NORTEL

Product Bulletin

Bulletin Number: P-2009-0143-Global
Date: 27 Nov 2009

UNIStim Software Release 4.0 for IP Phones, including:

- **0621C7A for IP Phone 2007,**
- **0623C7F, 0624C7F, 0625C7F and 0627C7F for IP Phone 1110, 1120E, 1140E and 1150E respectively and**
- **062AC7F for IP Phone 1210, 1220, and 1230**

REVISION HISTORY

Date	Revision #	Summary of Changes
27-Nov-09	Original bulletin	This is the original publication

Introduction

Nortel™ is pleased to announce the availability of UNIStim software release 4.0 for IP Phones. UNIStim software release 4.0 makes available the following software versions for the IP Phones[1].

IP Phone	Software
IP Phone 2007	0621C7A
IP Phone 1110	0623C7F
IP Phone 1120E	0624C7F
IP Phone 1140E	0625C7F
IP Phone 1150E	0627C7F
IP Phone 1210	062AC7F
IP Phone 1220	062AC7F
IP Phone 1230	062AC7F

Nortel recommends an upgrade to these releases of software for all applicable IP Phones and Call Servers at the earliest convenience. These releases are being provided as a no charge update to all customers, although some of the new functionality delivered in UNIStim software release 4.0 can only be activated with a purchased license.

[1] No UNIStim software release 4.0 is being offered for the Phase II IP Phone 2001, Phase II IP Phone 2002, and Phase II IP Phone 2004.

UNIStim software release 4.0 for IP Phones 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 Phones shipped from Nortel.**

UNIStim software release 4.0 for IP Phones delivers enhancements to Nortel's IP Telephony Solution and delivers general quality improvements. The enhancements available include:

- UNIStim VPN Client (UVC) in the IP Phone 1100 series
- Feature and Application Licensing
- Secure Signaling using DTLS
- Secure Call Recording (SCR)
- Designed for Operability (DfO)
- Enhancements to Certificate Support

Enhancements

1. UNIStim VPN Client (applies to the IP Phone 1120E, 1140E and 1150E)

UNIStim software release 4.0 introduces an integrated VPN Client inside the IP Phone 1100 series. The UNIStim VPN Client (UVC) is supported on all the IP Phone 1100 series phones except the IP Phone 1110. The UVC allows the IP Phone 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 VPN tunnel guarantees a secure connection between the remote IP Phone and the corporate network ensuring the integrity and confidentiality of enterprise communications. Once the VPN tunnel has been established all of the telephone related IP traffic traverses within the tunnel including signaling, media, duplicate media and application gateway traffic. Please be advised, however, that the IP traffic from the PC port of the telephone is **excluded** from the VPN tunnel.

The UVC within the phone is the client end of the tunnel. The corporate end of the tunnel is terminated by an enterprise VPN router or gateway. The UVC currently supports interoperability with the following VPN termination devices:

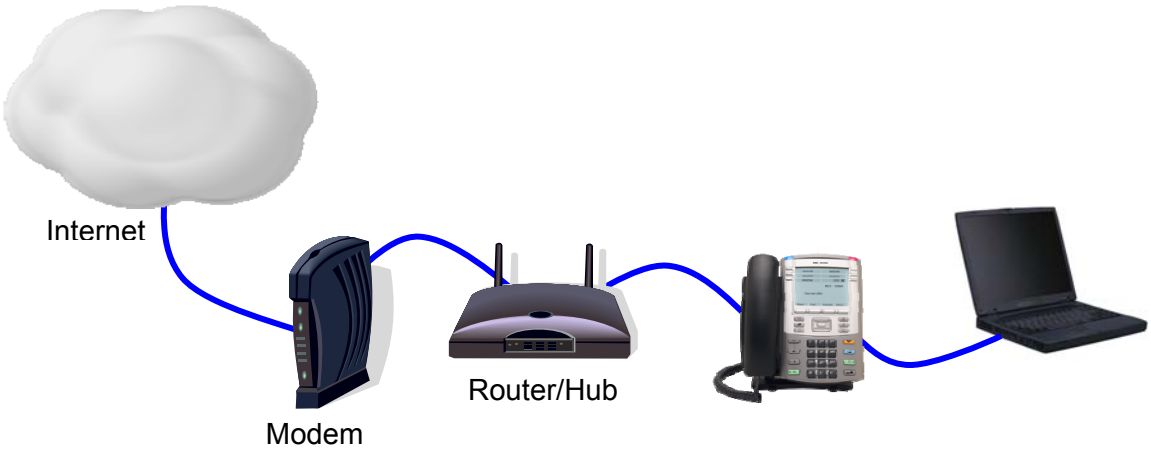
- Nortel VPN Router (NVR) family running software release 8.00 or greater. (NVR software release 8.00 has been qualified on the NVR 1010, 1050, 1100, 600, 1600, 17xx, 27x0, 4600 and 5000)

Installation

Typical home networks consist of one or more PCs connected either via wireless interfaces or Ethernet cables to a home router or hub which is then connected to the service provider termination equipment, typically a DSL or cable modem[2].

Adding the UVC phone to the home network is, in most cases, as simple as plugging in the Ethernet cable (provided with the phone) between the phone and an Ethernet connection on the router and/or DSL/cable modem. Since the phone does not have a wireless interface, the phone must be connected using an Ethernet cable – thus if the router or DSL/cable modem device is wireless, it must have at least one physical Ethernet connector for the UVC phone solution to work.

The following diagram depicts the typical connection scenario. Although the PC may be able to be plugged directly into the router or hub, Nortel recommends plugging the PC into the PC port on the phone. By plugging the PC into the PC port of the phone, the phone can better control the QoS of the voice during calls by prioritizing the telephone traffic over the PC traffic.



When the DSL/cable modem was installed, the number of devices that can operate on the network may have been restricted by either the service provider, the installer, or by the modems physical hardware. If this is the case, please refer to the modem's user guide or contact your service provider.

For additional information on installing the IP Phone in a home network, please refer to the *IP Phones Fundamentals* NTP NN43001-368 and the respective *IP Phone User Guide*.

[2] Some DSL/cable modems incorporate the router or hub, allowing the PC to be directly connected to the DSL/cable modem.

Authentication Modes:

The UVC within the IP phone currently supports three authentication modes:

1) Aggressive Mode with a PreShared Key and no X Authentication,
2) Aggressive Mode with a PreShared Key and with X Authentication, and
3) Main Mode using X.509 Certificates and no X Authentication.

The table below lists the security credentials required for each mode:

Mode	**Security Credentials Required**
Aggressive Mode with a PreShared Key and no X Authentication	User ID and Password
Aggressive Mode with a PreShared Key and with X Authentication	User ID, Password, XAuthentication User ID and XAuthentication Password
Main Mode using X.509 Certificates and no X Authentication	CA root certificate and device certificate

The authentication mode established by the corporate security policy will determine which parameters must be provisioned. The table below lists the various parameters that must be provisioned for valid VPN configurations[3].

[3] <user ID> and <user password> correspond to the GroupId and Password respectively configured on the Nortel VPN Router. <Xauth user ID> and <Xauth password> correspond to the credentials configured on the RADIUS server.

VPN Parameter	Aggressive Mode with a PreShared Key and no X Authentication	Aggressive Mode with a PreShared Key and with X Authentication	Main Mode using X.509 Certificates and no X Authentication
VPN type	Nortel	Nortel	Nortel
VPN mode	Aggressive	Aggressive	Main
VPN authentication type	PSK	PSK	Certificate
PSK user ID	<user ID>	<user ID>	n/a
PSK password	<user password>	<user password>	n/a
X authentication	none	Password	none
X authentication user ID	n/a	<Xauth user ID>	n/a
X authentication password	n/a	<Xauth password >	n/a
VPN Server 1	IP address or FQDN	IP address or FQDN	IP address or FQDN
VPN Server 2	optional	optional	optional
CA root certificate	n/a	n/a	Required
Device certificate	n/a	n/a	Required

Provisioning

Provisioning the UVC presents some unique challenges for remote deployments since the corporate provisioning server for auto-provisioning cannot be accessed by the remote phone until after the VPN is fully configured. There are three options for provisioning a phone for a remote VPN deployment:

1. Pre-provision the phone using auto-provisioning within the corporate network prior to deploying remotely,
2. Provision the phone remotely using the new Nortel Phone VPN Configuration Wizard PC Application, or
3. Manually Provision the phone using the phone's Network Configuration menu.

To auto-provision the UVC in the IP phone, new Info Block parameters have been introduced with UNIStim software release 4.0. The new parameters to allow the UVC to be auto-provisioned are provided in the table below. Please refer to Appendix B for the complete list of parameters supported within the Info Block.

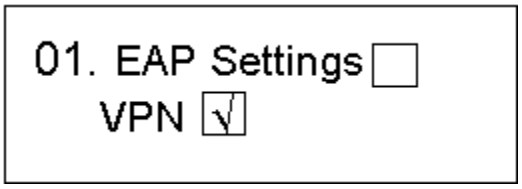
vpn	'y' enable 'n' disable	Enable the UNIStim VPN Client (UVC) within the phone
vpntype	'1' Nortel VPN	Only Nortel VPN devices are supported at this time
vpnmode	'aggressive' 'main'	Authentication mode
vpnauth	'psk' preshared key 'certificate' X.509 certificate	Authentication credential[4]
vpnxauth	'0' 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[5] 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	Security Banner timer (after initial acceptance) 0 = auto acknowledge and do not display the security banner 1 to 998 = display the banner for nnn seconds then auto acknowledge 999 = always display the banner until the user manually acknowledges

[4] 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.

[5] 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.

Since the UVC can be auto-provisioned, a change to the auto-provisioning menu has occurred within group #1. A “VPN” checkbox has been added. For the VPN feature, one is not allowed to manually override individual VPN parameters. There is only one checkbox for the entire feature set. Either the entire set of VPN parameters is auto-provisioned, or the entire set of VPN parameters is manually provisioned.

The new VPN auto-provisioning menu check box is as follows:



For detail on the changes to the Network Configuration menu to allow manual provisioning of the VPN parameters, please refer to Appendix G: IP Phone Configuration Menu on the IP Phone 1120E, IP Phone 1140E and IP Phone 1150E.

Nortel Phone VPN Configuration Wizard

Since a remotely deployed phone must have an active VPN service to connect to the corporate network, and since auto-provisioning of the IP phone’s VPN service requires a corporate connection, such a situation presents a dilemma. To allow the IP Phone to be provisioned at the remote site a PC application called the Nortel Phone VPN Configuration Wizard is being made available. The Phone VPN Configuration Wizard can run on either Microsoft Windows XP or Vista and on Mac OS. The Phone VPN Configuration Wizard 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 for the IP Phone 1100 series models under “Phones, Clients and Accessories”.

The Phone VPN Configuration Wizard uses the same configuration and provisioning files used to auto-provision a phone on the corporate network. These required configuration and provisioning files need to be loaded onto the PC at the remote location along with the Phone VPN Configuration Wizard.

The Phone VPN Configuration Wizard greatly simplifies the provisioning of the UVC on the IP Phone. For phones with UNIStim software release 4.0 already installed, to provision the UVC (and the entire phone for that matter) a user need only:

- Start the Nortel Phone VPN Configuration Wizard
- Select a zip file containing configuration and provisioning files (this file should have been sent to the user by their system administrator)

- Press a short key sequence on the phone
- Click a button on the Phone VPN Configuration Wizard to start configuration
- Wait for configuration to complete.

If the phone does not have UNIStim software release 4.0 already installed, the Phone VPN Configuration Wizard can also act as a file server allowing this application to update the phone's software.

The Phone VPN Configuration Wizard guides the user step-by-step through the provisioning process, but a summary on using of the Wizard is included in Appendix L: Phone VPN Configuration Wizard. For complete details on using the Phone VPN Configuration Wizard please refer to the respective *IP Phone User Guide*.

Tunnel Establishment

Once the IP Phone has been provisioned (either centrally or remotely), the phone is ready to be deployed and establish a VPN tunnel back to the corporation. If the UVC is enabled, when the phone boots, the VPN tunnel establishment is indicated to the user by the message:

```
Start VPN <server name>
```

where <server name> is either the provisioned IP address or the Fully Qualified Domain Name (FQDN) of the corporate VPN server. If the server name is specified as a FQDN the phone must first resolve the IP address of the VPN server by performing a DNS lookup[6].

The phone must also check to ensure all required user security credentials are loaded into the phone. If any of the credentials are missing the user is prompted to enter them.

If the VPN server's IP address is known and all required credentials are available in the phone the VPN tunnel setup process is initiated between the IP Phone and the corporate VPN server. Once the tunnel is established the following message is displayed on the phone's screen:

```
VPN Tunnel Established
```

The credentials required to establish the VPN tunnel is dependant on the authentication method chosen for the tunnel establishment.

The table below lists the security credentials required for each mode:

[6] To perform a DNS lookup, the DNS address must have already been provisioned into the phone or obtained from DHCP.

Mode	Security Credentials Required
Aggressive Mode with a PreShared Key and no X Authentication	User ID and Password
Aggressive Mode with a PreShared Key and with X Authentication	User ID, Password, XAuthentication User ID, and XAuthentication Password
Main Mode using X.509 Certificates and no X Authentication	CA root certificate and device certificate

If the authentication method chosen in the UVC is Aggressive Mode with a PreShared Key and no X Authentication only a User ID and Password are required. If Aggressive Mode with a PreShared Key and with X Authentication is chosen then in addition to the User ID and Password the XAuthentication User ID and XAuthentication Password are also required[7].

All the user IDs and passwords can be provisioned into the phone either manually or by auto-provisioning. If the user IDs and passwords are provisioned into the phone, the end user will not be prompted to enter the credentials. But if the user IDs and passwords required by the chosen authentication method are not provisioned into the phone the user is prompted to enter them prior to the establishment of the tunnel.

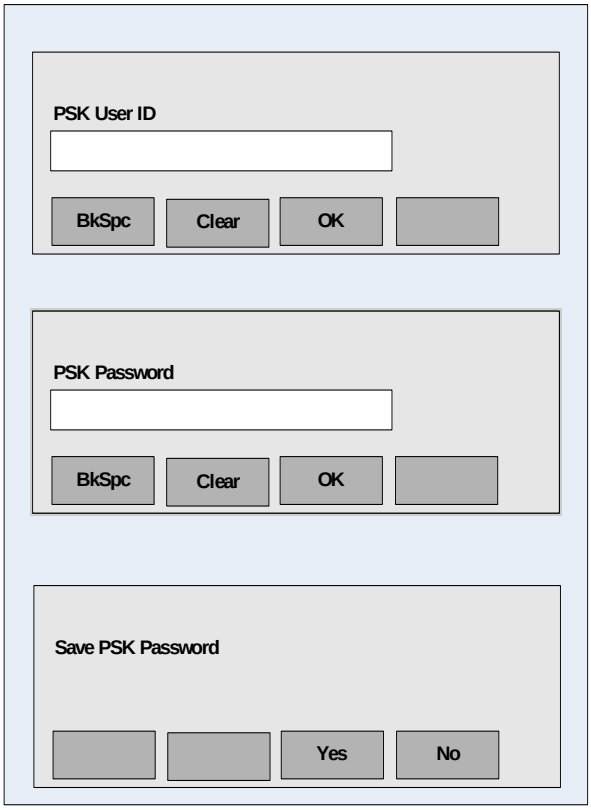
If the user IDs and passwords are entered by the end user, the user is also presented with the dialog box allowing the credentials to be stored permanently[8]

The diagram below shows the phone's screen prompts for entering the PSK User ID, PSK Password, and the request to save the password[9].

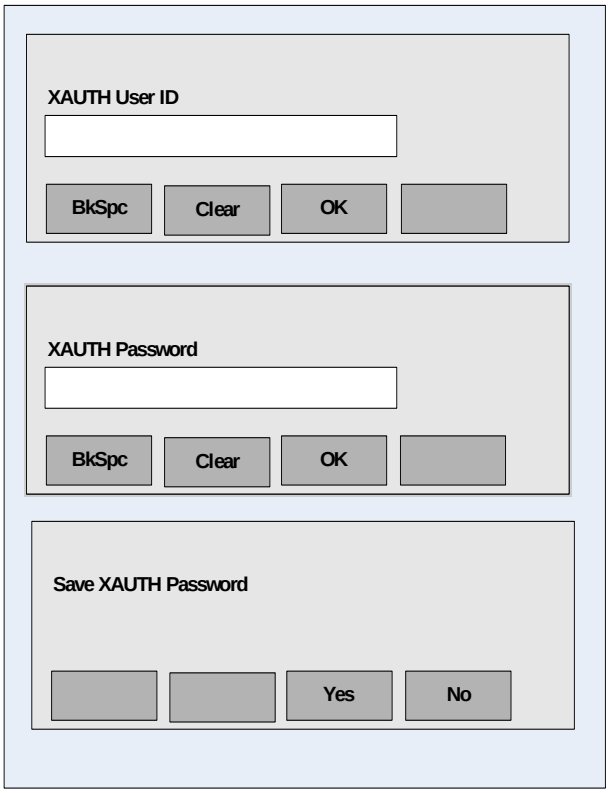
[7] User ID and Password correspond to the GroupId and Password respectively configured on the Nortel VPN Router. XAuthentication User ID and XAuthentication Password correspond to the credentials configured on the RADIUS server.

[8] The Nortel VPN Router can be configured with an option to disallow saving of the user passwords on the UVC. This option on the Nortel VPN Router takes precedence over provisioned passwords in the phone and over a user request to permanently save their password. If this disallow option is configured on the Nortel VPN Router, passwords are removed from the phone's storage and the user must re-enter credentials if the phone reboots for any reason.

[9] If Aggressive Mode with a PreShared Key and with X Authentication is configured, the user is not prompted to store the PSK password – it will automatically be stored.


PSK User ID
BkSpc
Clear
OK
PSK Password
BkSpc
Clear
OK
Save PSK Password
Yes
No

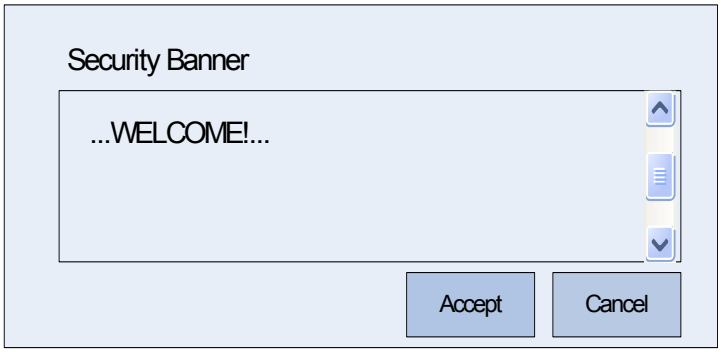
The diagram below shows the phone's screen prompts for entering the XAuthentication User ID, XAuthentication Password, and the request to save the password.



If tunnel establishment fails due to an invalid user ID or Password the user is re-prompted to enter the credentials again.

The first time a tunnel is established with the corporate VPN Router and if the Security banner text is configured in the Nortel VPN Router Profile the phone will display the VPN Security Banner. The user has to accept the security information or the tunnel will not be established and the user will be re-prompted to accept it. Once accepted, the banner will not be re-displayed again even if the phone reboots.

The diagram below shows the Security Banner acceptance window.



If the authentication method chosen in the UVC is Main Mode using X.509 Certificates and no XAuthentication then both a CA root certificate and a device certificate must be installed on the phone. For details on installing both a CA root certificate and a device certificate into the IP Phone please refer to Appendix A: Certificate Installation.

IP Clients UNIStim VPN Client License

The operation of the UVC depends on the availability of a license. If a license is available then the UVC operates in an Unrestricted mode. If no license is available, the UVC operates in a restricted mode where it can still establish a VPN tunnel to the corporate network, but the telephony traffic will be blocked from traversing the tunnel. Restricted mode allows the phone to connect to the corporate network to obtain configuration and provisioning information from the corporate network (including licensing information), but will prevent all voice services from operating.

UNIStim 4.0 software provides the capability to evaluate a licensed feature, including the UVC, without committing to an initial license purchase. The UVC can be activated for a period of 60 days license free. But once the 60 day evaluation period has passed, the UVC will require a license to allow its continued operation. The 60 day evaluation period is initiated the first time the UVC is enabled. Once the UVC is enabled the 60 day time will continue to count-down even if the UVC is subsequently disabled. In other words, the 60 day evaluation period is a “one-time” opportunity.

For details on licensing please refer to the Application and Feature Licensing section later in this document.

Diagnostics

With the introduction of the VPN service in UNIStim software release 4.0 the phone's local diagnostics capabilities has been revamped. Some menu items have been expanded and a complete new menu item has been added. The below diagram shows which menu items have been expanded and which menu item is new:

1. IP Set Information (expanded)

2. Network Diagnostic Tools (changed behavior)

3. Ethernet Statistics

4. IP Network Statistics (expanded)

5. USB Devices

6. Advanced Diag Tools

7. License Information

8. VPN Statistics (new)

9. Certificate Information

10. DHCP Information

Within the IP Set Information menu, if VPN is enabled, four new parameters are now available to show the "inner"[10] IP Address and associated information. The four new parameters are: VPN IP Address, VPN Mask, VPN Gateway IP, and VPN Server URL. If the VPN status is anything other than "Operational" these new items are not shown.

Within the Network Diagnostics Tools menu, if VPN is enabled, the behavior of Ping and TraceRoute are modified. When the VPN is Operational the Ping and TraceRoute utilities operate inside the tunnel[11]. When VPN is disabled, or failed, and no tunnel is available the Ping and TraceRoute operate consistent with previous operation using the "external" address outside the tunnel.

Within the IP Network Statistics menu, if VPN is enabled, five new statistics are available. The new statistics monitor the packets sent and received on the VPN virtual interface. When the VPN status is neither "Operational" nor "Connecting", the new statistics are not shown.

[10] During tunnel setup negotiation, the VPN router assigns an IP address to the client. This "virtual" or "inner" address represents the client on the Corporate network.

[11] Ping and TraceRoute will still be sent via the physical interface, even if the VPN is enabled, if the source address is the phone's inner IP Address, and the destination address is either the local subnet, or subnet of the VPN gateway.

The new menu, VPN Statistics, provides information on the operational status of the VPN, presents some key VPN parameters, and list statistical counters for the VPN service. If the VPN feature is not enabled this menu item is greyed out. The below diagram provides an example of the VPN Statistics screen.

VPN Feature Advisements

1. When using Main Mode using X.509 Certificates and no X Authentication:
   - The CA root certificate must be the CA certificate which issued the VPN Router certificate.
   - The device certificate's key usage must include DigitalSignature
   - The device certificate's Extended Key Usage (EKU) must either not be present or contain the value "anyExtendedKeyUsage"
   - For Nortel VPN Router compatibility, if a Subject Alternate Name is present, it should not include a FQDN or USER_FQDN. An IP address is permitted
   - The VPN Router certificate is subject to the same Key Usage and Extended Key Usage as the phone's device certificate.

- The VPN router's public IP address must appear in the VPN Router certificate's Subject Common Name (CN) or the Subject Alternate Name
- The phone will always send an ID Payload of type IPV4 ADDRESS containing the local IP address configured on the phone.
- The phone requires that the VPN Server configuration on the phone match the received ID Payload
- If the active VPN Server is configured as an IP address, then the ID Payload must provide the same IP address
- If the active VPN Server is configured as an FQDN, then the ID Payload must provide an exact match to the configured FQDN.

2. The IP Phone is capable of supporting multiple certificates. However as a security precaution all certificates installed into the phone subsequent to the initial certificate, must be signed and authenticated by the initial certificate. Therefore if a certificate is already installed in the phone for EAP-TLS and you wish to enable VPN Main Mode using X.509 Certificates and no X Authentication you will need to remove the existing certificate[12], install a new CA root certificate and then sign and reinstall the EAP-TLS certificate.

3. A license is required to allow the UNIStim VPN Client (UVC) in the UNIStim-based IP Phone 1100 series to operate in unrestricted mode. Without a valid license, the UVC will operate in restricted mode and not allowed any telephony operations to occur within the tunnel. In addition, without a valid license a recurring warning message will appear on the phone's screen. To allow unrestricted mode where telephony operations can occur within the tunnel a valid license is required. Please refer to the Application and Feature Licensing section for details on IP Clients licensing.

4. A VPN tunnel between the IP Phone and the corporate network is terminated at the corporate network end by enterprise VPN equipment. Separate provisioning and/or licenses may be required on the enterprise VPN equipment to allow the UVC connection.

[12] The existing EAP-TLS certificate can be removed by restoring the phone to factory default as explained in Appendix K: Restore to Factory Defaults

2. ***Application and Feature Licensing (applies to the IP Phone 1110, 1120E, 1140E, and 1150E)***

UNIStim software release 4.0 introduces application and feature licensing to control the activation of specific applications and features in the UNIStim software. **Application and feature licensing introduced with UNIStim release 4.0 is in addition to, and does not replace, any licensing which may be required to enable IP Phone service on the associated Call Server (e.g. ISM on the Communication Server 1000)**

All telephony functionality, including all features already delivered up to and including UNIStim release 3.0 will not be licensed. Of the new features in UNIStim software release 4.0 the following licensing rules will apply:

- UNIStim VPN Client (UVC) in the IP Phone 1100 series – licensed feature.
- Secure Signaling using DTLS – not licensed by UNIStim software. Included in the UNIStim software as a no charge update.
- Secure Call Recording – licensed feature. But, if the call recorder is the Nortel Contact Recording and Quality Monitoring (CRQM) product the license requirement in the UNIStim software is removed[13]. A UNIStim software license will be required however, if secure call recording is enabled with a 3rd party call recorder[14].
- Designed for Operability (DfO) – not licensed. Included in the UNIStim software to assist support personnel.
- Enhancements to Certificate Support – not licensed. Included in the UNIStim software as a no charge update.

At the time of this writing, Secure Call Recording in UNIStim software release 4.0 is only supported with the Nortel Contact Recording and Quality Monitoring (CRQM) product. Since there is no Secure Call Recording support with any 3rd party call recorder, there is no Secure Call Recording license offered at this time. Therefore, the only license available within UNIStim software release 4.0 is the "IP Clients UNIStim VPN Client" license.

The IP Clients UNIStim VPN Client is a license that is required to activate a UNIStim VPN Client (UVC) in the UNIStim-based IP Phone 1100 series as described in the UNIStim VPN Client section earlier in this document.

The IP Clients UNIStim VPN Client license includes a one year warranty period for access to software updates. Software updates delivered within the one year warranty period will be made available as a no charge update. Software updates delivered beyond the one year warranty period will require that the IP Clients UNIStim VPN Client license be refreshed for an additional year (by ordering IP Clients UNIStim VPN Client Refresh).

[13] Licensing may apply on the CRQM

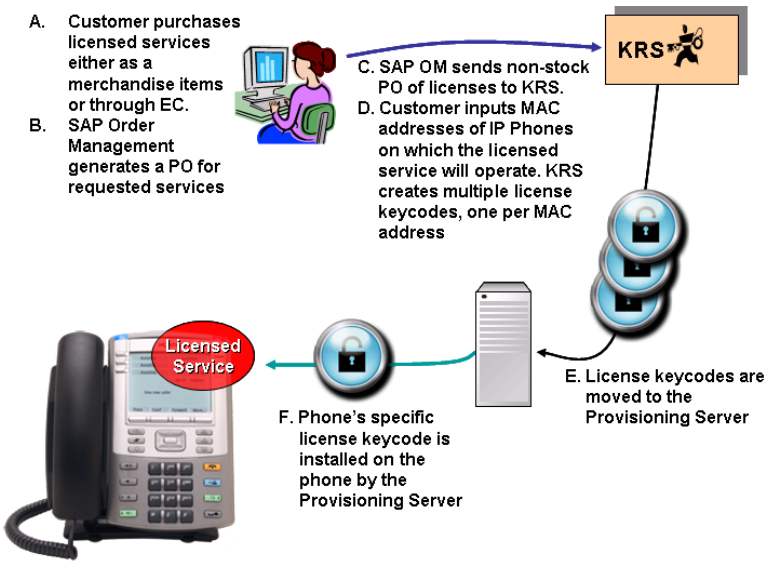
[14] At publication time Secure Call Recording is only supported with the Nortel Contact Recording and Quality Monitoring (CRQM) product. As such, at this time, there is no Secure Call Recording license for IP Clients since there is no Secure Call Recording support with any 3rd party call recorders.

Ordering

The IP Clients UNIStim VPN Client licenses can be ordered as a merchandise item. At the time of this writing the Enterprise Configurator has not been updated to allow the IP Clients UNIStim VPN Client license to be included with new system installs. Unfortunately, the IP Clients UNIStim VPN Client licenses must be ordered as a merchandise item for new installs until such time as the Enterprise Configurator is updated. The PEC for the IP Clients UNIStim VPN Client is:

PEC	CPC	Description
NTYS01EAE6	N0214767	IP Clients UNIStim VPN Client (includes one year warranty period for access to software updates)

The purchase order for IP Clients UNIStim VPN Client licenses contains the eAuth code to allow the generation of the actual license. The license is created in Nortel's Keycode Retrieval System (KRS). The below diagram depicts the ordering process for one or more IP Clients UNIStim VPN Client licenses.



License Generation

As mentioned above, Nortel KRS is used to generate the license keycodes. An overview of the KRS system is as follows:

- Customer logs into KRS and initially registers their system.
- Customer selects "Generate Keycode".
- Customer selects licenses/features from Purchase Order (PO) and generates keycode.

- KRS generates the license keycode and saves the result to its database. The license keycode is also displays to the customer
- Customer downloads the license keycode and applies the keycode to the IP Phone.

Nortel KRS is located on the Nortel website under Support and Training → Online Self-Service → Keycode Retrieval

http://www.nortel.com/support/tools/krs/index.html

A summary of using KRS to generate a keycode for an IP Clients UNIStim VPN Client license is included in Appendix M: Nortel Keycode Retrieval System (KRS).

For more details on using KRS for IP Clients licensing, please refer to the *IP Clients Keycode Retrieval System (KRS) User Guide*. A copy of the *IP Clients Keycode Retrieval System (KRS) User Guide*, can be retrieved from the KRS system. After selecting "IP Clients" from the PRODUCT FAMILY list, log into KRS using with your user ID and password. Once logged in, select the Documentation Forms & User Guides link from the sidebar on the left.

Loading Licensing Files onto the IP Phones

The license keycode file is distributed to an IP Phone using the same procedure as the other provisioning files. To support the loading of license keycodes onto the IP Phone a new section called [LICENSING] must be added to the phone's configuration file (i.e. 1120e.cfg, 1140e.cfg, 1150e.cfg). An individual keycode license file name is ipctokenMAC.cfg where MAC is the phone's 12 characters MAC address to which the license is associated.

The [LICENSING] section has three command lines:

- DOWNLOAD_MODE (required command) - The DOWNLOAD_MODE can only be AUTO at this time. When AUTO is used, the application looks at the VERSION and downloads the license files only if they are a newer version than what is currently stored on the phone. Support for FORCED (where the VERSION command is ignored and the licenses files are always downloaded) is currently not available (see *Advisement* below).
- VERSION (optional command) - if this command is not present, version 0 is assumed). The VERSION command specifies the version of the licenses being downloaded. The version applies to all files listed in the [LICENSING] section. When licenses are written to the phone's memory, the value for the configuration 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 keycode file to be downloaded. Recall that the individual keycode license file name is ipctokenMAC.cfg where MAC is the phone's 12 characters MAC address to which the license is associated. The FILENAME command can either reference a specific keycode 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 unique keycode file. Files can either be in the same folder as the configuration file or in a sub-folder. If they are in a subdirectory, the path needs to be pre-pended to each filename.

Below is an example of a LICENSING section in an 1140e.cfg file. Note that in this example the keycode licensing files are in a subdirectory named "\UNIStim\LICENSING\":

```
[LICENSING]
DOWNLOAD_MODE AUTO
VERSION 000001
FILENAME \UNIStim\LICENSING\ipctoken*.cfg
```

Once the license file is installed on the IP Phone once, it does not need to be downloaded again. A new license file should only need to be downloaded to update the warranty period.

Advisement

At the time of writing, an issue was discovered with the DOWNLOAD_MODE command in the [LICENSING] section. Unfortunately, only the AUTO option can be used at this time. Support for the FORCED option in DOWNLOAD_MODE is being fixed and will be delivered in a maintenance build of UNIStim software.

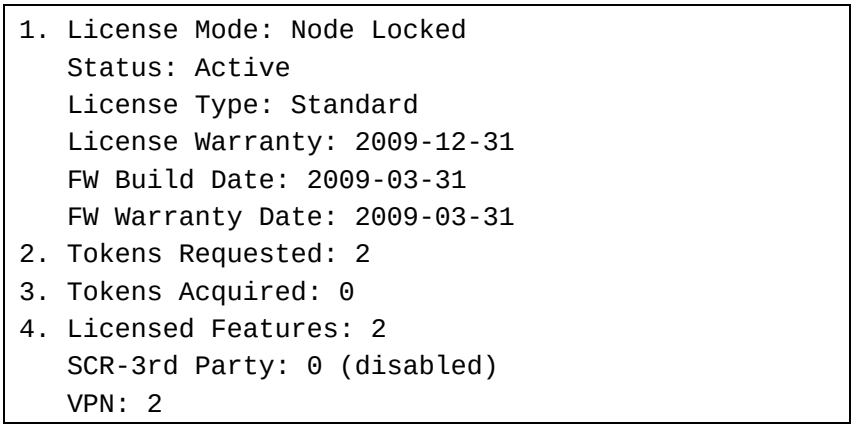
Warranty

The IP Clients UNIStim VPN Client license includes a one year warranty period for access to software updates. Software updates delivered within the one year warranty period will be made available as a no charge update. Software updates delivered beyond the one year warranty period will require that the IP Clients UNIStim VPN Client license be refreshed for an additional year (by ordering IP Clients UNIStim VPN Client Refresh) for the UVC to continue to operate on the new software.

Diagnostics

With the introduction of licensing in UNIStim software release 4.0 a complete new menu item has been added to the phone's local diagnostics capabilities. The below diagram shows the new menu item.

The new Licensing Information menu screen, as shown below, provides information on the status of the phone's license, the features that are licensed, the number of tokens (the licensing currency) that the license contains, and number of tokens being used.



The Status field is used to convey information about the license. The following statuses are available:

- Active – license is valid, or feature is within the evaluation period
- Released – a licensed feature has been de-commissioned and the license has been released
- Invalid License File – licensing file is invalid
- No License File – no license file has been loaded onto the phone
- No Token Needed – all licensed features have been de-commissioned

Alarms

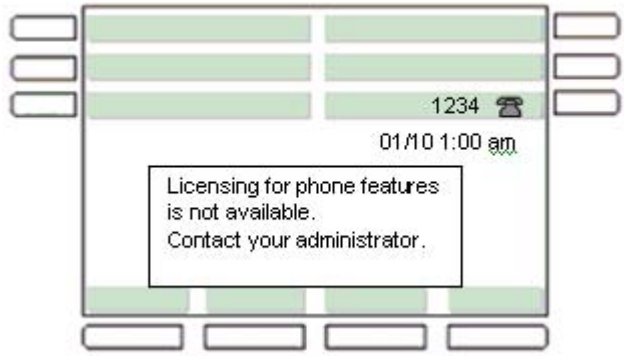
The license feature provides notification messages on the phone's display if there is no license available to enable features, or the license has expired, or the evaluation period has ended. These notifications messages allow the administrator to diagnose why a licensed feature is not working on the phone.

License notification messages will be displayed in a pop up window on top of the phone's telephony screen. The notification messages can be dismissed by pressing the stop key or by lifting the handset. Once a notification message is dismissed the phone will close the pop-up window. The notification messages will be displayed ever 24 hours at 1:00 am until the licensing offense is fixed or removed.

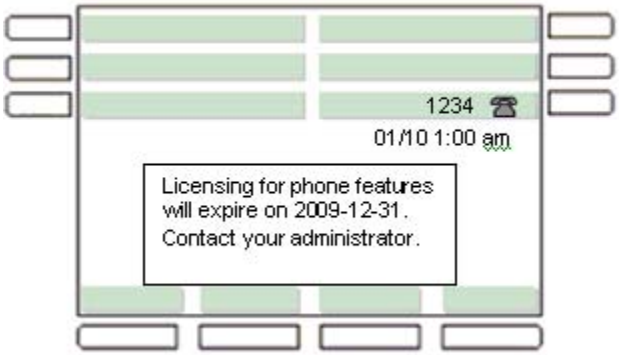
If no licensed feature is enabled, the phone will not display any of the license notifications messages described in this section.

The following diagrams depict the various license notification messages that can be displayed on the phone.

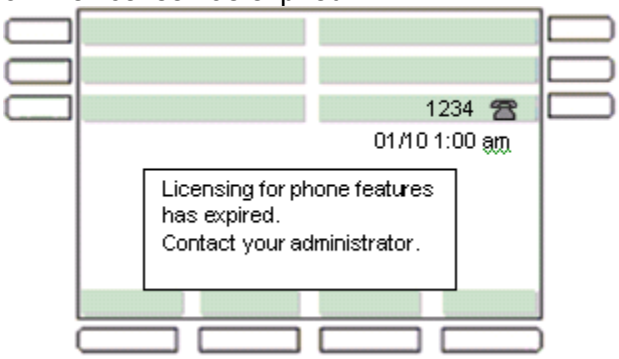
1. No license is available for the licensed feature:



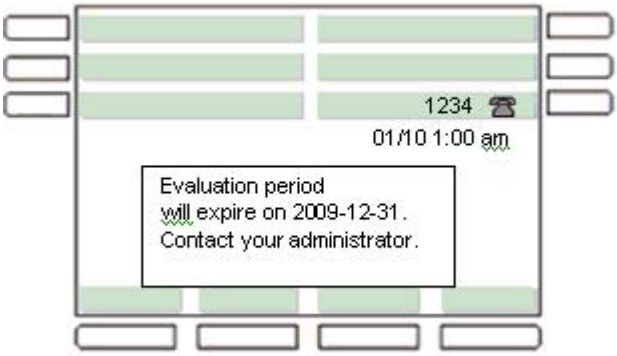
2. License is about to expire:



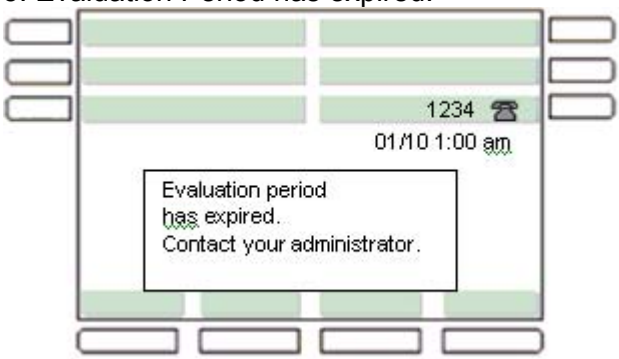
3. The license has expired:



4. Evaluation Period is about to expire:



5. Evaluation Period has expired:



Evaluation Period

UNIStim 4.0 software provides the capability to evaluate a licensed feature without committing to an initial license purchase. Every licensed feature can be enabled for a period of 60 days license free. But once the 60 day evaluation period has passed, the feature will require a license to allow its continued operation. The 60 day evaluation period is initiated the first time a licensed feature is enabled. Once the licensed feature is enabled the 60 day time will continue to count-down even if the feature is subsequently disabled. In other words, the 60 day evaluation period is a “one-time” opportunity. In addition, if a valid license is installed on the phone prior to the end of the 60 day evaluation period the evaluation period ends.

3. ***Secure Signaling using DTLS (applies to the IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230)***

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

The only Nortel call platform currently committed on supporting DTLS is the Communication Server 1000.

Support for DTLS was introduced with Communication Server 1000 Release 6.0. But at the time of this writing an issue has recently surfaced with the secure signaling using DTLS feature delivered 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 Phone and the Communication Server 1000, one has to deploy the Secure Multimedia Controller (SMC) 2450.

4. ***Secure Call Recording (applies to the IP Phone 1110, 1120E, 1140E and 1150E)***

Prior to UNIStim software release 4.0, for the IP phones that support dual audio stream (where the second audio stream is sent to a call recorder), the duplicate audio stream was sent unencrypted to a call recorder. Since the audio stream to the call recorder was not encrypted, the audio stream could potentially be captured and be reconstructed by a third party. This vulnerability compromised the confidentially and integrity of the communication.

UNIStim software release 4.0 now delivers the capability to encrypt the communication between the IP phone and the call recorder. The DTLS with SRTP extensions protocol is used to establish the secure connection from the IP phone to the call recorder and to exchange SRTP keys. Once the connection is established and the keys exchanged, the SRTP protocol is used for the actual media encryption and authentication.

Support for Secure Call Recording (SCR), is a joint effort between the IP Phone and the Nortel Contact Recording and Quality Monitoring (CRQM) solution. The IP Phone's UNIStim software must be at release 4.0 or greater, the Communication Server 1000 must be at release 6.0 or greater, and the Nortel CRQM must be on release 7.0 or greater.

The model used to secure the media stream sent to the call recorder is called "mirror mode". In this mode, the decision on whether or not to encrypt the secondary media stream being

sent to the call recorder is based on the secure state of the primary media stream. If the primary media stream (between the two calling parties) is encrypted, so too will be the media stream sent to the call recorder. If the primary media stream is not encrypted, the media stream sent to the call recorder will also not be encrypted.

The ability to encrypt the media stream sent to the call recorder, independent of the encryption status of the primary media stream, is not available.

To auto-provision SCR, two new parameters have been added to the provisioning Info-Block. The two new Info-Block parameters that have been created to allow the SCR to be auto-provisioned are provided in the table below. Please refer to Appendix B for the complete list of parameters supported within the Info-Block.

mscr	'n' do not encrypt the stream to the call recorder 'y' encrypt the audio stream to the call recorder based on the encryption status of the primary stream	Mirror mode encryption settings If the call recorder does not support SCR and the primary media stream is encrypted, mscr must be set to 'n'
callrec	'n' Nortel (default)	Only Nortel Call recording is supported at this time

SCR cannot be manually provisioned. As such, there are no additions to the IP Phone's Network Configuration menu, nor any changes to the auto-provisioning menu to support manual provisioning of SCR.

SCR requires that the IP Phone and the call recorder share security credentials to establish a secure connection. The Nortel call recorder ships with a Nortel certificate installed allowing "out of the box" secure connections with the Nortel CRQM solution. However, if the customer wishes to use their corporate Certificate Authority (CA) then a customer root certificate must be installed on the phone. Please refer to Appendix A: Certificate Installation for details on installing certificates into the phone.

For additional information on Nortel CRQM solution and its support for Secure Call Recording, please refer to the *CRQM 7.0 Planning, Installation and Administration Guide* NN44480-300 found on the Nortel technical documentation website at http://support.nortel.com

5. ***Designed for Operability (applies to the IP Phone 1110, 1120E, 1140E and 1150E)***

The UNIStim software release 4.0 introduces Design for Operability (DfO) capabilities to assist support personnel with IP Phone diagnostic. The enhanced diagnostic capabilities include:

- Flight Recorder
- Overload Protection
- Task Monitor
- Common Alarming
- Common Logging
- Traffic Monitor

Flight Recorder:

The Flight Recorder captures base system performance on a regular interval, including register usage and buffer usage.

Overload Protection:

Overload Protection consists of monitoring several key components of the IP Phone including:

- CPU usage is monitored for normal, warning and critical threshold levels
- Memory is monitored for normal, warning and critical threshold levels
- Flash File System is monitored for normal, warning and critical storage threshold levels
- Stack usage is monitored for normal, warning and critical threshold levels
- Message queues are monitored for normal, warning and critical threshold levels[15]

Task Monitor:

Task Monitor checks the status of a set of essential tasks running on the IP Phone. If any of these essential tasks are suspended or deleted for any reason the event is logged as Critical

Auto Recovery

Overload protection and task monitoring take advantage of the Auto Recovery feature already built into the IP Phone software. Recall that Auto Recovery was delivered in UNIStim software release 3.0 as part of the Enhanced Diagnostics capabilities. Auto Recovery allows the phone to auto reboot should it encounter a critical event. If Auto

[15] Message queues are used for message sending and receiving between critical tasks. If the receiving task is not fast enough to receive all messages at one time, the extra messages will be held in a message queue waiting to be received. If the number of messages sent is greater than the length of the queue, overflow happens, and some messages will be lost.

Recovery is enabled and the overload protection reaches a critical threshold or if the task monitor finds a suspended or deleted task, the phone will automatically reboot.

Auto recovery is enabled by default. If support staff wishes to disable Auto recovery, perhaps to analyze an unexpected occurrence of a critical event, then Auto recovery can be disabled either through the Advanced Diagnostics Tool Menu under Local Diagnostics menu or can be disabled via auto-provisioning.

Common Alarming:

Common Alarming sends UNIStim message to the call server when overload protection detects a state change. Whenever an IP phone changes states from Normal to Warning and from Warning to Critical, the IP Phone send a General Information UNIStim message to the call sever. Whenever an IP phone changes state form Critical to Warning or from Warning to Normal, the IP phone send a General Information UNIStim message to clear the alarm.

Common Logging:

Common Logging provides the ability to log information into the phone's flash file system. By logging all error and info messages into the flash file system it provides a persistent storage of messages allowing the IP Phone to be checked after an event has occurred to determine if a problem exists. The log file is 64KB circular buffer. Five severity levels for logging are defined. The five severity levels are:

- Critical
- Major
- Minor
- Warning
- Info

A separate Security log has also been defined. It is used for logging security related events only.

Traffic Monitor:

The Traffic Monitor checks the IP traffic inbound packet rate. The IP phone has a DoS filter to protect the phone from Denial of Service (DoS) attacks. High threshold, low threshold, and holdoff times have been setup for unicast, multicast, and broadcast packets. The DoS checking function will check the rate of the received packets. If the high threshold is reached, the Ethernet driver will turn off packet reception for the holdoff time. After the holdoff time, if the rate of the traffic is lower than the low threshold, the Ethernet driver will re-enable packet reception.

6. ***Enhancements to Certificate Support (applies to the IP Phone 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230)***

UNIStim software release 4.0 for IP Phones introduces enhancements to the existing certificate support in the phones as well as introduces a new method for installing and managing device certificates on the phone.

SCEP Enhancements:

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

With UNIStim software release 4.0 the phone's support for SCEP has been 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

PKCS#12:

New with UNIStim software release 4.0 for IP Phones is the support for PKCS#12 device certificates. 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[16]. 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.

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

The PKCS#12 certificate is downloaded to the IP Phone via the IP Phone'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.

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)[17].

[17] Please note that since negative one means that the device certificate can be used by all applications, it cannot be combined with other 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 phone'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
```

Device Certificate Profiles (DCP):

Also new with UNIStim software release 4.0 for IP Phones is the support for Device Certificate Profiles (DCP). 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:

Model	Number of supported DCP
IP Phone 2007	3
IP Phone 1100 series (except the IP Phone 1110)	6
IP Phone 1110	5
IP Phone 1200 series	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 maximum 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.

dcpsource1	'scep' 'pkcs12'	Method used to install device certificates
dcpactive1	'n' Inactive 'y' Active	Profile is active or not
dcppurpose1[18]	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

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.

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

[18] 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

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 IP Phone 1100 series (except the IP Phone 1110), an additional 4 times for the IP Phone 1110 and the IP Phone 1200 series, and an additional 2 times for the IP Phone 2007. 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;
```

Diagnostics

UNIStim software release 4.0 introduces a new diagnostic screen to view the X.509 certificates installed in the phone as well as view the phone's certificate revocation list. The new Certificate Information menu choice is depicted in the diagram below.

Under the new Certificate Information menu three choices are presented: Trusted Certificates, Device Certificates and Certificate Revocation List. The new choices as shown in the diagram below.

The Trusted Certificates and Device Certificates menu choices present a list of trusted certificates and device certificates respectively installed in the IP Phone. The Certificate Revocation List presents a list of certificates that the phone has been provisioned to revoke. Within each menu, if one highlights a particular certificate, the "View" softkey can be used to display more details on the particular certificate.

Product Advisements

The following is a list of advisements associated with UNIStim software release 4.0. Some advisements remain from previous releases of software, whereas other advisements reflect new or changed behavior introduced with UNIStim software release 4.0. Advisements that are new to UNIStim software release 4.0 or have changed since previous releases of UNIStim software are prefixed with “NEW”.

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

If the IP Phone 1110 is upgraded (or downgraded) from UNIStim software release 4.0 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.

NEW - Phone appears locked when downloading large font files over the VPN (applies to the IP Phone 1120E, 1140E, 1150E)

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

NEW – Initial certificate accepted by the IP Phone 1110 cannot be signed (applies to the IP Phone 1110 only)

In UNIStim software prior to release 4.0, the initial X.509 certificate installed in the phone had to be unsigned. With UNIStim software release 4.0, for all phones except the IP Phone 1110, the initial certificate can now be signed. Unfortunately the IP Phone 1110 does not yet support the ability to accept a signed certificate as the initially installed certificate. Support for the IP Phone to accept a signed certificate as the initially installed certificate will be delivered in a maintenance build of UNIStim software.

NEW – DOWNLOAD_MODE cannot be FORCED for license keycode files (applies to the IP Phone 1110, 1120E, 1140E and 1150E)

An issue was discovered with the DOWNLOAD_MODE command in the new [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 maintenance build of UNIStim software.

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

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

2-step upgrade may be required to load UNIStim software release 4.0 on the IP Phone 2007 (applies to the IP Phone 2007 only)

Due to changes in the memory structure of the IP Phone 2007, a 2-step upgrade may be required to load UNIStim software release 4.0 onto the IP Phone 2007 if the upgrade is performed with TFTP. If the IP Phone 2007 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 4.0. But if the IP Phone 2007 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 4.0. The 2-step up upgrade is not required if the upgrade is performed from the call server using UFTP.

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

Recent hardware changes in the IP Phone 1120E and IP Phone 1140E restrict the minimal allowable software version on these phones. The new hardware phones will absolutely accept an upgrade to UNIStim software release 4.0. But the new hardware IP Phone 1120E and new hardware IP Phone 1140E will NOT accept a downgrade to any software version previous to UNIStim software release 3.1 (0624C6J and 0625C6J respectively)

The new hardware is introduced with the following specific PEC and hardware release numbers:

PEC	Hardware Release	Description
NTYS03ADE6	01	IP Phone 1120E Graphite with Icon Keycaps (RoHS)
NTYS03BDE6	01	IP Phone 1120E Graphite with English keycaps (RoHS)
NTYS03BDGS	01	IP Phone 1120E GSA (RoHS)
NTYS05ACE6	50	IP Phone 1140E Graphite with Icon Keycaps (RoHS)
NTYS05BCE6	50	IP Phone 1140E Graphite with English keycaps (RoHS)
NTYS05BCGS	01	IP Phone 1140E GSA (RoHS)

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 Phone).

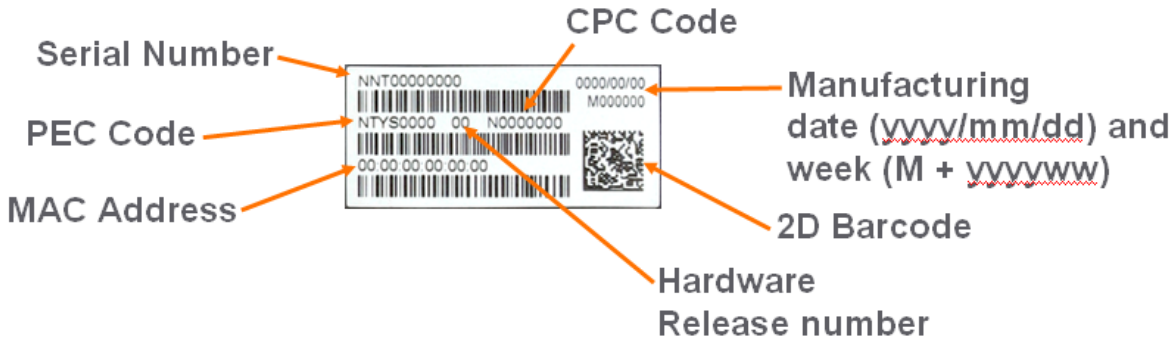


Figure 1 – IP Phone Product Label

If UFTP software download is used within the Communication Server 1000 environment, Nortel recommends that the software image for the IP Phone 1120E and IP Phone 1140E on the signaling server be upgraded minimally to UNIStim software release 3.1.

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 require 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.

If TFTP software download is used, and the TFTP server is not upgraded to UNIStim software release 3.1 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, the "umsUpgradeAll" Main Office system command should **not** to be executed when the branch office sites has the new hardware IP Phone 1120E or the new hardware IP Phone 1140E and the IP phone software at the Main Office precedes UNIStim software release 3.1.

Two SRG atomic patches 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 atomic patch BCM.R400.294-SRG-4.8-1-0 and later.

For SRG50 release 3.0, the denial of software downgrade support is included in atomic patch BCM050.R300.SRG-194-1 and later. This patch is not available for SRG50 release 2.0

For complete details on the minimal allowable software for the new hardware changes in the IP Phone 1120E and IP Phone 1140E, please refer to product bulletin **P-2009-0015-Global.**

EAP-MD5 and Microsoft Windows Server 2008 (applies to IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230)

If access control is enabled on the IP Phone and MD5 is chosen as the EAP mode, realize that EAP-MD5 is not available by default in the Microsoft Windows Server 2008 NPS[19] 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 Phones using MD5 access control.

PC Port resets during software upgrade (applies to IP Phone 2002, 2004, and 2007)

The PC port on the IP Phone 2002, 2004 and 2007 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 Phone's PC port will be disrupted during these periods.

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

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

The Algo 4900 USB ATA must have firmware version v1.00.32v or greater before connecting the adapter to the IP Phone. 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 the phone 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.

Constant humming sound may be heard in Nortel USB Adapter (applies to the IP Phone 1120E, 1140E and 1150E)

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

The humming noise is within the headset adapter can be corrected with upgrading the headset adapter firmware to version 2.00.98 or greater.

Nortel 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 IP Phone 1120E, 1140E and 1150E models under "Phones, Clients and Accessories" as file Adapter3v2.0098.zip.

To load the version 2.00.98 firmware onto the Nortel 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 Nortel USB Headset Adapter to the PC.
5. Start the Adapter3v2.0098.exe application to load the firmware onto the device.

IP Phone's performance will be diminished during broadcast storms (applies to IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230)

By default, network traffic to the IP Phone 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 Phone'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 IP Phone 2007, 1120E, 1140E, and 1150E)

In UNIStim software prior to release 3.2 (0621C6M, 0624C6O, 0625C6O and 0627C6O on the IP Phone 2007, 1120E, 1140E, and 1150E 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.

Therefore with UNIStim software release 3.2, 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 IP Phone 1120E, 1140E and 1150E)

In networks in which a PC is connected to the IP Phone’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 which due to the speed mismatch between the two phone ports can overflow the buffers in the phone resulting in retransmissions.

Although the IP Phones 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 Phone can request a brief “pause” from the transmitting Ethernet device if the IP Phone 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.

Incompatibility between older IP Phones and the Nortel-i2004-B option string (applies to Phase 0 IP Phone 2004, Phase 1 IP Phone 2002 and Phase 1 IP Phone 2004 only)[20]

A compatibility issue was found with the new Nortel-i2004-B option type and the older Phase 0 IP Phone 2004 (NTEX00), Phase 1 IP Phone 2002 (NTDU76) and Phase 1 IP Phone 2004 (NTDU82). Even thought these older phones ignore the Nortel-i2004-B option type, the length of the DHCP frame causes problems for the older phones. Since the list of all the parameters that can be provisioned via the Nortel-i2004-B options is extensive, the length of the DHCP frame can be quite large. The older phones will only accept a DHCP message to a maximum of 590 bytes (far short of the maximum DHCP message size of 1456 bytes). In a mixed environment of phones that support Nortel-i2004-B with Phase 0 and Phase1 phones one must either:

- Ensure any option string that are defined are small enough that the DHCP message does not exceed 590 bytes, or
- Service the Phase 0 and Phase 1 phones with a DHCP offer that excludes the Nortel-i2004-B option.

Receiving a LLDP MED Network Policy TLV from the network infrastructure will cause the phone to ignore DSCP from the Communication Server 1000 Element Manager and the Info Block (applies to IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230)

Because of the precedence order, in auto-provisioning mode (i.e. the value has not been overridden manually) if the IP Phone 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" introduced in UNIStim software release 3.3 provides a work-around to this advisory.

[20] The Phase 0 IP Phone 2004, Phase 1 IP Phone 2002 and Phase 1 IP Phone 2004 are now End of Life (EOL) products

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

In software loads prior to UNIStim software release 2.2 for IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230 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 2.3) 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 and existing deployment.

Manually provisioned link speed and duplex mode restored to "Auto" after software upgrade (applies to IP Phone 2007, 1120E, 1140E and 1150E)

In UNIStim software release 1.3 (0604DAX, 0621C3N, 0623C3F, 0624C3F, 0625C3F and 0627C3F for Phase II Phones, IP Phone 2007, IP Phone 1110, 1120E, 1140E and 1150E

respectively) Nortel introduced greater low level network control available through the phones configuration menus. The greater control included allowing the link speed and the duplex mode on the IP phones to be provisioned independently for both the network port and the PC port

By delivering this greater network control, the software unfortunately has 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 Phone 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 Phones, 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 IP Phone 2007, IP Phone 1110, 1120E, 1140E, 1150E and 1210)

The IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E and IP Phone 1210 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 IP Phone 1140E and 1150E)

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

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

One important note when upgrading the IP Phone 1120E and IP Phone 1140E to UNIStim software release 4.0 from any load previous to 0624C1B or 0625C1B respectively is that a 2-step upgrade will be required. The IP Phone 1120E 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 4.0 respectively.

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

Adding Asian languages to an IP Phone 2007 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 IP Phone 2007 software to using TFPT with the former configuration files ("BasicConfig" folder) – or upgrade the software from the call server.
2. Once the IP Phone 2007 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 IP Phone 2007, 1110, 1120E, 1140E and 1150E)

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 Phones. But, if one wishes to run SRTP PSK with Communication Server Release 5.0, patch MPLR24632 is required on the Communication Server 1000[21]. 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 IP Phone 2007, 1110, 1120E, 1140E and 1150E)

As stated above, running SRTP using PreShared Keys (PSK) is still a valid option in the IP Phones. But one important note when upgrading the IP Phones 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

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

SRTP PSK is backward compatible is UNIStim software release 1.3 (0621C3N, 0623C3G, 0624C3G, 0625C3G and 0627C3G for the IP Phone 2007, 1110, 1120E, 1140E and IP Phone 1150E respectively).

One way speech path behind NAT routers (applies to IP Phone 2007, 1120E, 1140E and 1150E)

A problem exists with some NAT routers that cause one way speech path. This problem is addressed by the application of patch MPLR21030 on the Communication Server 1000 Release 4.5 and 4.0[22]. The Communication Server 1000 patch is located in the Meridian PEP library at the www.nortel.com/support web site.

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

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 IP Phone 2007 (applies to IP Phone 2007 only)

It has been discovered that certain USB Mice do not work with the IP Phone 2007. 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 IP Phone 2007. 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.

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

The IP Phone 1110, 1120E, 1140E and 1150E graphical display contrast control can be adjusted either locally (on the phone) or through the call server (TPS) control. The Communication Server 1000 TPS 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 TPS contrast setting is restored and the user may need to adjust contrast again.

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

[22] The patch is not required on Communication Server 1000 Release 5.0 and greater

Volume adjustments are not persistent across phone resets (applies to IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230)

Even though the speech volume and ringer volume is controlled by the IP phone, 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 IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230)

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 IP Phone 2007, the IP Phone 1100 series and the IP Phone 1200 series, 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 NTP 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 4.0 for IP Phones also continues to improve the overall quality of the IP Phone software through the delivery of ongoing resolution of CRs and closed cases. Numerous quality improvements have been delivered, and 6 customer cases have been closed in UNIStim 4.0.

UNIStim software release 4.0 for IP Phones close the following cases:

Case #	Title
090708-75234	Slight chance that the IP Phone 2004 may freeze when ending an IP Call Recording (IPCR) call
090824-03336	Problem with the IP Phone 2004 obtaining an IP address when 802.1Q is enabled
090805-92397	Issue with Mouse Cursor on the IP Phone 2007 when backlight turns off
090713-78022	Issue with menu access when Lock Menu is enabled
090519-43214	SSH challenge prompt causes issue on IP Phone 1100 series
090728-87526	Concern with lowest ring tone setting on the IP Phone 1120E

IP Phone Compatibility

UNIStim software release 4.0 for IP Phones is compatible with the following IP Phones:

PEC	Description	Software file
NTDU96xxxxxx	IP Phone 2007	0621C7A.bin
NTYS02xxxxxx	IP Phone 1110	0623C7F.bin
NTYS03xxxxxx	IP Phone 1120E	0624C7F.bin
NTYS05xxxxxx	IP Phone 1140E	0625C7F.bin
NTYS06xxxxxx	IP Phone 1150E	0627C7F.bin
NTYS18xxxxxx	IP Phone 1210	062AC7F.bin
NTYS19xxxxxx	IP Phone 1220	062AC7F.bin
NTYS20xxxxxx	IP Phone 1230	062AC7F.bin

IP Phone 2004 (NTEX00), Phase 1 IP Phone 2002 (NTDU76), and Phase 1 IP Phone 2004 (NTDU82) cannot load these releases.

Call Server Compatibility and Requirements

These software releases are compatible with the below Nortel Call Servers. Note that the IP Phone 1200 series is 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.

Communications Server 1000

Call Server Release	Notes / Advisements
CS 1000 6.0R - IP Line 6.00.18 - SS (Linux App) 6.00.018	*Nortel recommends an upgrade to these software releases 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**. Please refer to NTP NN43001-315 Linux Platform Base and Applications Installation and Commissioning for patch installation instructions.
CS 1000 5.5J - IP Line 5.5.12 - SS 5.5.12	*Nortel recommends an upgrade to these software releases at the earliest opportunity.* The DTLS and SCR features are not supported on this platform.
CS 1000 5.00W - IP Line 5.00.31 - SS 5.00.31	*Nortel recommends an upgrade to these software releases at the earliest opportunity.* The DTLS and SCR features are not supported on this platform The IP Phone 1200 series is not supported on this platform.

Survivable Remote Gateway (SRG)

Call Server Release	Notes / Advisements
SRG 50 3.0	*Nortel recommends an upgrade to these software releases at the earliest opportunity.* No SRG50 patches are required to support the Enhanced Software Download feature that allows the IP Phone 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 Phone. But if the "Main" Communication Server 1000 is on release 4.0 a Communication Server 1000 patch is required on the "Main" to allow the SRG50 to upgrade the IP Phone software. The patch is MPLR21148 and is available from the Meridian PEP library at the www.nortel.com/support web site. The IP Phone 1150E is not supported on the SRG50 5.0.
SRG 50 2.0	*Nortel recommends an upgrade to these software releases at the earliest opportunity.* No SRG 50 patches are required to support the Enhanced Software Download feature that allows the IP Phone 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 Phone. But if the "Main" is Communication Server 1000 release 4.0, a Communication Server 1000 patch is required on the "Main" to allow the SRG 50 to upgrade the IP Phone software. The patch is MPLR21148 and is available from the Meridian PEP library at the www.nortel.com/support web site. The IP Phone 1110, IP Phone 1150E and IP Phone 1200 series are not supported on SRG 50 2.0.

SRG 200/400 1.5	*Nortel recommends an upgrade to these software releases at the earliest opportunity.* No SRG patches are required to support the Enhanced Software Download feature that allows the IP Phone 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 Phone. But if the “Main” is Communication Server 1000 release 4.0, a CS1000 patch is required on the “Main” to allow the SRG 200/400 to upgrade the IP Phone software. The patch is MPLR21148 and is available from the Meridian PEP library at the www.nortel.com/support web site. The IP Phone 1110, IP Phone 1150E and IP Phone 1200 series are not supported on SRG200/400 Rls1.5

Business Communications Manager (BCM)

Call Server Release	Notes / Advisements
BCM 200/400 4.0	*Upgrading of the set software is dependent upon a BCM system patch that includes the set software.* Although UNIStim software release 4.0 for IP Phones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The IP Phone 1110, IP Phone 1150E and IP Phone 1200 series are not supported on BCM 200/400.
BCM 50 5.0	*Upgrading of the set software is dependent upon a BCM system patch that includes the set software.* Although UNIStim software release 4.0 for IP Phones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The IP Phone 1150E is not supported on BCM 50 5.0.
BCM 50 3.0	*Upgrading of the set software is dependent upon a BCM system patch that includes the set software.* Although UNIStim software release 4.0 for IP Phones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The IP Phone 1150E is not supported on BCM 50 3.0.
BCM450 5.0	*Upgrading of the set software is dependent upon a BCM system patch that includes the set software.* Although UNIStim software release 4.0 for IP Phones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The IP Phone 1150E is not supported on BCM 450 5.0.
BCM450 1.0	*Upgrading of the set software is dependent upon a BCM system patch that includes the set software.* Although UNIStim software release 4.0 for IP Phones is GA quality, at the time of this writing, the extent of BCM support is being confirmed. The IP Phone 1150E is not supported on BCM 450 1.0.

Communication Server 2100 Centrex IP Client Manager (CICM)

Call Server Release	Notes / Advisements
CICM 10.1 MR2 (Succession)	*Upgrading of the set software is dependent upon CICM performing regression test activities on UNIStim software release 4.0 for IP Phones to verify their performance on this CICM product.* Although UNIStim software release 4.0 for IP Phones is GA quality, at the time of this writing, the extent of CICM support is being confirmed. The IP Phone 1210 is not supported on CICM 10.1
CICM 10.0 (Succession)	*Upgrading of the set software is dependent upon CICM performing regression test activities on UNIStim software release 4.0 for IP Phones to verify their performance on this CICM product.* Although UNIStim software release 4.0 for IP Phones is GA quality, at the time of this writing, the extent of CICM support is being confirmed. The IP Phone 1200 series are not supported on CICM 10.0
CICM 9.0 (Succession)	*Upgrading of the set software is dependent upon CICM performing regression test activities on UNIStim software release 4.0 for IP Phones to verify their performance on this CICM product.* Although UNIStim software release 4.0 for IP Phones is GA quality, at the time of this writing, the extent of CICM support is being confirmed. The IP Phone 1200 series are not supported on CICM 9.0

System Compatibility and Requirements

System	Notes / Advisements
Contact Recording and Quality Monitoring (CRQM) 7.0	*The Secure Call Recording feature in UNIStim software release 4.0 interworks with Nortel Contact Recording and Quality Monitoring release 7.0* For additional information on Nortel CRQM solution and its support for Secure Call Recording, please refer to the *CRQM 7.0 Planning, Installation and Administration Guide* NN44480-300
Nortel VPN Router (NVR) 8.00 or greater	*The UNIStim VPN Client (UVC) feature in UNIStim software release 4.0 interworks with Nortel VPN Routers running release 8.00 and greater*
Nortel Application Gateway 2000 6.3 and higher	*These software releases provide support to interwork with Nortel Application Gateway 2000 (AG2000) release 6.3* The Nortel Application Gateway solution continues to deliver on IP Telephony's promise of convergence with important enhancements to the powerful packaged applications on the IP Phone's desktop, applications that are simply not possible to deliver with the traditional digital telephone. With the Nortel Application Gateway, IP Phone communication is truly transformed into a new feature-rich communications experience. For more information on the capabilities introduced with AG2000 please refer to the Product Bulletin **P-2008-0005-Global.** The AG2000 does not support the IP Phone 1150E.
Nortel Secure Multimedia Controller (SMC) 1.0	*These software releases continue to provide support to interwork with Nortel Secure Multimedia Controller (SMC) 2450.* The SMC 2450 is a purpose-built application firewall, delivering an integrated inside threat security solution to protect Nortel's IP phones 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 introduced with Nortel SMC 2450 please refer to the SMC 2450 Product bulletin P-2006-0131-Global and the SMC 2450 Sales and Marketing bulletin SM-2006-0132-Global.

IP Phone Software Upgrade Methods (Communication Server Dependent)

Upgrading the software in a Communication Server 1000 environment

The IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220 and 1230 supports remote software upgrades through both a TFTP process and the more automated UFTP process direct from the Communication Server 1000.

Note that the IP Phone 1200 series is only supported on Communication Server 1000 Release **5.5** 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 NTP NN43001-368.

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

Upgrading the software in a Survivable Remote Gateway (SRG) 200/400 and SRG50 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, NTP 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, NTP 553-3001-207.

Upgrading the software in a Business Communications Manager (BCM) environment

Upgrading of the software is dependent upon a BCM system patch that includes the set 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 which includes all atomic patch content since the previous Smart Update.

Patches and Smart Updates 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 software in a Communication Server 2100 CICM environment

Depending on the MR level, the IP Phone 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 Phones, refer to the CICM Administration and Security NTP (NTP NN10252-611.06.03) in the section titled "Downloading firmware to the CICM Element Manager".

Nortel is a recognized leader in delivering communications capabilities that enhance the human experience, ignite and power global commerce, and secure and protect the world's most critical information. Serving both service provider and enterprise customers, Nortel delivers innovative technology solutions encompassing end-to-end broadband, Voice over IP, multimedia services and applications, and wireless broadband designed to help people solve the world's greatest challenges. Nortel does business in more than 150 countries. For more information, visit Nortel on the Web at www.nortel.com.

Appendix A: Certificate Installation (applies to the IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220, 1230)

Installing CA Root Certificates using the phone's configuration file

The recommended means to install a CA root certificate on the phone is to use the 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.

Installing CA Root Certificates and Device Certificates using SCEP

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

With UNIStim software release 4.0 the phone's support for SCEP has been enhanced as well support for PKCS#12 device certificates has been introduced.

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

- *CA Server*: Enter 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 NTIPP012345 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.[23] 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.

After the certificate is approved (automatically or manually), the "Waiting for Approval…" prompt will be removed. If for any reason the approval fails (and while the phone is actually waiting for approval), an "Abort" key will appear to allow the installer a chance to abort the process.

Once approved, phone will be ready to use the device certificate[24].

With UNIStim software release 4.0 the phone's support for SCEP has been 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 phone, please refer to the IP Phones Fundamentals document (NTP NN43001-368).

[23] 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.

[24] 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.

Installing Device Certificates using PKCS#12:

New with UNIStim software release 4.0 for IP Phones is the support for PKCS#12 device certificates. 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[25]. 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 Phone via the IP Phone'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.

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

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

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)[26].

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 phone'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
```

[26] 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 Certificate Profiles (DCP):

Also new with UNIStim software release 4.0 for IP Phones is the support for Device Certificate Profiles (DCP). 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:

Model	Number of supported DCP
IP Phone 2007	3
IP Phone 1100 series (except the IP Phone 1110)	6
IP Phone 1110	5
IP Phone 1200 series	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 maximum 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.

dcpsource1	'scep' 'pkcs12'	Method used to install device certificates
dcpactive1	'n' Inactive 'y' Active	Profile is active or not
dcppurpose1[27]	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

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.

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

[27] 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

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 IP Phone 1100 series (except the IP Phone 1110), an additional 4 times for the IP Phone 1110 and the IP Phone 1200 series, and an additional 2 times for the IP Phone 2007. 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 Phone Info Block (applies to the IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220, 1230)

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 parameter will retain its default value, or the value that was previously provisioned for the parameter if the "stickiness" parameter is also set.

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 IP Phone 2007 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 ~~15~~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 ~~15~~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 ~~15~~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]
stickiness	‘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 IP Phone 1100 series Value from 7 to 39 for IP Phone 2007	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 (IP Phone 2007 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 (IP Phone 2007 only)
bt	‘y’ yes ‘n’ no	Enable Bluetooth (IP Phone 1140E 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[28]
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[29] 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

[28] 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.

[29] 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.

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
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.

[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

Appendix C: Provisioning the IP Phone with an Info Block via TFTP or HTTP (applies to the IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220, 1230)

The IP Phones 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 Phones that support the auto-provisioning feature (e.g. system.prv)
- ZONE provisioning file – provides provisioning information to IP Phones that belong to a unique defined zone or group (e.g. headqrtr.prv)
- TYPE provisioning file – provides provisioning information to all the IP Phones 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 Phone 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.

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
vlanf=y;                    # Enable VLAN filter
pc=y;                       # Enable PC port
pcs=a;                      # PC port speed
pcd=a;                      # PC port duplex
dq=y;                       # Enable 802.1Q for PC port
lldp=y;                     # Enable 802.1ab (LLDP)
pk1= ffffffffffffffff;      # force pk1 to ff SMC will update
pk2= ffffffffffffffff;      # force pk1 to ff SMC will update
stickiness=y;               # Enable stickiness
cachedip=n;                 # Enable cached IP
igarp=n;                    # Ignore GARP
srtp=n;                     # Enable PSK SRTP
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
hd=w;                      # Headset type
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 IP Phone 1140E
# Applies to all IP Phone 1140E within the network
bt=y;                      # Enable Bluetooth
```

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

Appendix D: Auto-Provisioning the IP Phone's Node and TN in a Communication Server 1000 Environment (applies to the IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220, 1230)

The introduction of auto-provisioning on the IP Phone 2007, the IP Phone 1100 series, and the IP Phone 1200 series also provides a centralized method of provisioning the Node and TN fields for these IP Phones when they are connected on a Communication Server 1000 system.

Prior to the availability of UNIStim software release 3.0 for IP Phones, 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.

With the delivery of UNIStim software release 3.0 for IP Phones 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 phone 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: Provisioning the IP Phone with an Info Block via DHCP (applies to the IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220, 1230)

The new Nortel specific option type ("Nortel-i2004-B") that was introduced in UNIStim software release 2.2 and release 2.3 for IP Phones. 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 IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E and IP Phone 1150E the IP Phones could obtain only limited provisioning parameters via Nortel specific DHCP options. The Nortel specific DHCP option types supported included:

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

With the introduction of the UNIStim software release 2.2 and greater for the IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E and IP Phone 1150E[30] a new Nortel specific option type is 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 Phone 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 Phones requires DHCP to send a class identifier option with the valid option type in each DHCP Offer and DHCP Acknowledgement.

[30] IP Phone 1210, 1220 and 1230 were introduced with UNIStim software release 2.2 for IP Phones and support Nortel-i2004-B from initial release.

The IP Phone 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[31] 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; …

An example DHCP provisioning string is as per the following[32]:

```
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 following table. 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.

Feature Advisements

A compatibility issue was found with the new Nortel-i2004-B option type and the older Phase 0 IP Phone 2004, Phase 1 IP Phone 2002 and Phase 1 IP Phone 2004. Even thought these older phones ignore the Nortel-i2004-B option type, the length of the DHCP frame causes problems for the older phones. Since the list of all the parameters that can be provisioned via the Nortel-i2004-B options is extensive, the length of the DHCP frame can be quite large. The older phones will only accept a DHCP message to a maximum of 590 bytes (far short of

[31] RFC 3942 states that DHCP site-specific options 128 to 223 are hereby reclassified as publicly defined options. The IP Phone 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.

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

the maximum DHCP message size of 1456 bytes). In a mixed environment of phones that support Nortel-i2004-B with Phase 0 and Phase1 phones one must either:

- Ensure any option string that are defined are small enough that the DHCP message does not exceed 590 bytes, or
- Service the Phase 0 and Phase 1 phones with a DHCP offer that excludes the Nortel-i2004-B option.

Appendix F: IP Phone Provisioning Precedence Rule and Stickiness Control (applies to the IP Phone 2007, 1110, 1120E, 1140E, 1150E, 1210, 1220, 1230)

The IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, IP Phone 1210, IP Phone 1220 and IP Phone 1230 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 Phone 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 Phone 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 Phone 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: IP Phone Configuration Menu on the IP Phone 1120E, IP Phone 1140E and IP Phone 1150E

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

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]
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 menu item is on the IP Phone 1140E and 1150E only.*

The IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E 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: IP Phone Configuration Menu on the IP Phone 2007

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

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 IP Phone 2007 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: IP Phone Configuration Menu on IP Phone 1110, IP Phone 1210, IP Phone 1220 and IP Phone 1230

The single-line based configuration menu structure below presents the complete configuration menu now available on the IP Phone 1110, IP Phone 1210, IP Phone 1220 and IP Phone 1230:

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 IP Phone 1110, IP Phone 1210, IP Phone 1220 and IP Phone 1230 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: IP Phone Configuration Menu on Phase II IP Phone 2001, Phase II IP Phone 2002 and Phase II IP Phone 2004

The single-line based configuration menu structure below presents the complete configuration menu now available on the Phase II IP Phone 2001, Phase II IP Phone 2002 and Phase II IP Phone 2004:

EAP Enable?[0-N,1-Y]:0
- *if "1"*
- **DeviceID:[ ]**
- **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**
- **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:**
- *else if "1"*
- **DHCP:0-Full,1-Partial:1**
  - *if "1"*
  - **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

The VLAN Cfg menu is only presented if DHCP is provisioned to "Partial" or "Full" above or if LLDP is enabled above.

if "0"

LLDP MED? [0-N, 1-Y] :0

The LLDP MED menu is only presented if LLDP is enabled above.

if "0"

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

The LLDP VLAN menu is only presented if LLDP is enabled above.

if "0"

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

The DHCP menu is only presented if DHCP is provisioned to "Partial" or "Full" above.

else if "1"

VOICE VLAN ID :

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

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

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

PC Port? [0-OFF,1-ON] :1 *This menu item, and submenus, are not available on the IP Phone 2001.*

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"

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

if "1"

DATA VLAN Cfg?0-A,1-M:0

This DATA VLAN Cfg menu item is only presented if LLDP is enabled above.

if "1"

DATA VLAN ID:

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

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

Cached IP? [0-N, 1-Y]:0

This Cached IP menu item is only presented if DHCP is provisioned to "Yes" above and Voice VLAN is not provisioned as "Auto".

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

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

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

Appendix K: Restore to Factory Defaults

The UNIStim software release 3.0 for IP Phones introduced the ability to restore an IP Phone to a “factory default” configuration. This can be useful when redeploying an IP Phone from one location to another, when starting to use an IP Phone 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 Phone which can be found on a label on the back of the IP Phone.

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 Phone 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 Phone has finished its boot-up procedure.

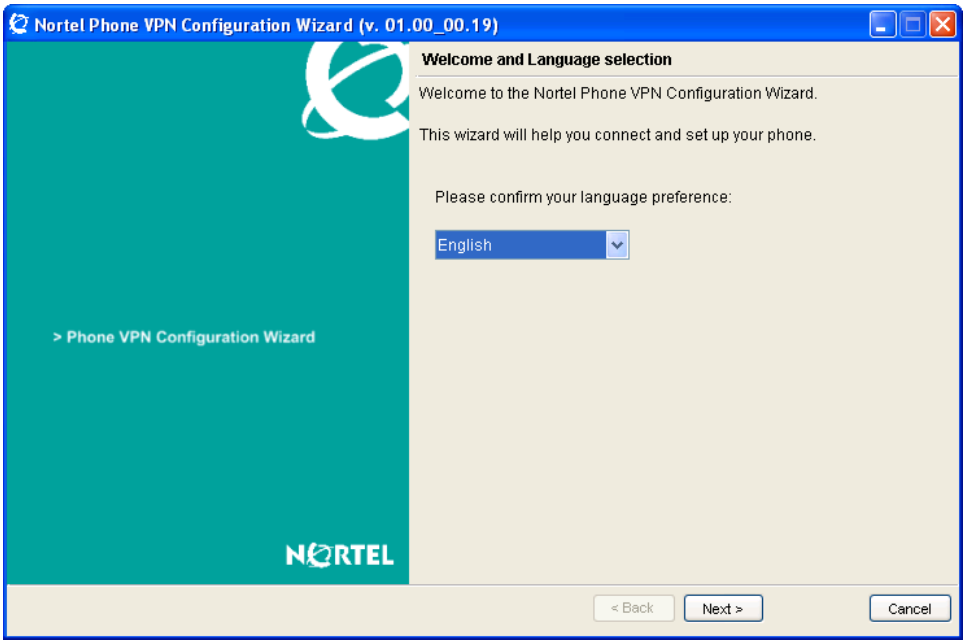
Appendix L: Phone VPN Configuration Wizard

The following paragraphs 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

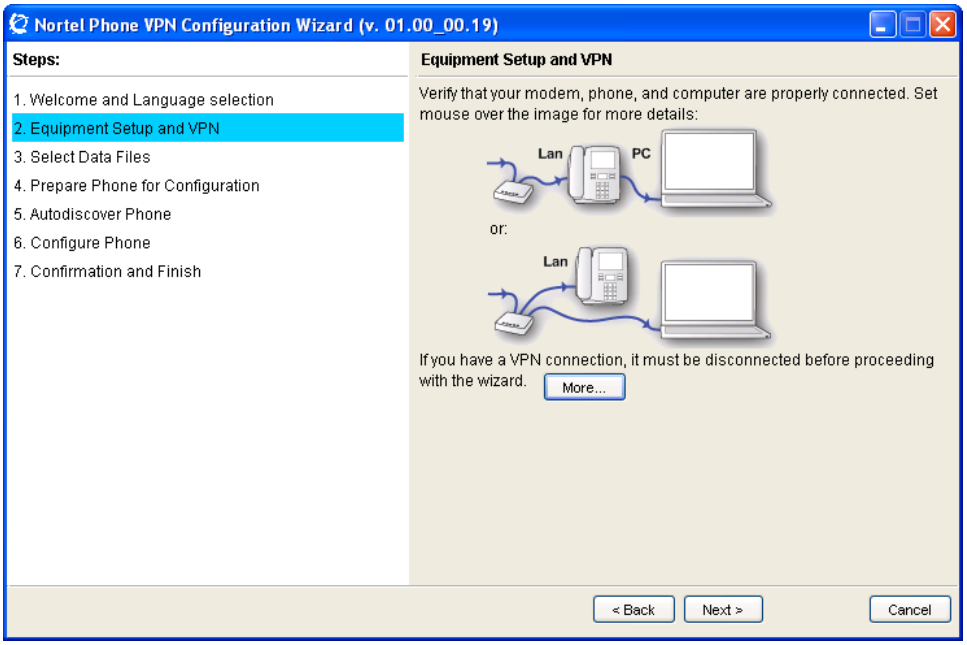
Welcome and Language selection

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.

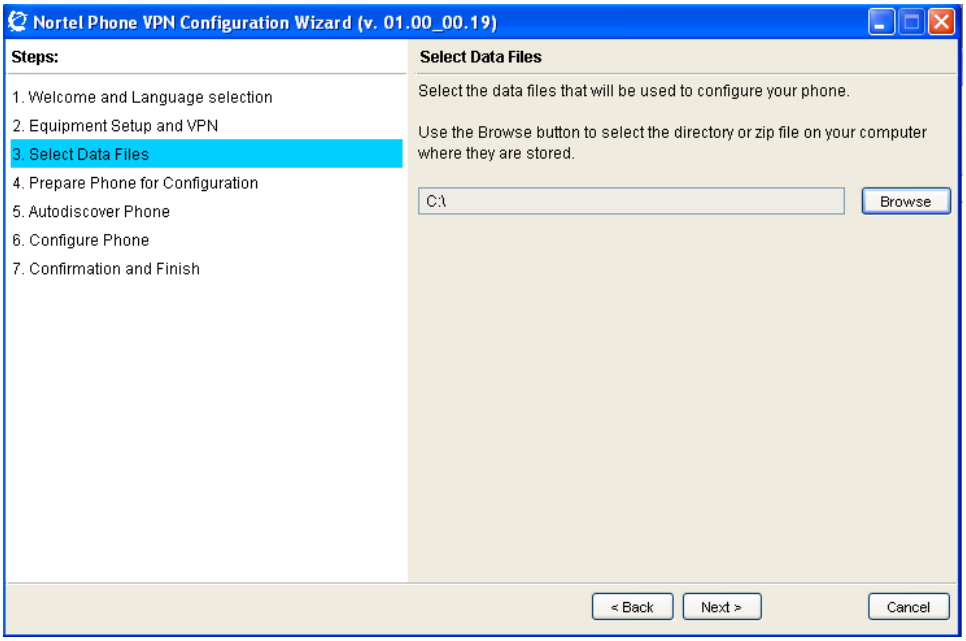


The Equipment Setup and VPN screen shows that the PC running the Phone VPN Configuration Wizard must either be plugged into the PC port of the IP Phone, or into a multi-port router or hub to which the IP Phone is also connected.

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 Phone. Once the Phone VPN Configuration Wizard finishes, the VPN client running on the PC can be re-established.

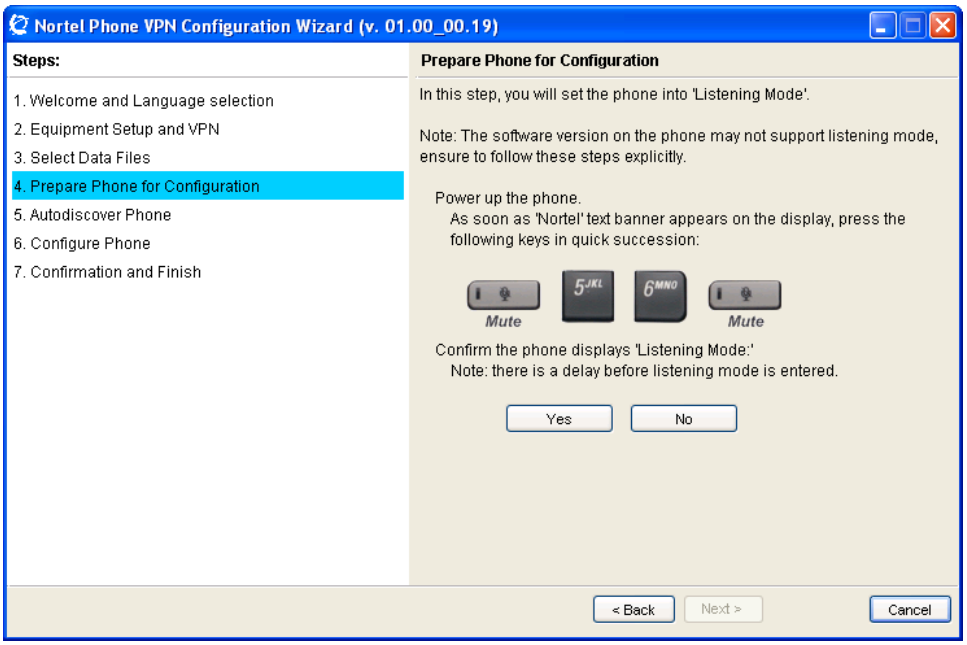
Select Data Files

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

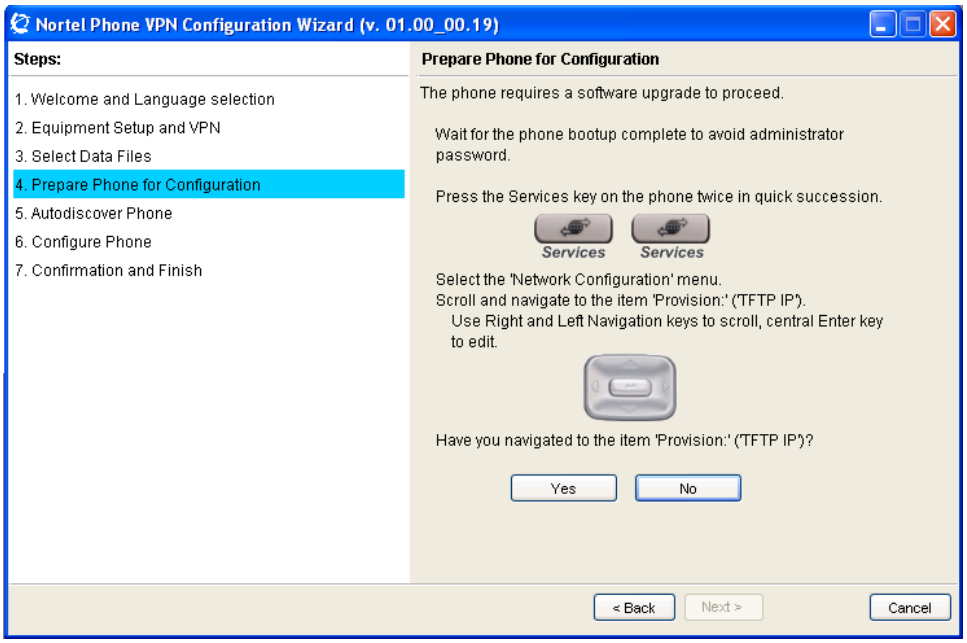
Once the data files (configuration and provisioning files) are located, the Prepare Phone for Configuration Screen provides instructions for placing the phone into “Listening Mode”. Listening Mode allows the phone to listen for the Phone VPN Configuration Wizard to establish a connection and transfer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



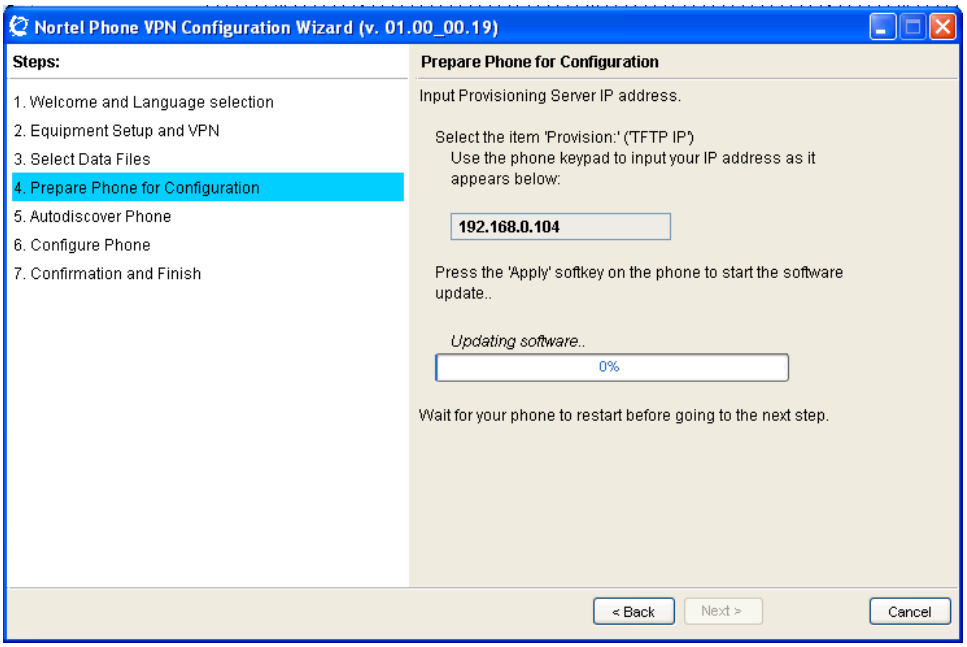
Autodiscover Phones

The IP Phone must now be power cycled and when the IP Phone 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 Phone'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.

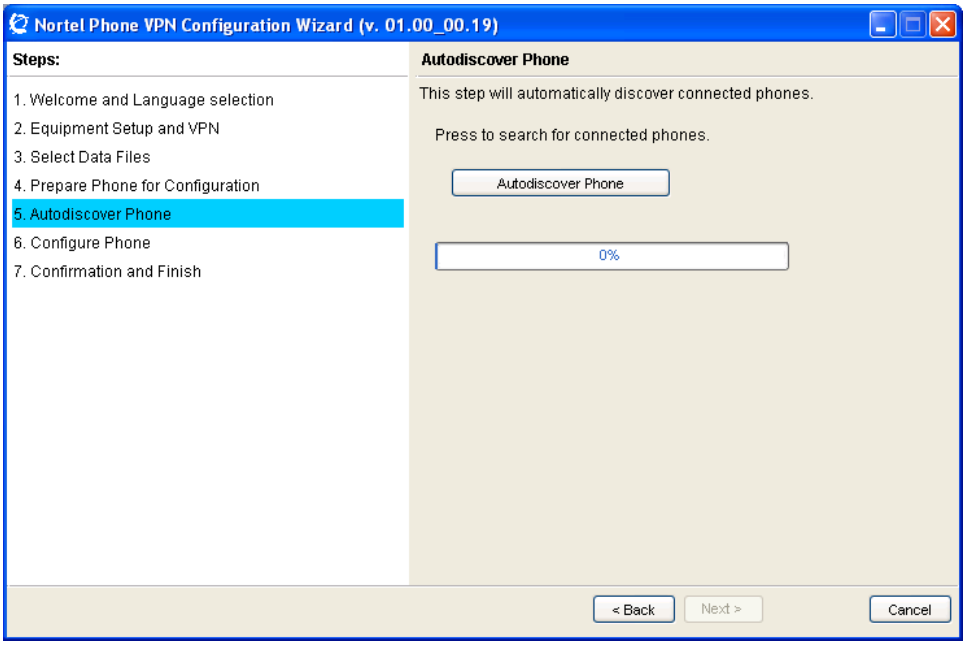


Once the phone has been upgraded to UNIStim software release 4.0, the phone should be able to enter Listening Mode. The IP Phone will reboot after the new software is downloaded.

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

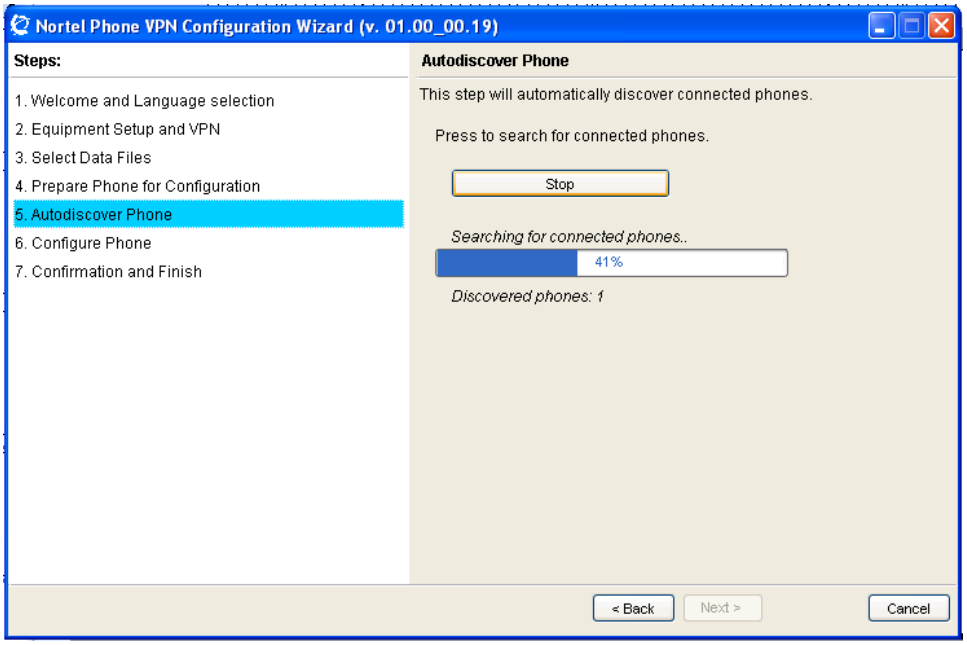
Once the phone is in Listening Mode, the next screen of the Phone VPN Configuration Wizard guides the user to discover the IP Phones that are in Listening Mode. The user is prompted to start the discovery process by pressing the “Autodiscover Phone” button. The Autodiscover Phone screen is shown in the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



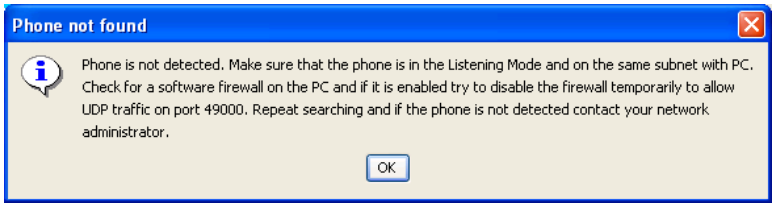
The Autodiscover process will find all phones in Listening Mode on the network. In most cases there will only be one phone discovered – the phone that the user placed in Listening Mode. But if for whatever reason several phones are found in Listening Mode, the user will be prompted to select the phone 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[33].

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

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

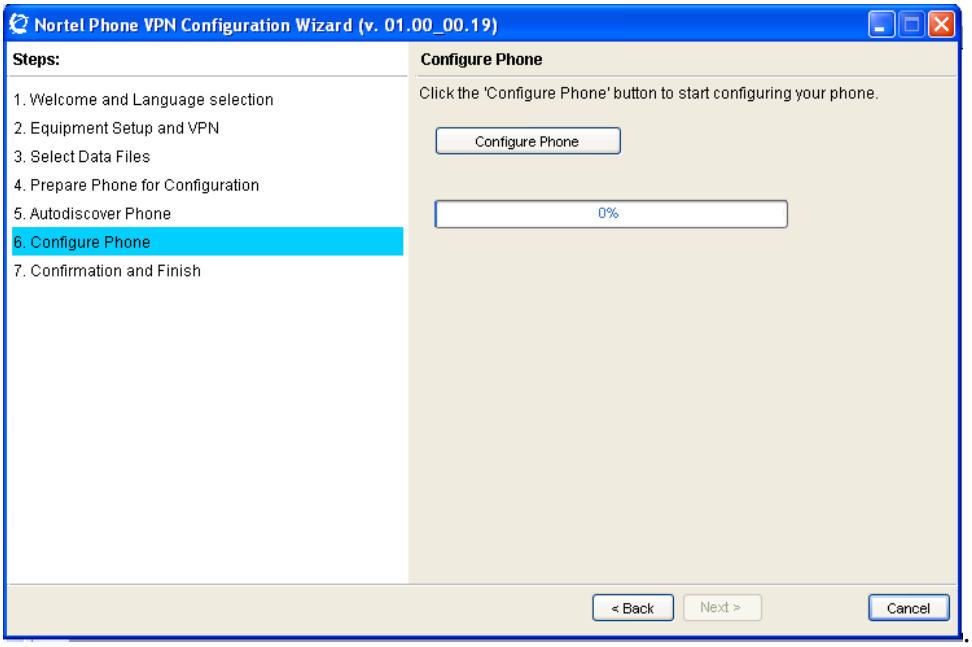


If a phone cannot be discovered, the Phone VPN Configuration Wizard warns that no phones can be found with the Phone not found screen shown below. If repeated attempts fail to discover a phone in Listening Mode please contact your network administrator.



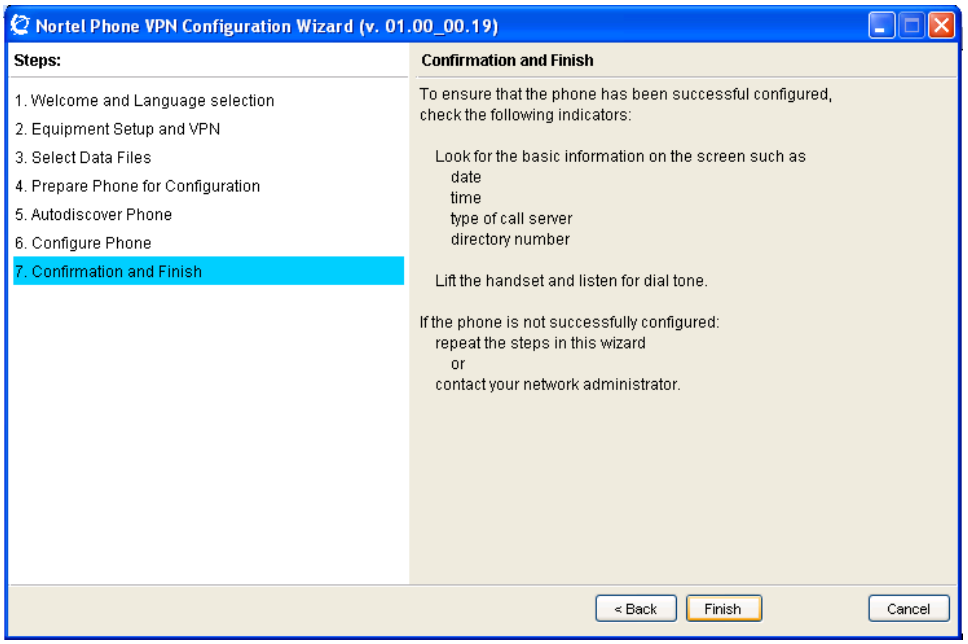
Configure Phone

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.



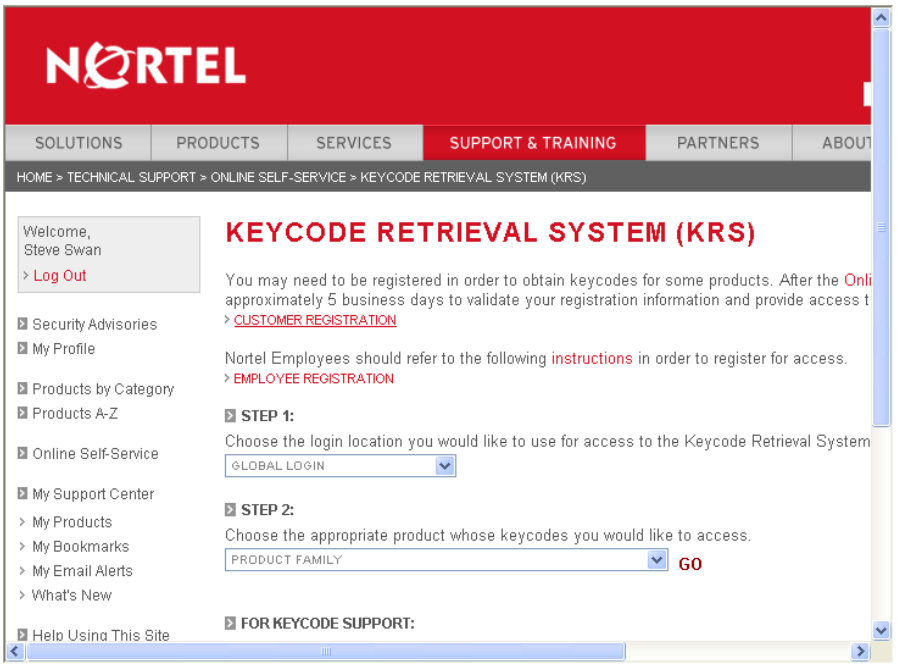
Confirmation and Finish

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.

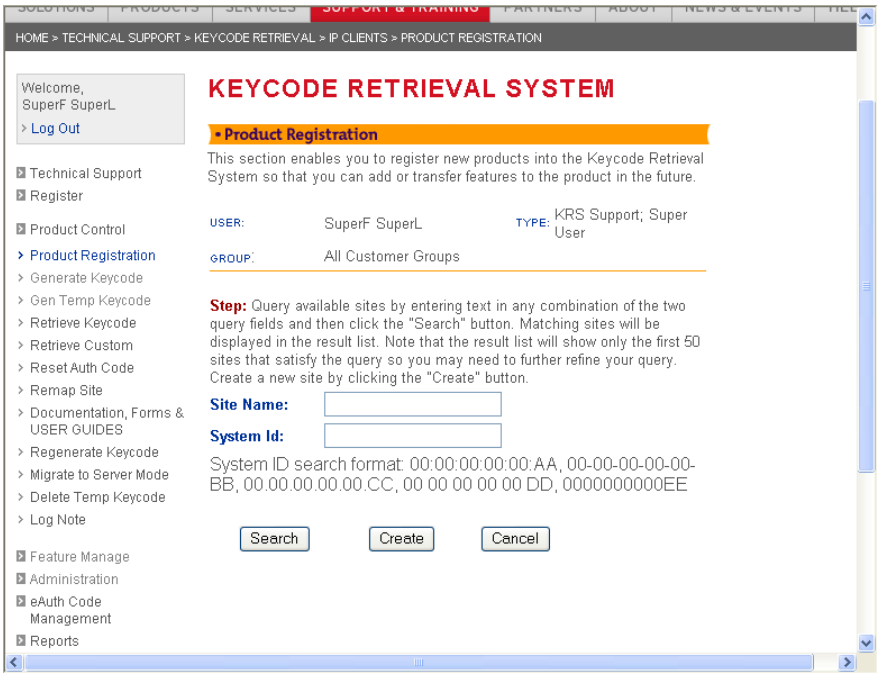


Appendix M: Nortel Keycode Retrieval System (KRS)

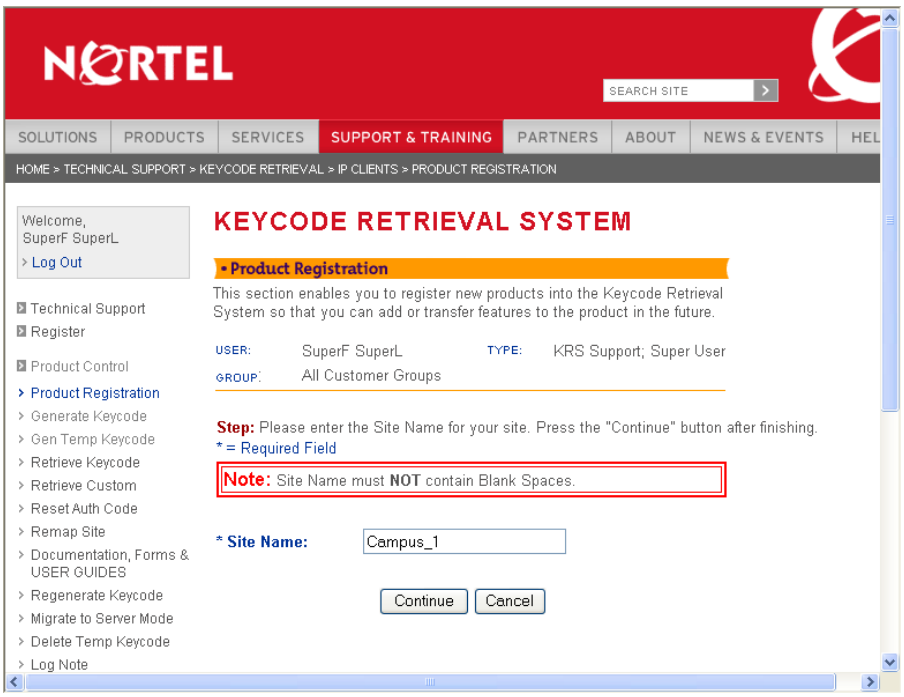
The home page of KRS is the login and Product Select page as shown in the diagram below. If you do not already have a KRS account, click on Customer Registration and follow the instructions to request an account.



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.

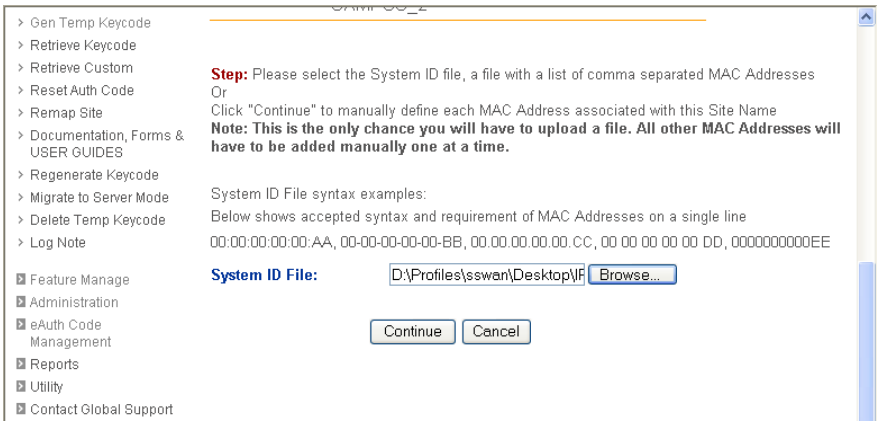


Before a keycode can be generated the system for which the keycode is to be generated must be registered. To begin Registration, one selects “Create” on the Product Registration Screen. After which the screen as shown below will allow one to enter a site name that will be used to identify the system. Please note that blank spaces are <u>not</u> 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 Phone 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.

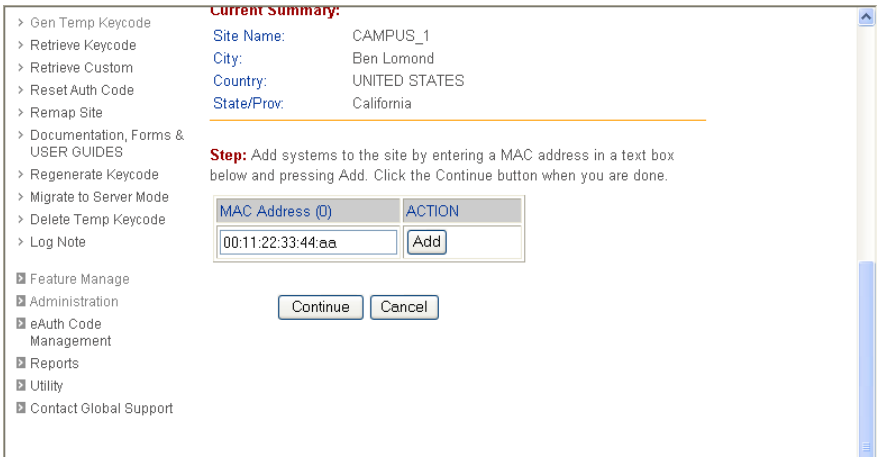
To use a comma delimited file of MAC addresses, select the Browse button to locate the file on the computer connected to KRS as shown on the diagram below. Once the comma delimited file of MAC addresses has been selected click Continue.



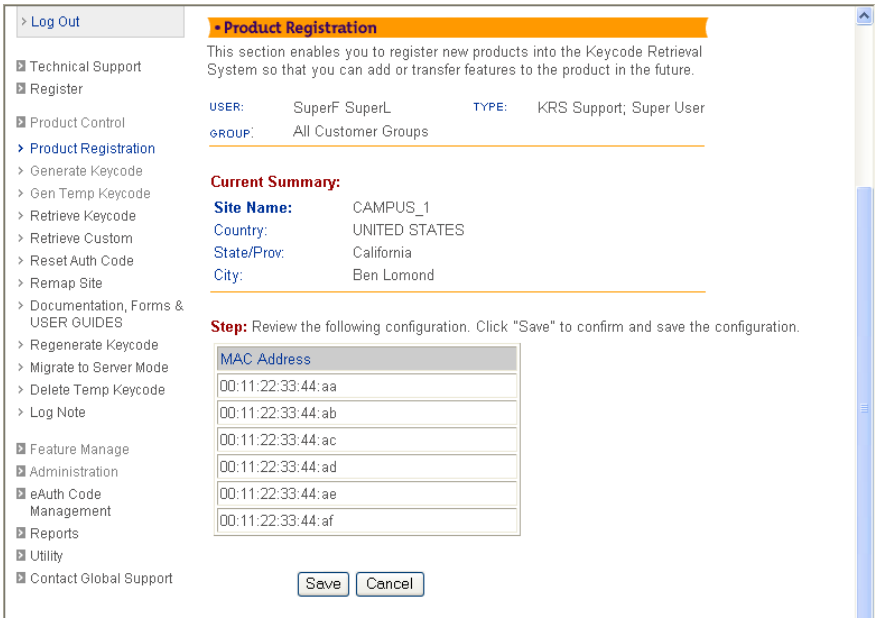
To manually type in each MAC address instead, leave the System ID File field blank and simply click Continue.

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.

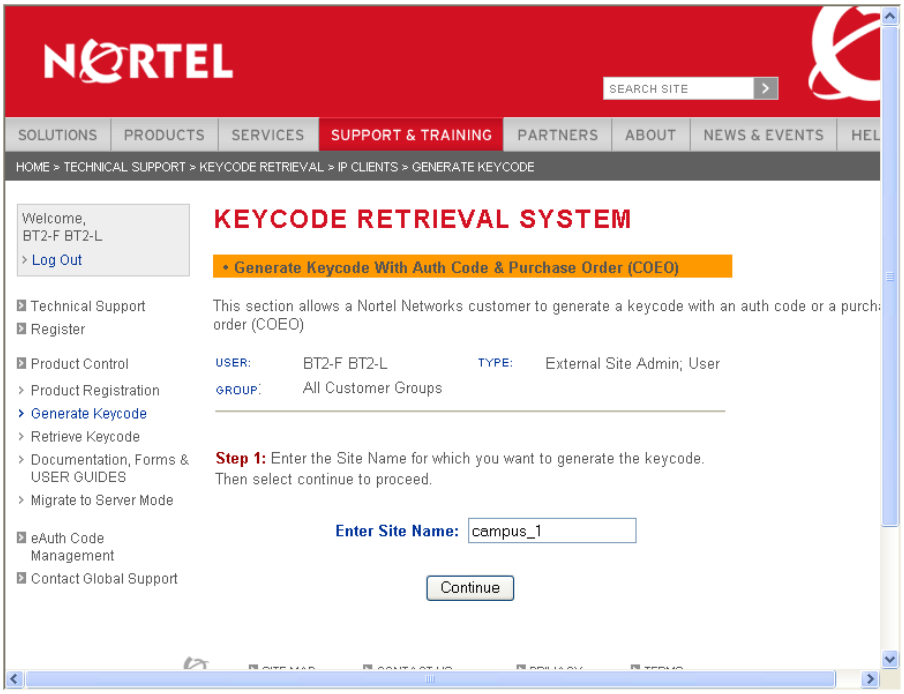


After all the MAC addresses have been entered (either manually or from a file) a summary screen as shown below will be presented to allow the user to review the list of MAC addresses a



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.

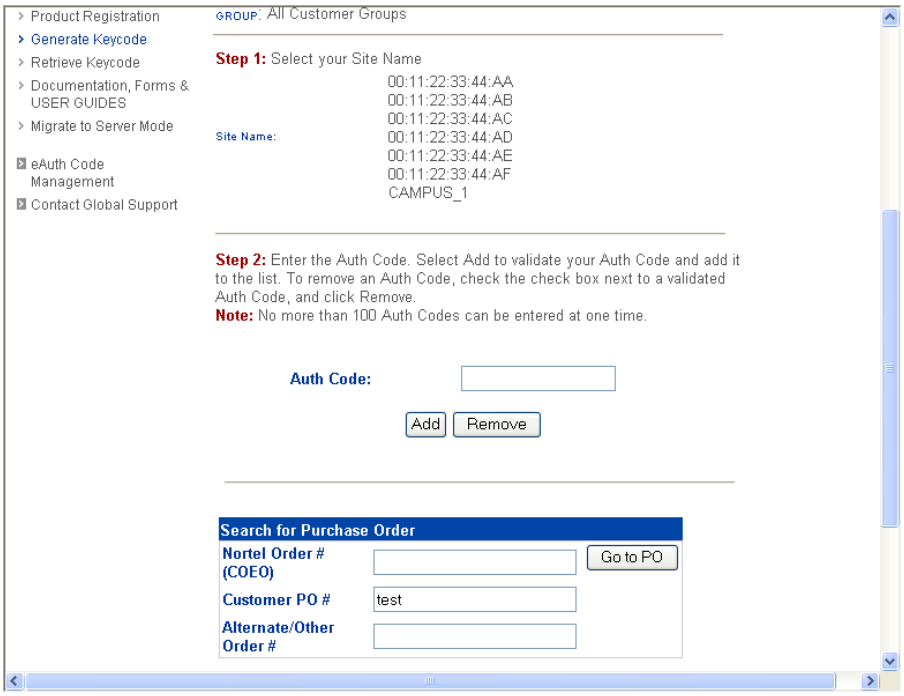
Registration is now complete and one is ready to generate the keycode by selecting Generate Keycode from the side bar on the left. The Generate Keycode page will be presented as shown below.



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[34].

[34] 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.



Once the correct PO is found, the next screen will show a list of each licensed feature on the PO[35]. 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.)[36] Once the quantity of each licensed feature has been specified click on Continue.

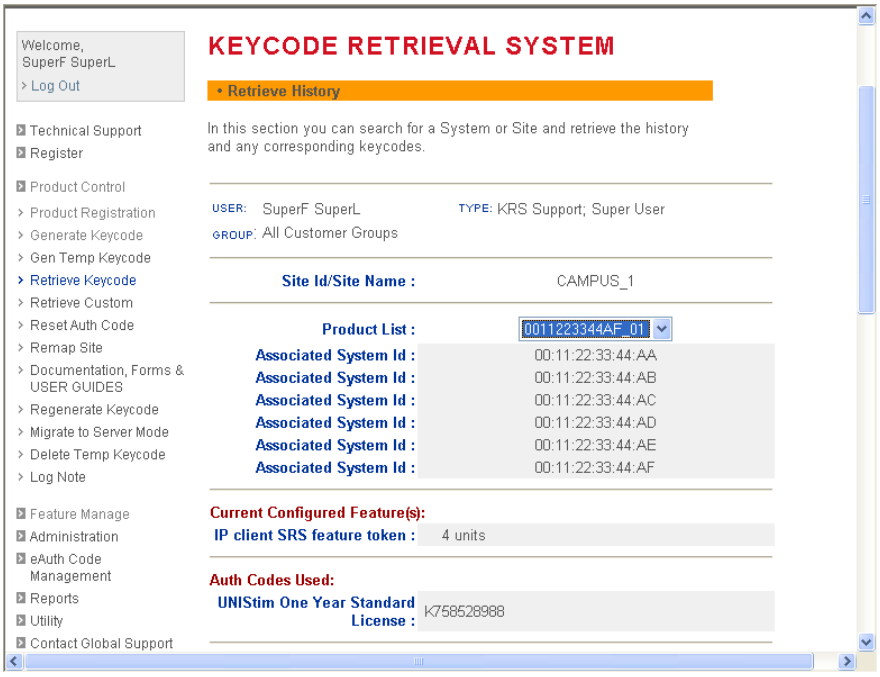
KRS will then show a summary of the current PO selection. Clicking on Continue returns the user to the "select" PO screen again, where if one wish they can search for additional PO's from which to pull additional licenses to add to the Keycode.

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.

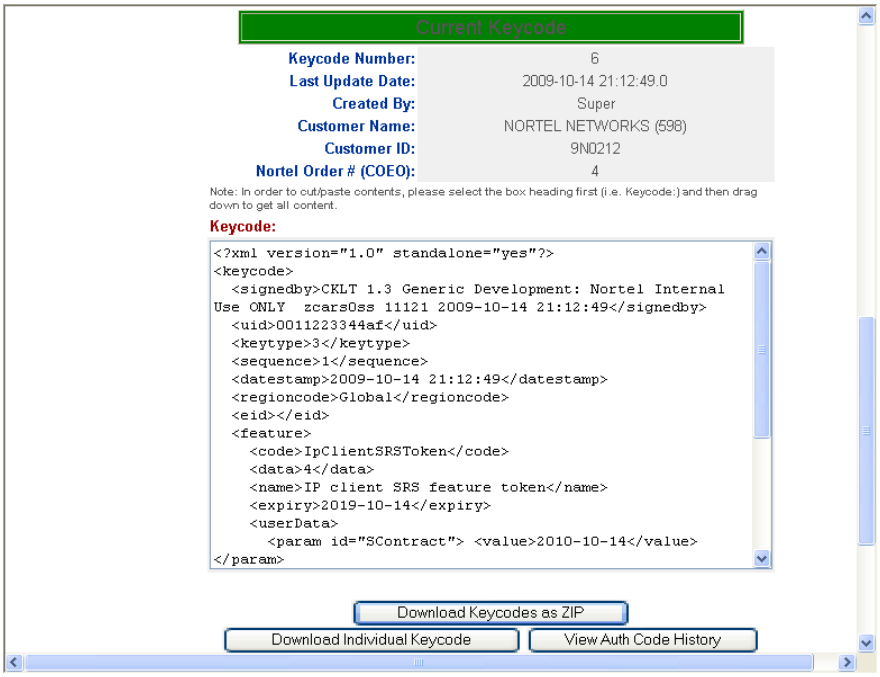
On the Retrieve History screen, as shown below, KRS will display keycode associated to each MAC address.

[35] 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

[36] 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 Phone provisioning server to load the keycode onto the IP Phone.

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.