutes, the menu can be freely navigated, exited and entered without being prompted again for the password. When the 5 minutes expires, the menu is closed. The password must be reentered to access the Local Tools menu.

Appendix I: Manual Configuration Menu on the 1110, 1210, 1220 and 1230 IP Deskphones

The single-line based configuration menu structure below presents the complete configuration menu now available on the 1110 and 1200 Series IP Deskphones:

EAP[0-N,1-M, 2-P, 3-T]:0
if "1" or "2" or "3"
ID 1: [ ]
also if "1" or "2"
ID 2: [ ]
Password: [*******]
LLDP Enable?[0-N,1-Y]:0
DHCP? [0-N,1-Y]:1
if "0"
Set IP: xxx.xxx.xxx.xxx
Netmsk: xxx.xxx.xxx.xxx
Def GW: xxx.xxx.xxx.xxx
DNS1 IP: xxx.xxx.xxx.xxx
DNS2 IP: xxx.xxx.xxx.xxx
CA Server:
Domain Name:
Hostname:
S1 IP: xxx.xxx.xxx.xxx
S1 Port:
S1 Action:
S1 Retry Count:
S2 IP: xxx.xxx.xxx.xxx
S2 Port:
S2 Action:
S2 Retry Count:
Speed[0-A,1-10,2-100]:0
if "1" or "2"
Duplex[0-A,1-F,2-H]:0
Cfg XAS? [0-N, 1-Y]:1
if "1"
XAS IP: xxx.xxx.xxx.xxx

Voice 802.1Q[0-N,1-Y]:1

if "1"

Voice VLAN?[0-N,1-Y]:0

if "1"

VLAN Cfg ?0-Auto,1-Man :1

This VLAN Cfg menu is only presented if DHCP is provisioned to "Y" above or if LLDP Enabled is provisioned to "Y" above.

if "1"

VLAN ID :

VLAN Filter?[0-N,1-Y] :0

Ctrl pBits[0-7,8-Au] :8

Media pBits[0-7,8-Au] :8

NT AutoQOS? [0-N,1-Y]:0

DSCP Ovride [0-N,1-Y]:0 *This DSCP Override menu item is only presented if "LLDP Enable?" is enabled above and neither the "Control DSCP" or "Media DSCP" are not manually set below*

CTRL DSCP [0-63]: xx

Media DSCP [0-63]: xx

PC Port ? [0-Off,1-On] :1

if "1"

Speed[0-A,1-10,2-100]:0

if "1" or "2"

Duplex[0-A,1-F,2-H]:0

Data 802.1Q[0-N,1-Y]:1

if "1"

VLAN ID :

Data pBits[0-7,8-Au] :8

PCUntagAll? [0-N,1-Y]:1

Stickiness? [0-N,1-Y]:1

Cached IP? [0-N, 1-Y]:0 *This Cached IP menu item is only presented if DHCP is provisioned to "Y" above*

GARP Ignore?[0-N,1-Y]:0

SRTP PSK? [0-N, 1-Y]:0

PayID[0-96,1-115,2-120]0

Prov: xxx.xxx.xxx.xxx

Prov Zone ID:

End of Menu

The 1110, 1210, 1220 and 1230 IP Deskphones contain a password protection mechanism to lock out access to the Local Tools menu including the Network Configuration menu. If enabled, access to the Local Tools menu is password protected and the password is prompted by a pop up window. One must type the password from the dial pad and press the center of the navigation cluster (enter key) to enter the Network Configuration menu. The default password is 26567*738 (color*set), but this password can be changed by the system administrator.

When an incorrect password is entered, the Local Tools menu is not opened.

To thwart password guessing, only 3 incorrect password entries in a row are allowed. After the 3rd incorrect entry, the password entry is ignored for 5 minutes. During this period of time, the password prompt is displayed and the entered digits accepted; however, the phone will not process the incoming digits. The password prompt window simply closes and the behavior is identical to that of an incorrect password entry. The user will assume the incorrect password has been entered and try again. Thus even if the correct password is guessed during the 5 minute period, it will be ignored. This effectively reduces the guess entry rate to 3 guesses every 5 minutes.

Once the password has been entered, access to the Local Tools menu remains active for 5 minutes. During the 5 minutes, the menu can be freely navigated, exited and entered without being prompted again for the password. When the 5 minutes expires, the menu is closed. The password must be reentered to access the Local Tools menu.

Appendix J: Restore to Factory Defaults (applies to all the IP Deskphones)

The UNIStim software release 3.0 for IP Deskphones introduced the ability to restore an IP Deskphone to a “factory default” configuration. This can be useful when redeploying an IP Deskphone from one location to another, when starting to use an IP Deskphone with unknown history, or to reset to a known baseline configuration.

With UNIStim software release 3.0, and greater, the following keypad sequence is used to reset all provisioning parameters to a “factory default”:

[*][*][7][3][6][3][9][MAC][#][#]

Where MAC corresponds to the MAC address of the IP Deskphone which can be found on a label on the back of the IP Deskphone.

Since a MAC address can contain the letters A through F, the letters A, B and C can be entered via the [2] key on the dialpad, and letters D, E and F can be entered via the [3] key.

For example, an IP Deskphone with MAC address 00:19:E1:E2:17:12 would be reset to “factory default” when the sequence **73639001931321712## is entered on the keypad.

Please note that the keypad sequence will only be accepted by the phone after the IP Deskphone has finished its boot-up procedure.

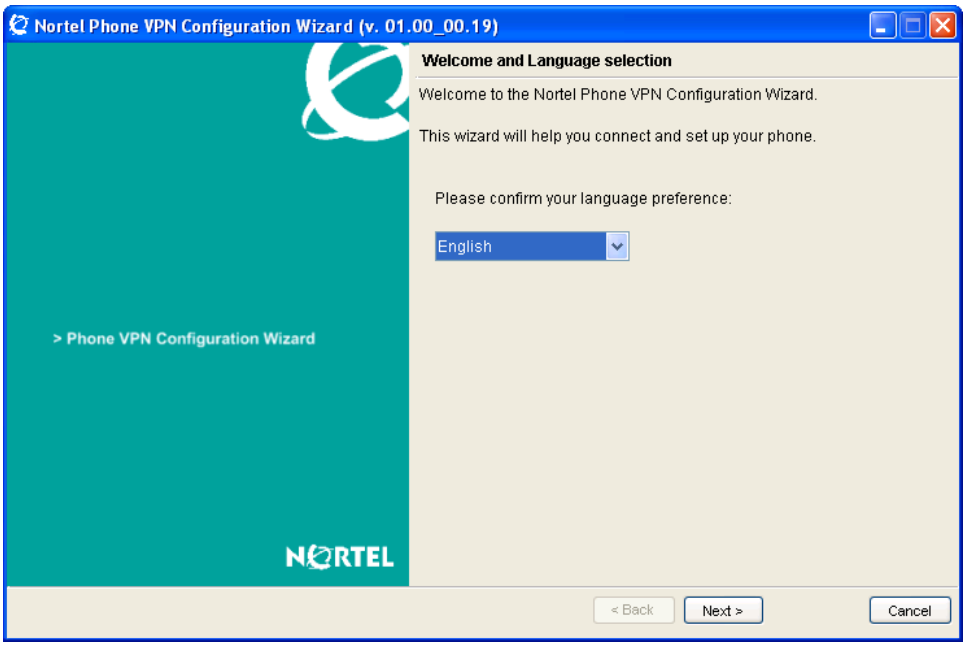
Appendix K: Phone VPN Configuration Wizard

This Appendix will walk though the few steps required to use the Phone VPN Configuration Wizard. Using the Phone VPN Configuration Wizard involves seven simple steps including:

1) Welcome and Language selection
2) Equipment Setup and VPN
3) Select Data Files
4) Prepare Phone for Configuration
5) Autodiscover Phone
6) Configure Phone
7) Confirmation and Finish

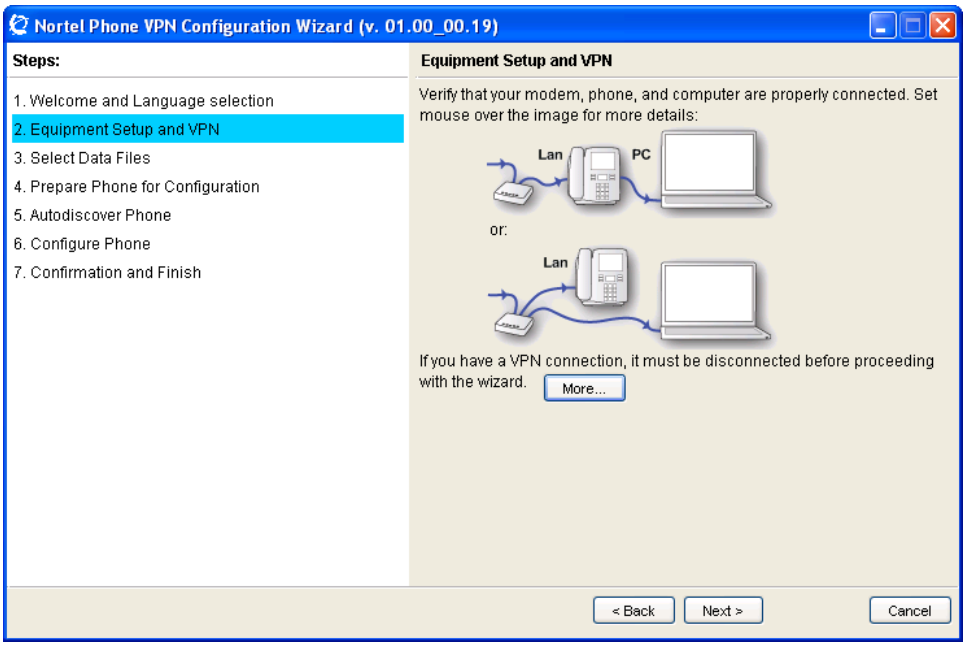
Welcome and Language selection

Upon launching the Phone VPN Configuration Wizard, the user is presented with the welcome screen. At the welcome screen the user can select from a choice of languages (English is the default). The diagram below shows the welcome screen.



Equipment Setup and VPN

Once the language is selected the Equipment Setup and VPN screen is presented as depicted below.

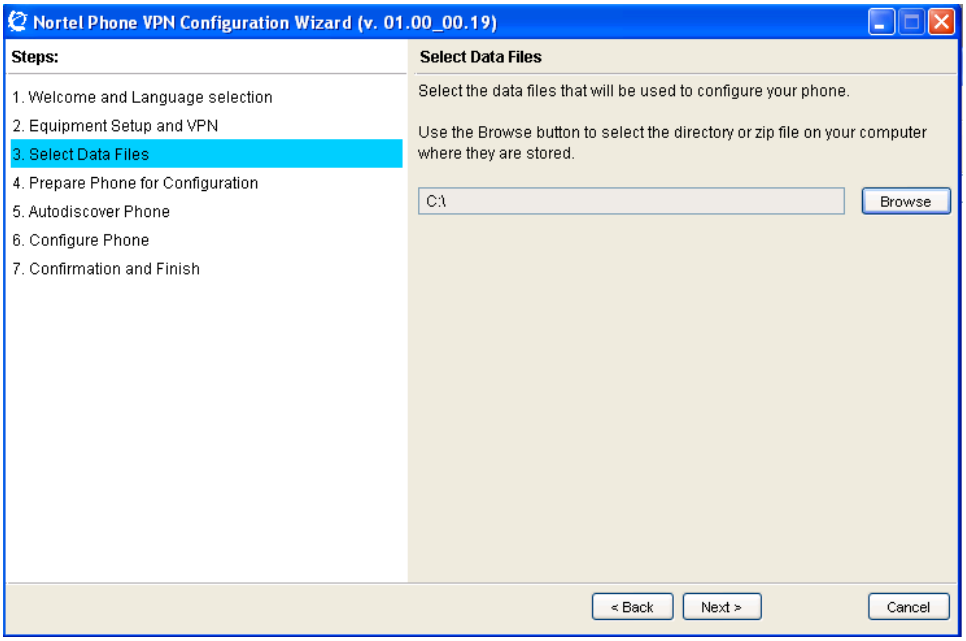


The Equipment Setup and VPN screen shows that the PC running the Phone VPN Configuration Wizard must either be plugged into the PC port of the IP Deskphone, or into a multi-port router or hub to which the IP Deskphone is also connected.

Please be advised that if a VPN client is running on the PC, the VPN client on the PC must be disconnected to allow the Phone VPN Configuration Wizard to provision the IP Deskphone. Once the Phone VPN Configuration Wizard finishes, the VPN client running on the PC can be re-established.

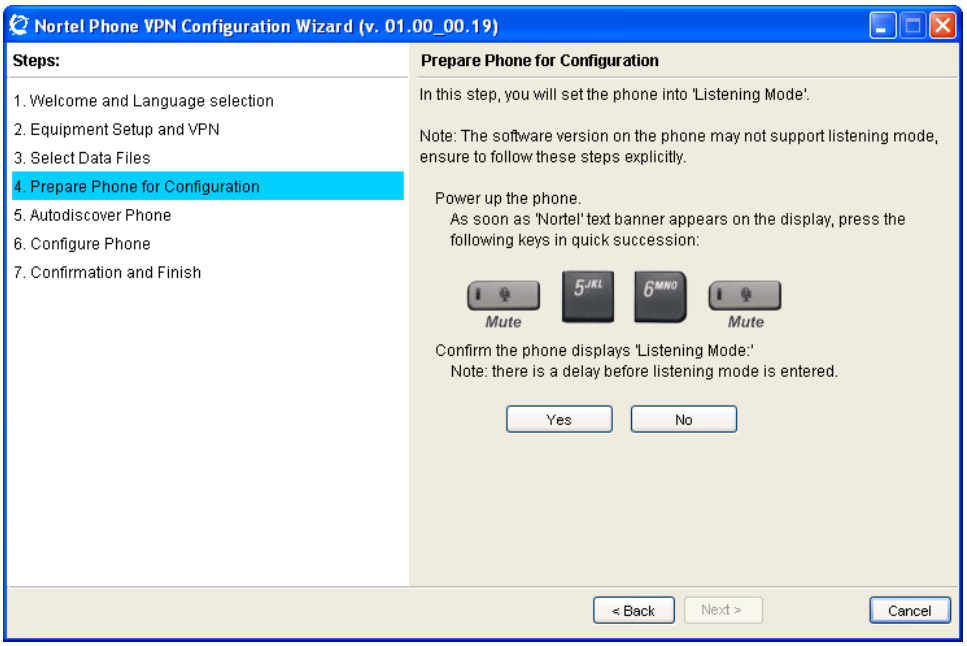
Select Data Files

Once the PC that is running the Phone VPN Configuration Wizard is connected in one of the requested setup, the next screen, as depicted below, asked the user to select the Data Files. The data files are the configuration and provisioning files that were supplied by the System Administrator and which are stored somewhere on the PC. The Select Data File screen asked the user to locate either the zip file containing the configuration and provisioning files or the directory where the configuration and provisioning files are located.



Prepare Phone for Configuration

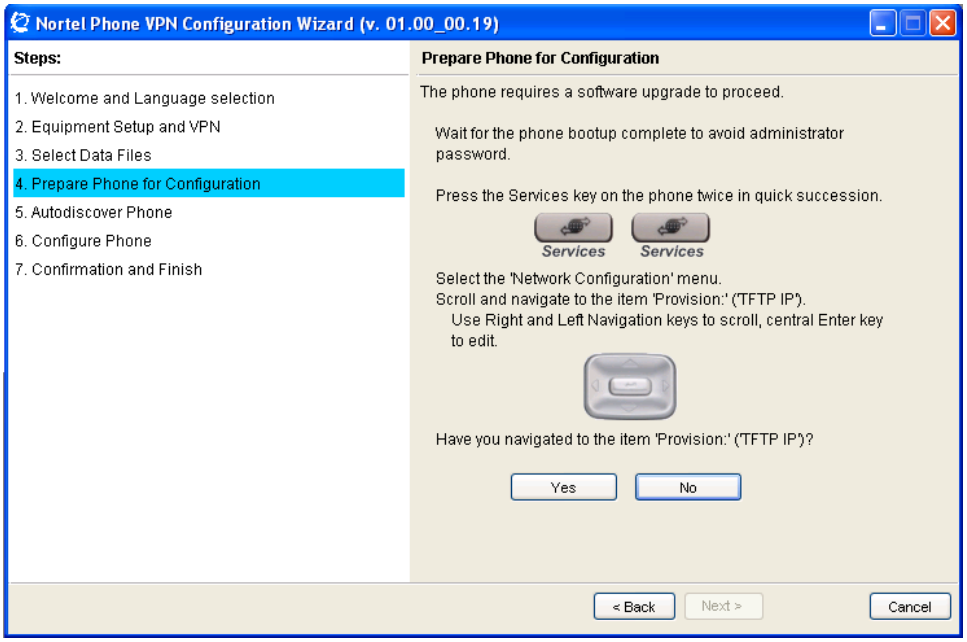
Once the data files (configuration and provisioning files) are located, the Prepare Phone for Configuration Screen provides instructions for placing the phone into “Listening Mode”. Listening Mode allows the phone to listen for the Phone VPN Configuration Wizard to establish a connection and transfer the data files. The Prepare Phone for Configuration screen is depicted below.



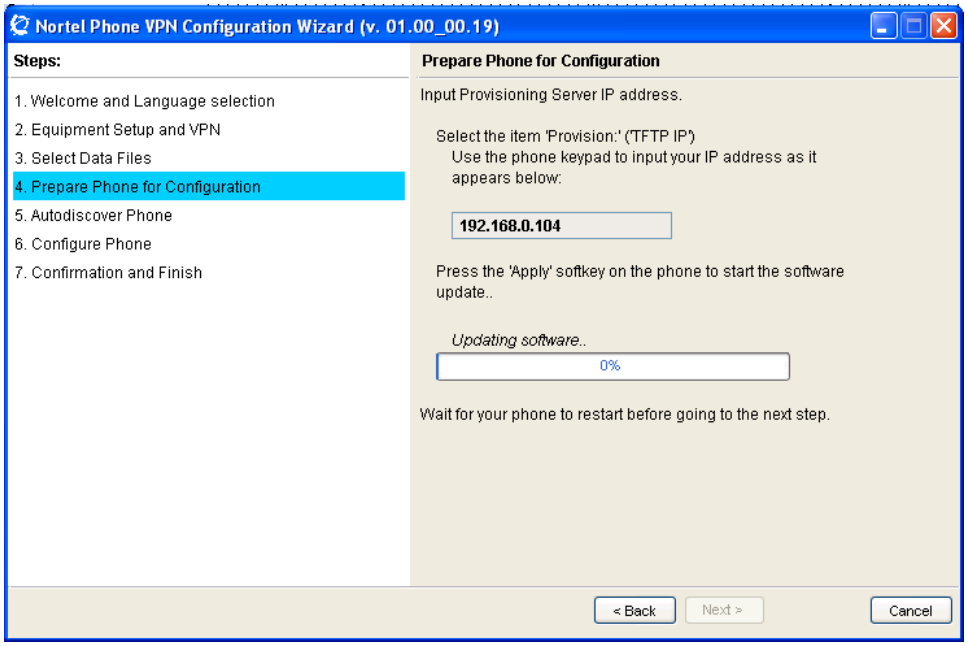
Autodiscover Phones

The IP Deskphone must now be power cycled and when the IP Deskphone is rebooting the user must watch the phone screen for when the “Nortel” text banner (not the Nortel icon) is displayed. The “Nortel” text banner will be displayed for roughly 5 seconds. During this 5 second window the user must press the key sequence of “mute, 5, 6, mute” on the phone as shown on the Prepare Phone for Configuration screen. If successful, the phone will display “Listening Mode” on its screen. If the phone successfully entered Listening Mode, please skip ahead to the “Autodiscover Phones – Listening Mode” section below.

If the phone did not successfully enter Listening Mode, the user can answer “No” on the Prepare Phone for Configuration Screen. The Phone VPN Configuration Wizard will ask the user to try again, and after two unsuccessful attempts, the Phone VPN Configuration Wizard will assume the phone cannot be placed in Listening Mode because the software release on the phone is prior to UNIStim release 4.0. The Phone VPN Configuration Wizard will then guide the user through the steps to use the Phone VPN Configuration Wizard to actually upgrade the phone’s software. The diagram below depicts the screen presented to guide the user through the software upgrade procedure if the phone did not successfully enter Listening Mode.



To upgrade the IP Deskphone’s software, the Provisioning server address in the Network Configuration menu needs to be modified to point to the PC running the Phone VPN Configuration Wizard. The steps required are detailed in the Prepare Phone for Configuration screens depicted above and below. Initially the Provisioning server address parameter has to be located as instructed in the screen above. After which the parameter has to be modified to point to the PC running the Phone VPN Configuration Wizard. The Wizard provides the IP address of the PC that needs to be entered into the Provisioning server address parameter as shown in the below.

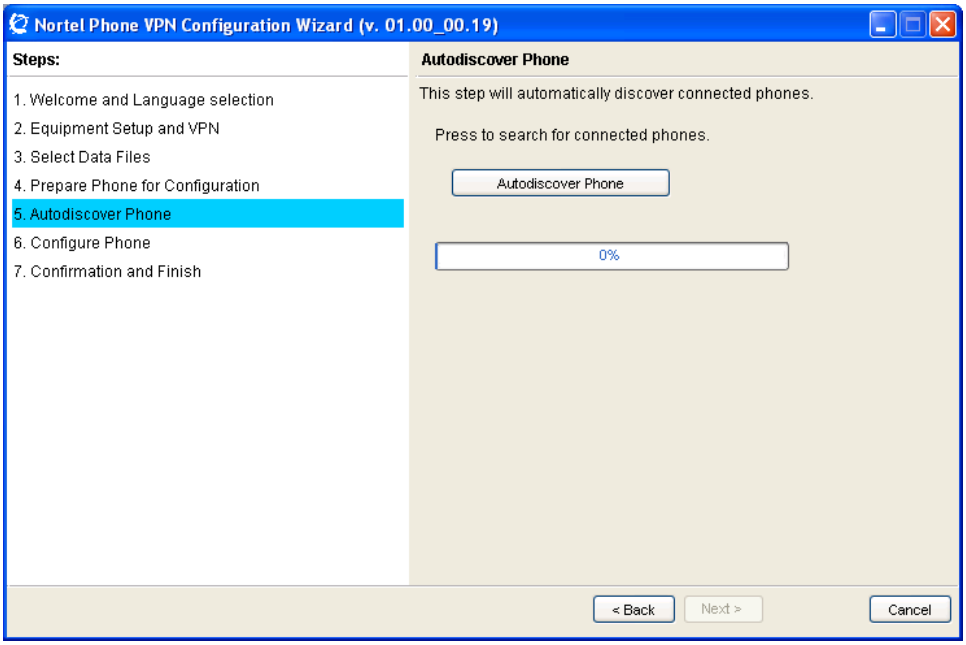


Once the phone has been upgraded to UNIStim software release 4.0 or greater, the phone should be able to enter Listening Mode. The IP Deskphone will reboot after the new software is downloaded.

Again, during reboot the user must watch the phone screen for when the “Nortel” text banner (not the Nortel icon) is displayed. The “Nortel” text banner will be displayed for roughly 5 seconds. During this 5 second window the user must press the key sequence of mute, 5, 6, mute. If successful, the phone will display “Listening Mode” on the screen.

Autodiscover Phones – Listening Mode

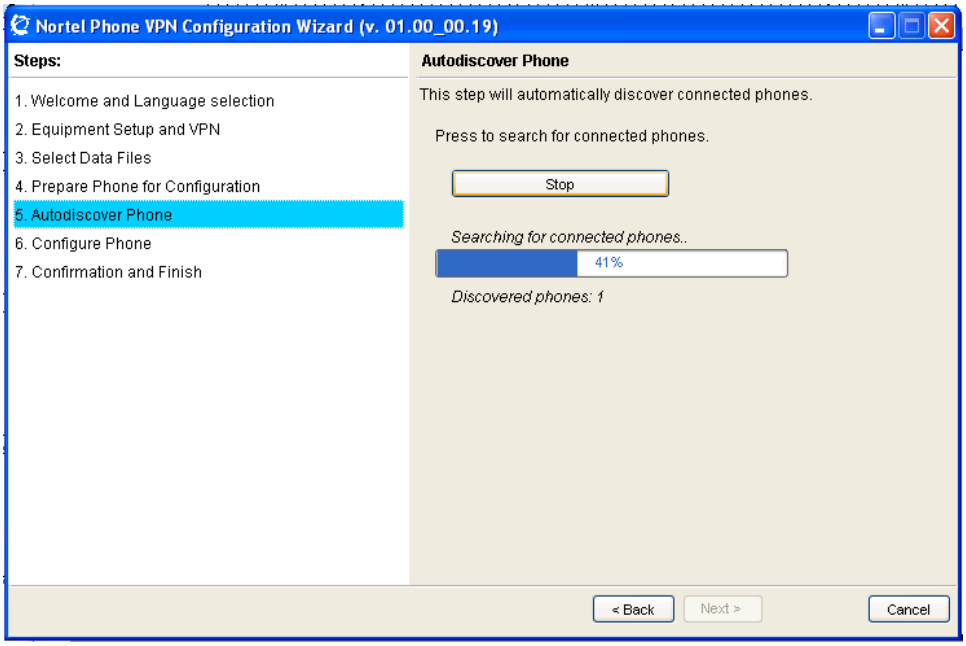
Once the phone is in Listening Mode, the next screen of the Phone VPN Configuration Wizard guides the user to discover the IP Deskphones that are in Listening Mode. The user is prompted to start the discovery process by pressing the “Autodiscover Phone” button. The Autodiscover Phone screen is shown in the diagram below.



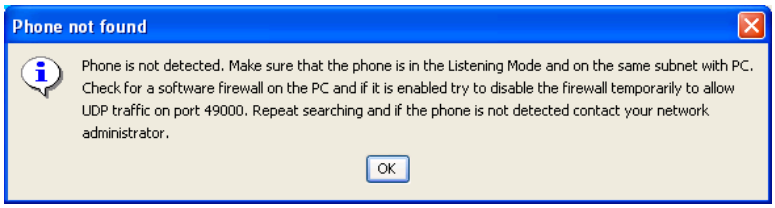
The Autodiscover process will find all phones in Listening Mode on the network. In most cases there will only be one phone discovered – the phone that the user placed in Listening Mode. But if for whatever reason several phones are found in Listening Mode, the user will be prompted to select the phone they wish to provision from a list. The phone’s MAC address is used as the selection mechanism to decide which phone is to be configured[14].

[14] The MAC address of the IP Deskphone can be found on a label on the back of the IP Deskphone.

The diagram below depicts the Autodiscovery mechanism in progress and indicates that one phone has been discovered.

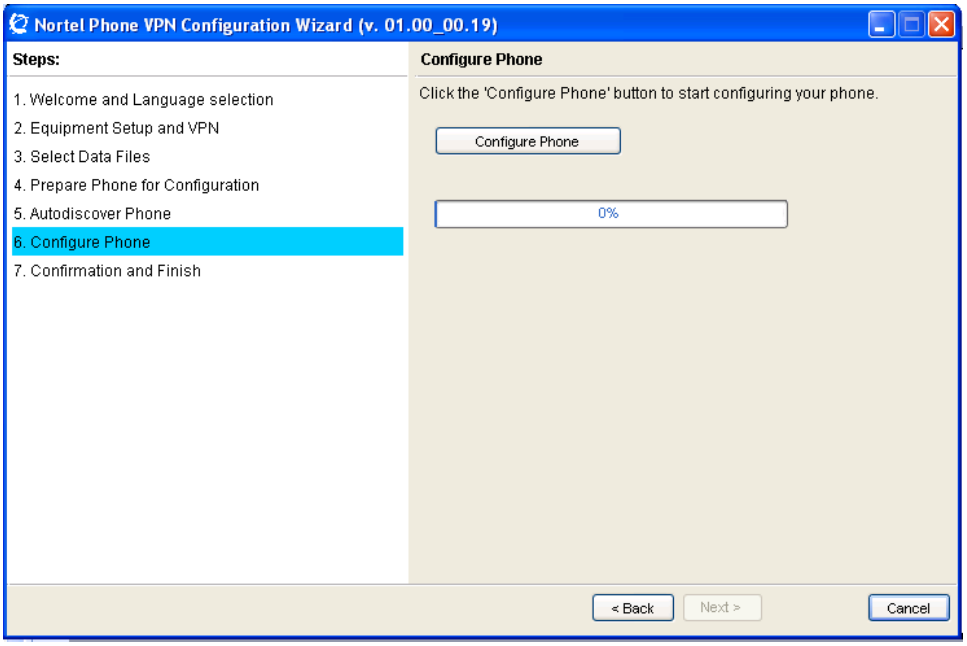


If a phone cannot be discovered, the Phone VPN Configuration Wizard warns that no phones can be found with the Phone not found screen shown below. If repeated attempts fail to discover a phone in Listening Mode please contact your network administrator.



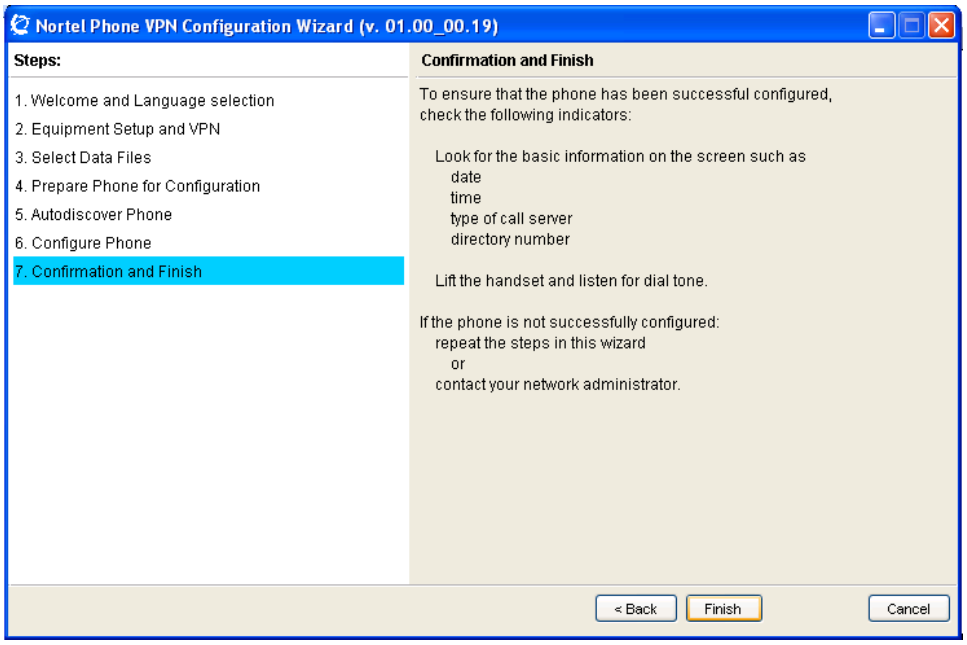
Configure Phone

Once a phone has been discovered the Phone VPN Configuration Wizard is ready to configure the phone. The Configure Phone screen, as depicted below, prompts the user to start the configuration process by pressing the ‘Configure Phone’ button.



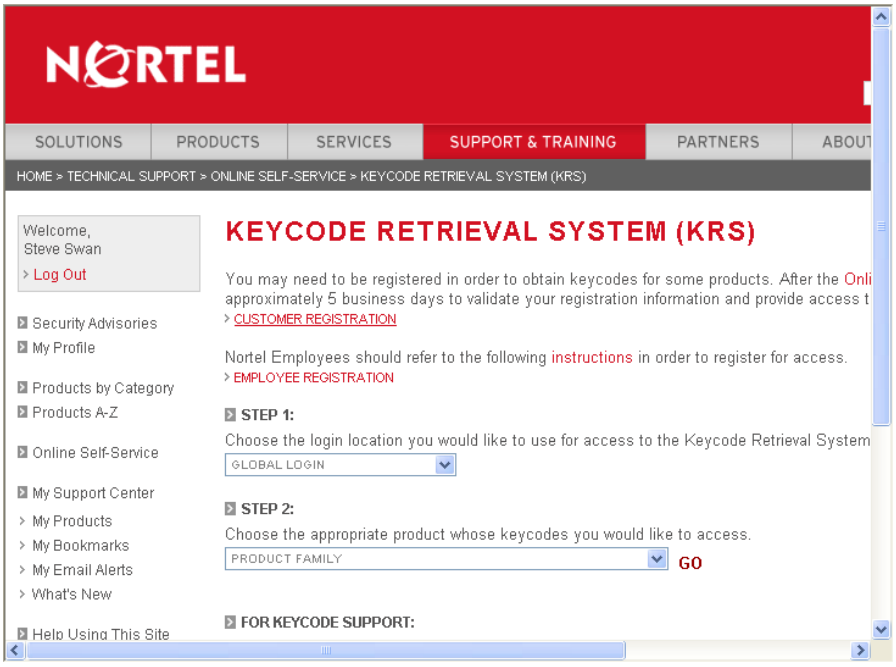
Confirmation and Finish

After the phone has been successfully configured, the Confirmation and Finish screen is presented. The Confirmation and Finish screen is shown below. At this point the phone is ready to connect to the corporate network.

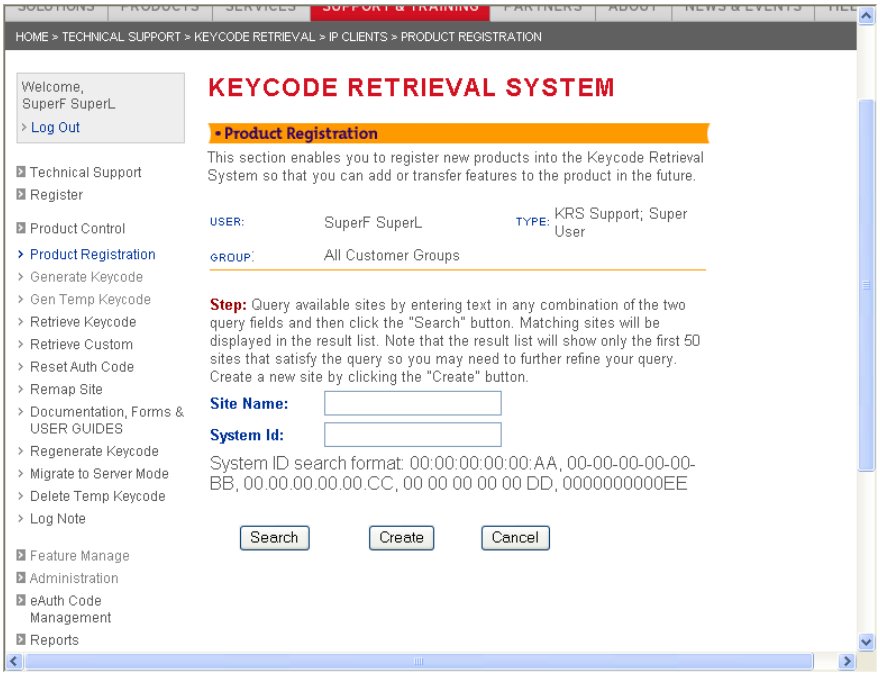


Appendix L: Nortel Keycode Retrieval System (KRS)

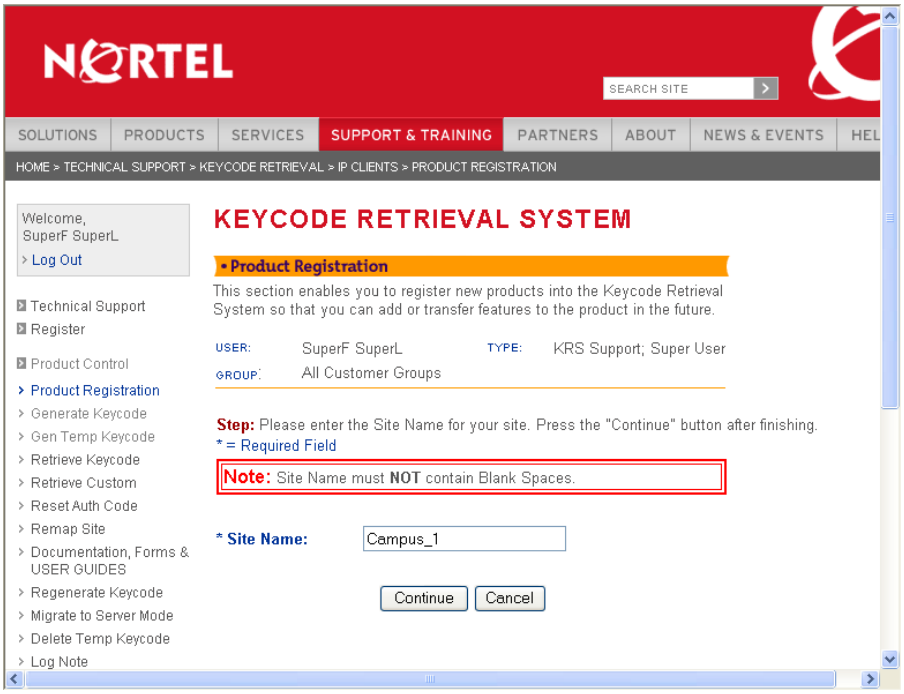
The home page of KRS is the Login and Product Select page as shown in the diagram below. If you do not already have a KRS account, click on Customer Registration and follow the instructions to request an account.



If you do already have an account, select “IP Clients” from the PRODUCT FAMILY pull down list which will then prompt you to enter your user ID and password. After logging into the IP Clients’ KRS product family, the default screen is the Product Registration page as shown below.

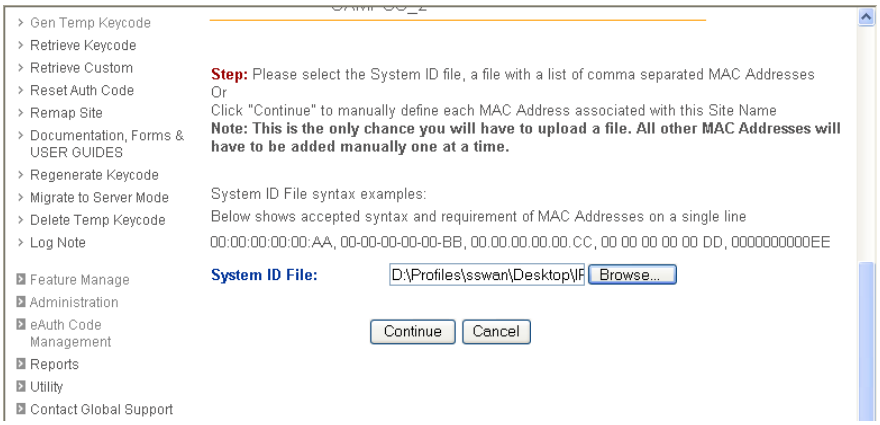


Before a keycode can be generated the system for which the keycode is to be generated must be registered. To begin Registration, one selects “Create” on the Product Registration Screen. After which the screen as shown below will allow one to enter a site name that will be used to identify the system. Please note that blank spaces are not allowed within the site name. Once a site name is entered, clicking on “Continue” advances to the next screen.



At present, for IP Clients UNIStim VPN Client licenses, one must register the MAC address of each IP Deskphone onto which a license is to be installed. The MAC addresses can be provided to KRS using one of two methods: 1) using a comma delimited file of MAC addresses to KRS or 2) manually typing in each MAC address.

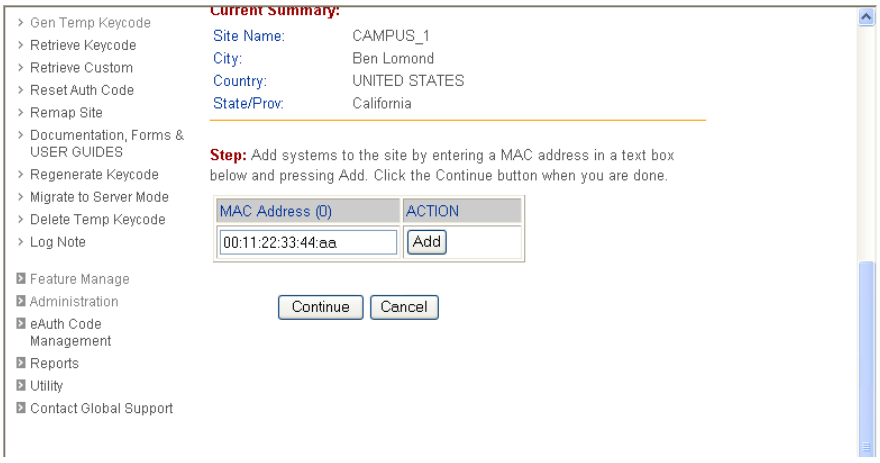
To use a comma delimited file of MAC addresses, select the Browse button to locate the file on the computer connected to KRS as shown on the diagram below. Once the comma delimited file of MAC addresses has been selected click Continue.



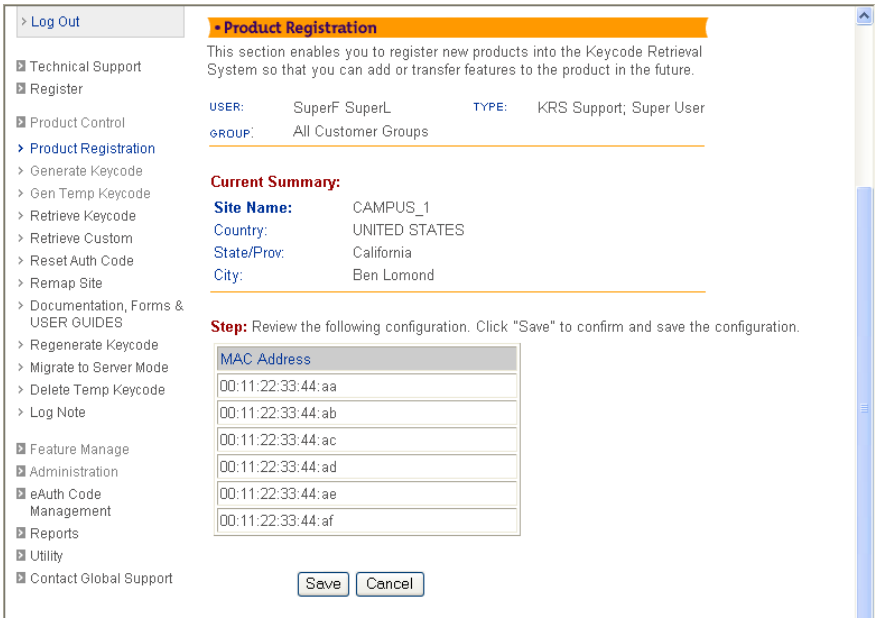
To manually type in each MAC address instead, leave the System ID File field blank and simply click Continue.

The next screen simply request information on the System location. Once it is entered click Continue.

If the MAC addresses were supplied by a comma delimited file, after entering the location information the next screen displayed is a summary screen. But if the MAC addresses were not supplied by a comma delimited file, after entering the location information, the next screen, as depicted below, allows the user to enter the MAC addresses manually. The MAC addresses are entered, one at a time, in the field labeled MAC Address ID. After each MAC address is entered click on Add which will then bring up a new blank MAC Address ID field to allow the entry of the next MAC address. This process should be repeated until all the MAC addresses have been entered. When all the MAC addresses have been entered, click on Continue.

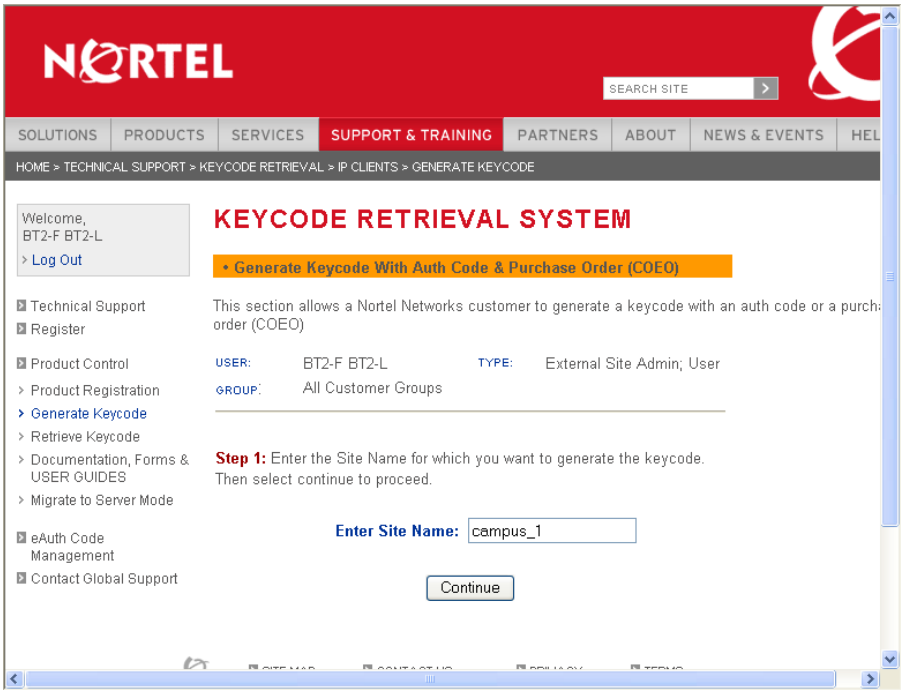


After all the MAC addresses have been entered (either manually or from a file) a summary screen as shown below will be presented to allow the user to review the list of MAC addresses



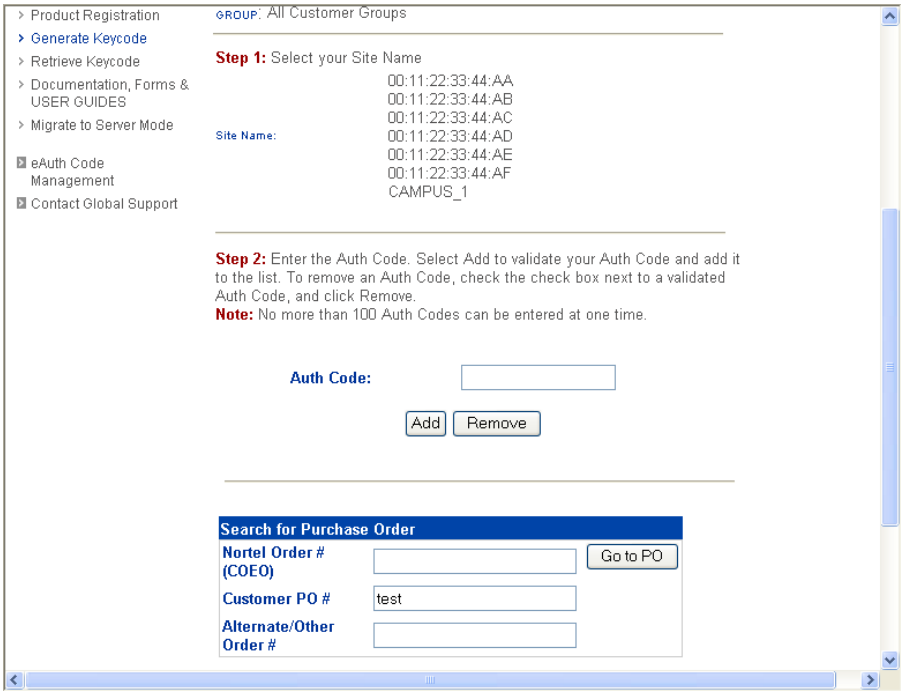
Once the user is satisfied that all the MAC addresses are correct, click Save to confirm and save the configuration. If the Save is successful a Thank You confirmation will be displayed.

Registration is now complete and one is ready to generate the keycode by selecting Generate Keycode from the side bar on the left. The Generate Keycode page will be presented as shown below.



On the Generate Keycode page, the system for which a keycode is to be generated must be identified. The system is identified by entering the system ID, (i.e. the same site name used when the system was registered). Once the system ID is entered click on Continue.

To generate a keycode one must either have a numeric authorization code or one can search for a specific Purchase Order (PO). The example screen below depicts searching for a PO. Click Go to PO after entering the PO number[15].



Once the correct PO is found, the next screen will show a list of each licensed feature on the PO[16]. On this licensed feature screen the user can select the quantity of each licensed feature required within the keycode. Please note that KRS requires that the quantity selected be evenly divisible by the number of "registered" MAC addresses. For example if 6 MAC addresses were registered then one must select multiples of 6 (i.e. 6, 12, 18, 24 etc.)[17] Once the quantity of each licensed feature has been specified click on Continue.

KRS will then show a summary of the current PO selection. Clicking on Continue returns the user to the "select" PO screen again, where if one wish they can search for additional PO's from which to pull additional licenses to add to the Keycode.

Once all the necessary PO have been reviewed, selecting "Go To Summary" will take move KRS to the final summary screen showing; the system ID, list of MAC addresses, PO(s), feature(s) and quantity selected going into the keycode. If everything is correct in the summary clicking on Generate Keycode starts the actual keycode generation. Generation of the keycode can take between 10 and 20 seconds. When complete, the KRS will show the Retrieve History screen.

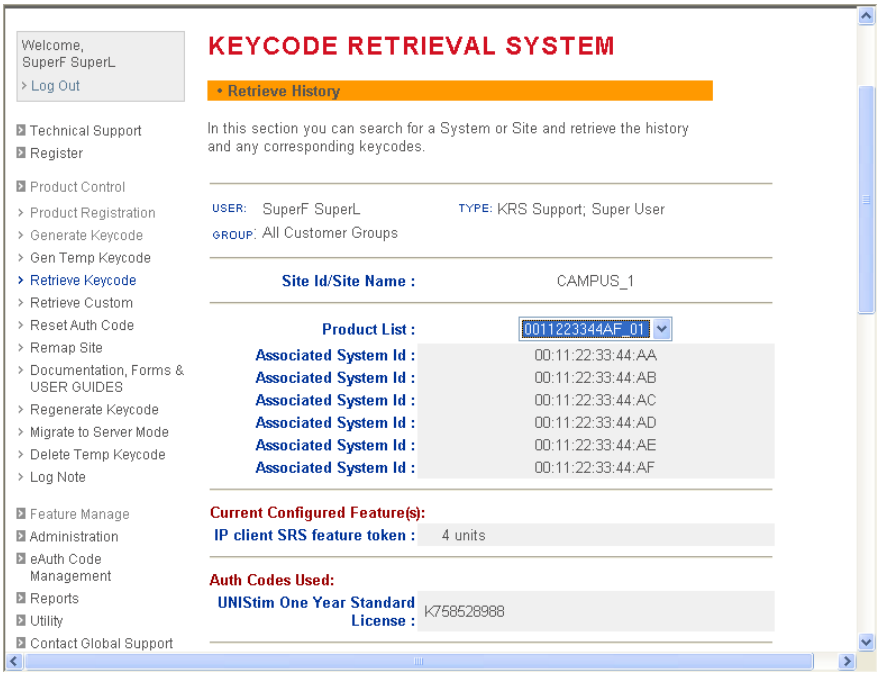
On the Retrieve History screen, as shown below, KRS will display keycode associated to each MAC address.

---

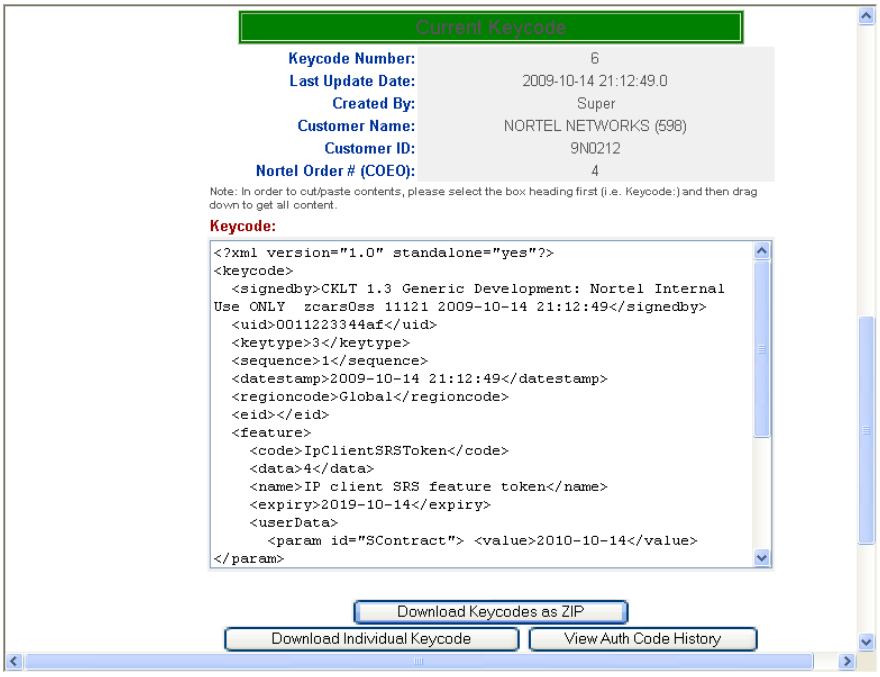
[15] KRS also supports wildcard searching. By entering the first few characters of a PO number all PO's with that string that are associated with your customer account will be returned.

[16] At the time of this writing, the only licensed feature in UNIStim software release 4.0 is the UVC so there will only be one line item

[17] Since it doesn't make sense to load multiple licenses for the same feature, the quantity selected should always be the same as the number of MAC addresses.



Note that each MAC address' keycode can be viewed by selecting the individual MAC from the Product List dropdown box. If selected a summary will be displayed as shown below, indicate Current Configured features, the line items or authcodes last used, creation date and the keycode itself.



At this point, the choice is to either download the individual keycode license, view the authcode specifics, or download all the keycodes as a single ZIP file.

To download the specific IP Clients keycode being displayed select Download Individual Keycode. But to download all the keycode at once select Download Keycodes as ZIP. Download and save the individual keycode file or the combined keycode ZIP file to the PC connected to KRS. This file must now be transferred to the IP Deskphone provisioning server to load the keycode onto the IP Deskphone.

Expanding a Site and Licensing Additional Phones

If the site is expanding and one needs to register additional MAC addresses one must create a new Site name within KRS to register the additional phones. It is recommended, however, to use the original site name but add a suffix to distinguish between the two registrations.

All the remaining steps as outlined above now still apply to the new registration.

References and Related Documents

Product Bulletin P-2009-0143-Global, UNIStim Software Release 4.0 for IP Phones.

IP Phones Fundamentals, NN43001-368

IP Phone 1165E User Guide, NN43101-102.

Clarify Bulletin 2010009988 Rev3, Minimum IP Phone Software Requirement for IP Phone 1150E

Clarify Bulletin 2009009363 Rev2, New Minimum Firmware Requirement for IP Phone 1120E and 1140E

Clarify Bulletin 2009009916 Rev1, New Product Codes for IP Phone 1120E and 1140E

Product Bulletin P-2006-0084-Global-Rev7, Headsets for Nortel IP Phones

IP Line Fundamentals, NN43100-500.

Main Office Configuration Guide for SRG200/400 Rls1.5, 553-3001-207

Main Office Configuration Guide for SRG50 Rls 2.0, 553-3001-207

CICM Administration and Security, NN10252-611.06.03

CRQM 7.0 Planning, Installation and Administration Guide, NN44480-300

Product Bulletin P-2006-0131-Global, SMC 2450

About Avaya

Avaya is a global leader in enterprise communications systems. The company provides unified communications, contact centers, and related services directly and through its channel partners to leading businesses and organizations around the world. Enterprises of all sizes depend on Avaya for state-of-the-art communications that improve efficiency, collaboration, customer service and competitiveness. For more information please visit www.avaya.com.

INTELLIGENT COMMUNICATIONS

02/10