NEC \Orchestrating a brighter world

NEC Meeting Center (NMC)

NMC Version 8.0 or above

Integration Guide to UNIVERGE® 3C™

Version 14
Revised 2/27/2017

Contents

For Questions regarding this document or the NMC, please send an email to NMC@Necam.com.

For questions regarding the UNIVERGE 3C, please send an email to 3CsalesSupport@Necam.com.

Overview

The NEC Meeting Center provides a collection of Value Added Service (VAS) applications. These applications can be hosted on physical or virtual servers (e.g., VMware). The NMC integrates with the U3C via SIP trunks for the bearer path and via Web Services for applications requiring access into U3C database (e.g., Text messaging to U3C IP phones).

Maximum Port Capacity supported is 384 Ports on one server if you are utilizing the web collaboration application. If you are performing audio conferencing, mass notification and/or emergency conferencing, a single server can support up to 1,000 ports. Greater capacity beyond this is possible by linking multiple servers together (if you have this need, please check with NEC Product Management at nmc@necam.com).

Following section describes the VAS applications available on the NMC:

Audio Conferencing Application

- Audio Conferencing Application provides rich conferencing experience for demanding users.
- Support both reservation-less and reservation based audio conferences.
- Customize each audio conference room per your requirements, e.g., select entry tones, select memorable vanity PINs, turn recording on/off, select enter audio conference muted on/off, select Moderator presence required or not etc.
- Schedule recurring audio conferences via the Web Portal. Use Microsoft Outlook iCalendar application to send invitations to desired participants. Use Microsoft Outlook iCalendar application to send invitations to desired participants.
- HTML-5 based Web Portal for seeing real time view of a running audio conference. See/edit Participant's name on the Web Portal. PC and iPAD compatible.
- Display loudest speaker. Allows the identification and muting of a participant who may be inadvertently injecting noise into the audio conference.
- Exercise multiple in-conference controls via phone key presses or the Web portal.
- Auto mute noisy lines or lines with excessive echo.
- Merge two or more audio conferences into one without dropping any calls. Transfer participants between conferences.
- Send a detailed end of conference summary report to the moderator after a given audio conference is over.
- Record entire conference or excerpts from a conference and playback via PC's media player
- Trigger a dial-out conference based on a) incoming phone call, or b) click on a web portal
- Support unlimited number of call out groups
- Send a greeting message prompting recipients to join the conference (Select communications medium to be used for message delivery (Voice only, Email only, or both)
- Schedule one time or recurring dial out calls
- Provide summary and detailed reports on call completions (Busy, No Answer, Answering machine etc.)
- Usage reporting

Web Conferencing Application

Web Conferencing Application is designed to significantly boost the productivity of your meetings.
- Web based application, Client download required only for the Presenter
- Web Browser: Internet Explorer 8 and above, Chrome, Firefox, Mac Safari
- Desktop sharing
- Application sharing

- Participant control sharing
- Instant messaging
- Bandwidth optimization control
- Detachable windows, dual monitor support
- Webinar support – stream Microphone audio and Webcam video while sharing Desktop or an Application
- Usage reporting

Mass Notification Application

The Mass Notification Application is designed to send multi-modal messages to thousands of people during emergency and non-emergency situations.

- Select one or more communication mediums to be used for message delivery (Voice only, Email only, SMS using SMTP, etc.)
- Use built-in 'Find-you' capability to increase the probability of delivering a message.
- Multiple automatic retries of uncontacted members
- Control the speed of dialing out.
- Display real time call activity and a progress bar on a Web Portal.
- Abandon a Group Alert in progress via web portal or through DTMF.
- Provide summary and detailed reports on call completions (Busy, No Answer, Answering machine etc.)
- Usage reporting
- Deliver voice messages to 3C Internal Zone Paging Groups. **(Applicable to U3C only)**
- Deliver Text Message to NEC IP Phones located on the LAN. **(Applicable to U3C only)**

Connect to 3C via Web Services and perform scheduled synchronization of 3C users, IP Addresses and MAC Addresses of IP Phones, 3C Emergency Groups. **This requires a license for the NEC IP Phone Text Messaging Manager.**

- The NEC IP Phones must be on the Local Area Network and not using Network Address Translation (through an SBC)
- The NEC IP Phone must have its Push Server Application turned on and pointed to the IP Address of the NMC. This can be done in two ways: 1) via the phone by going into Admin Settings, Applications, Push Server; 2) by creating a customer config file and adding the appropriate settings to enable and point the phone push server to the NMC – refer to Appendix within this document for the procedure to follow on setting this up.

The NMC can be used to send SMS blast via an external carrier SMSC. **This requires a license for SMS Platform Extension**.

- Deliver thousands of text messages to cellular phones quickly
- Requires end customer to have access to a carrier SMSC that supports SMPP 3.4 or HTTP protocol

IP Phone Location Manager Application

The NMC Phone Location service can determine the location of the port and Ethernet switch where the IP phone is connected.

Connect to 3C via Web Services and perform scheduled synchronization of 3C users, IP Addresses and MAC Addresses of IP Phones, 3C Emergency Groups

- Search Network POE switches MAC Address Tables on scheduled basis using SNMP V2 and V3 to identify moves of IP Phones
- Automatically move IP Phones from one 3C Emergency Group to another based upon identified POE switch location change and NMC administrator POE switch to 3C Emergency group association
- Populate the correct Caller ID associated with the Emergency Group on a call going to 911
- Provide report output of synchronized information upon completion of a synchronization
- Not supported items are as follows:

- Soft Media Phone (SMP) moves as they do not have a MAC Address as in the normal IP Phone MAC Address. This includes SMPs on PC's and on mobile devices
- Wireless Phones
- POE switches that do not support MAC Table Address scans via SNMP Community String access

This NMC service is priced per POE switch or per 48-port module, whichever is smallest, to be scanned for IP Phone MAC Addresses. A minimum of two (2) switches or two (2) 48-port modules for scanning is required for purchase up to 30 switches or 30 48-port modules, after which no additional charge is required.

Platform Extensions

The NMC provides additional Platform Extensions that can be licensed separately. These platform extensions can be used to further enhance the operation of the Value Added Services applications available on the NMC.

- **Light weight Data Access Protocol (LDAP)** – allows synchronization of NMC groups with groups set up on Microsoft Active directory.

- **High Availability – Active/Standby** - The database of the Primary NMC is replicated to the Secondary NMC in real time. The upstream Switch/IP PBX/SBC can be set up to automatically route the traffic to Secondary NMC if the there is a network or equipment issue with the Primary.

- **Enhanced Security** – Adds multiple Information Assurance capabilities (e.g., strong passwords, intrusion prevention etc.)

- **Short Message Service (SMS)** – Provides ability to interface with a Carrier based SMSC system. This can be used for adding SMS blast capability to the Mass Notification application.

- **SNMP** – Allows external Network Management System (e.g., HP Open View) to ascertain health of the NMC using SNMP V2/V3 protocol. Also, pertinent errors/faults can be logged in an external SYSLOG server.

Required Licensing

On the UNIVERGE 3C system, the following licensing is required:
- Trunk Access License (TAL, part number BE116814 per trunk required) for each SIP Port configured on the NEC Meeting Center when integrating with UNIVERGE 3C system. The NMC uses Dialogic SIP Licenses to interface to the 3C TAL ports.
- If synchronizing with the UNIVERGE 3C for NEC IP Phone Text Message sending or for IP Phone Location Services, a User Access License or Subscriber Access License (UAL or SAL, part number BE111898 or BE111892) to allow user to be setup in Microsoft Active Directory and within UNIVERGE 3C for web services access.

On NEC Meeting Center, the following licensing is required:

- Maximum quantity of simultaneous audio conference ports.
- Maximum quantity of simultaneous web conference ports.
- Maximum quantity of simultaneous mass notification ports.
- Maximum quantity of simultaneous system ports that might be in use at any one time depends upon the number of audio conference and Mass Notification ports in use. Example: a 48 port NMC can support 20 ports for audio conferencing and 28 ports for Mass Notification simultaneously. If no audio conference is in progress then all 48 ports can be used for Mass Notification and vice versa.

- The NMC LDAP (Lightweight Directory Access Protocol) package allows the NMC to be interfaced to corporate directory such as Active Directory in order to populate the NMC Address Book and Groups. This is a separate licensing option and is priced on a per NMC system port basis up to the first 240 ports (sum of all ports specified for Audio, and Mass Notification ports). For systems supporting more than 240 ports, there is no additional charge. In other words, there is only a charge for the first 240 ports.
    - o If selecting this option, we highly recommend that Professional Services be utilized the first few times you implement.

- For attaining High Availability two NMC servers can be deployed in Active/Standby mode. The HA option is priced on a per NMC system port basis up to the first 240 ports (sum of all ports specified for Audio, and Mass Notification ports). For systems supporting more than 240 ports, the charge is limited to up to first 240 ports.
    - o On Active/Standby, if you need 300 simultaneous ports, you must purchase 600 simultaneous ports, 300 for each server. The benefit of this option is that it provides complete failover support to the Standby server in case there is any network or equipment issue with the Primary server.
    - o If selecting this option, we highly recommend that Professional Services be utilized the first few times you implement.

- The NMC Enhanced Security Package adds multiple Information Assurance capabilities to the platform. It also adds a digital certificate so that the systems web portal can be accessed using HTTPS. Any attempts for hacking either through the web portal or via voice path lead to account getting locked and that can only be unlocked by system admin. This is a separate licensing option and is priced on a per NMC system port basis up to the first 240 ports (sum of all ports specified for Audio, and Mass Notification ports). For systems supporting more than 240 ports, there is no additional charge for the High Availability option. In other words, there is only a charge for the first 240 ports.
    - o If selecting this option, we highly recommend that Professional Services be utilized the first few times you implement.

- The NMC SMS (Short Message Service) Package allows the NMC to be interfaced to a Cellular Carrier's SMSC. The Customer must work with a Carrier to provide this capability to their system. This is a separate licensing option and is priced on a per NMC system port basis up to the first 240 ports (sum of all ports specified for Audio, and Mass Notification ports). For systems supporting more than 240 ports, there is no additional charge for the SMS option. In other words, there is only a charge for the first 240 ports.
    - o If selecting this option, we highly recommend that Professional Services be utilized the first few times you implement.

- The NMC SNMP Package allows external Network Management Systems (NMS) to interface to the NMC system. The NMC supports SNMP V3 compliant GET/SET and TRAPs. This capability is used by a NOC to ascertain the health of the NMC server, its various components and associated Network interfaces. The NMC can also send pertinent errors and fault conditions to an external SYSLOG server. This is a separate licensing option and is priced on a per NMC system port basis up to the first 240 ports (sum of all ports specified for Audio, and Mass Notification ports). For systems supporting more than 240 ports. In other words, there is only a charge for the first 240 ports.
    - o If selecting this option, we highly recommend that Professional Services be utilized the first few times you implement.

Calculating Required Ports for Mass-Notification

Regarding Mass Notification and determining how many ports a customer needs, is based on the following combinations:
- How long their greeting message is
- How long their message body is
- How many times do they estimate a phone will ring before someone answers (estimate 6 seconds per ring cycle)
- How many different telephone numbers will be dialed before one individual is reached (NMC allows up to 4 telephone numbers to be dialed. If the person does not answer on first number, NMC can second, then third and finally the forth number to try and get an answer).
- How many times will they allow individuals who have answered a notification to replay the message body

- If the NMC dials all the telephone numbers for a party and they have not answered the call yet, how many times should NMC attempt to call "unreached parties"
- How many people do they need to notify via a voice call
- How fast do they want all these people to be notified or put another way, within what time period must these people be notified

Within the NEC Anytime Studio the below methodology presented from an Excel sheet is available next to the Mass Notification Port entry question. Here is an example of this Excel Sheet input:

Items to consider	Input Quantity	Unit of Measurement	Notes
Greeting Time	6	Seconds	If Greeting/Notification is to be played to all callers
Message Time	15	Seconds	Message time to be played
Ring Time	18	Seconds	Ring Time until recipient answers call
Quantity of Phone Numbers called per "party to be called"	2		On average, quantity of phone numbers that will be called per "party to call" before the party answers and receives the notification
Quantity of times to replay message	1		Average Quantity of times to replay message body if the called party selects to have the message replayed
Quantity of times to retry called parties if they do not answer any of their numbers this first time through	1		Quantity of times to retry unanswered calls
Quantity of parties to call	1000		Number of people to be contacted via voice call
Time Period within which to complete all calls	60	Minutes	Time within which to call all voice recipients
Quantity of Ports Needed	**18**		

Table 1: Mass Notification Port Calculations

Note, the minimum quantity of NMC system ports is 8 but you can have any quantity of Mass Notification ports up to 1,000. The quantity of System ports must be equal to or greater than the greatest quantity selected for Audio, Emergency or Mass Notification ports.

Training

NMC Technician Training

To receive technical support on the NEC Meeting Center Application, your technicians must be certified. Certification Training is online within MyNEClearning.com and is free of charge. Within MyNEClearning, type NEC Meeting Center into the search dialog box to register and take the online certification training as shown below:

In Search dialog, type in "NEC Meeting Center" and press "GO"

The NEC Meeting Center online training for Release 8.0 is under development

NMC End-User Admin Training

NEC Meeting Center end-user online administration training can be found at
http://www.myneclearning.com/video/externaltraining/index.htm:

Go to http://www.myneclearning.com/video/externaltraining/index.htm, scroll to bottom and select link to NEC Meeting Center

The NEC Meeting Center online training for Release 8.0 is under development

Integration Steps

STEP 1: Setup the NMC server and install the NMC Software Disks	Refer to "NMC Software Installation"
STEP 2: Configure network integration on the NMC Server, i.e. IP Address, Default Gateway, Host Names, etc.	Refer to "Network Configuration on NMC"
STEP 3: Begin administrative setup within the NMC application, i.e. load license file, input URL Host Names, define trunk interface to UNIVERGE 3C, input or import users, groups, etc. If connecting to 3C via Web Services, make sure user is setup in Active Directory and configure the PBX synchronization parameters.	Refer to "NMC Administrative Setup"
STEP 4: Configure integration within the UNIVERGE 3C system, i.e. SIP Trunks, Extension/DID numbers, etc. If using 3C Web Services for NEC IP Phone Text messages or for IP Phone Location Services, make sure user is created in Active Directory and define Web Service user in 3C.	Refer to "UNIVERGE 3C Integration Configuration"

Customer Site Requirements

The Table below lists items that need to be provisioned on a typical NMC system. This table should be completed before beginning the installation process.

Row #	Parameter Name	Parameter Value Example	Parameter Value for this Installation
1	IP Address of NMC	10.1.1.252	
2	Subnet Mask	255.255.255.0	
3	Gateway IP address	10.1.1.1	
4	Primary DNS address	10.1.1.211	
5	Secondary DNS address	8.8.8.8	
6	Admin GUI Hostname	nmc.acme.com*	
8	NTP Time Server address	pool.ntp.org	
9	Dial in Phone Number for the NMC	(972) 555 1212	
10	IP Address of SV 9100 (Circuit Group Address)	10.1.1.250	

Table 2: Customer Site Networking Parameters

*Note: The site network administrator will need to create a DNS entry that points the Admin GUI Hostname (e.g., nmc.acme.com) to the NMC's IP address (e.g., 10.1.1.252) or whatever the assigned address is for the specific installation). This is needed to allow users outside the office to access the NMC Web Portal by typing the hostname in the URL window of their browser.

STEP 1: NMC Software Installation

After setting up the NMC server physically, i.e. connecting power, rack mounting, connecting Ethernet connection to "Port 0/1", (you want to use the first Ethernet Port) on back of server, perform the following steps. Note: the NMC licensing is tied to the MAC Address of the Server. If in doubt as to which Ethernet Port matches the MAC Address on the license you received from NMC@necam.com, you can press F1 while server begins its boot-up to go into BIOS and identify the MAC Address of the Ethernet ports. The MAC address of the license is included in the file name of the ZIP File sent to you. Note, do not unzip the file. When it is loaded to NMC server it must be loaded in its ZIP Format.

1. Place Disk 1 of the NMC software package into the DVD Drive.
2. Power on the Server.
3. If loading the Disk 1 from an external DVD drive, rather than an internal DVD drive, when the splash screen appears, go into the BIOS setup and select "Boot-up" from the appropriate DVD drive. Save this configuration and then exit. Remember, after completing the installation, you will want to change the BIOS Boot-up process back to booting first from the hard drive.
4. When the notice/warning appears that all data on your system will be removed by proceeding, press enter and proceed.
5. Allow Disk 1 to continue loading. When it is complete, it will automatically eject from the DVD drive and the screen will provide a note that it is waiting for Disk 2 to be input. Disk 1 installation will take about 15 to 25 minutes.
6. At the message, "Waiting for Disk 2", remove Disk 1 and insert Disk 2 into the DVD drive and press "Enter".
7. Allow Disk 2 to complete its installation. When it is completed, it will automatically eject and the system will re-boot.
8. After the reboot, you will be presented with a login screen to the Centos Shell. Login with the default username is **"confguest"** and password is **"itworks".**
9. Open the Web Browser found at the top of the Centos Shell and point it to http://192.168.0.207 (default IP Address for NMC Administration Page on the Local Machine). This will take you to the login to the NMC Administrator. Default username and password is "admin", "admin".

Figure 1: NMC Admin Login Page

STEP 2: NMC Network Configuration

This chapter provides the steps required for changing the default network settings to those applicable to the site as per Table 2. **Note, the NMC ships with a default IP address of 192.168.0.207.**

Changing the network settings

Go to Administration/Network Settings tab and enter the data from Table 2.

Enter the Hostname, IP address, Gateway IP address, Subnet Mask IP Address, and the Primary and Secondary DNS IP addresses. Press Apply.

Next, enter the System Clock and Time zone information. Press Apply.

Next, enter the Email Relay related information, Press Apply.

Next, enter the NTP server URL. Press Apply

Next, Press Reboot (found at bottom of screen shot below) for the new network settings to get configured on the NMC.

Figure 2: Network Setup Page

Now as the local networking parameters are configured on the NMC, connect the Ethernet cable to the local LAN. At this point you should be able to use any networked computer to access the NMC's web portal.

STEP 3: NMC Administrative Setup - Uploading Application License

Use a browser and go to NMC's IP address (e.g., http://10.1.1.205 in above case) and login as System Administrator.

Figure 3: NMC Admin Login Page

Use following credentials to log in:

Account Name: admin
Password: admin

Applying the NMC Application License

Click on 'Administration' Menu and the select 'Licensing'.
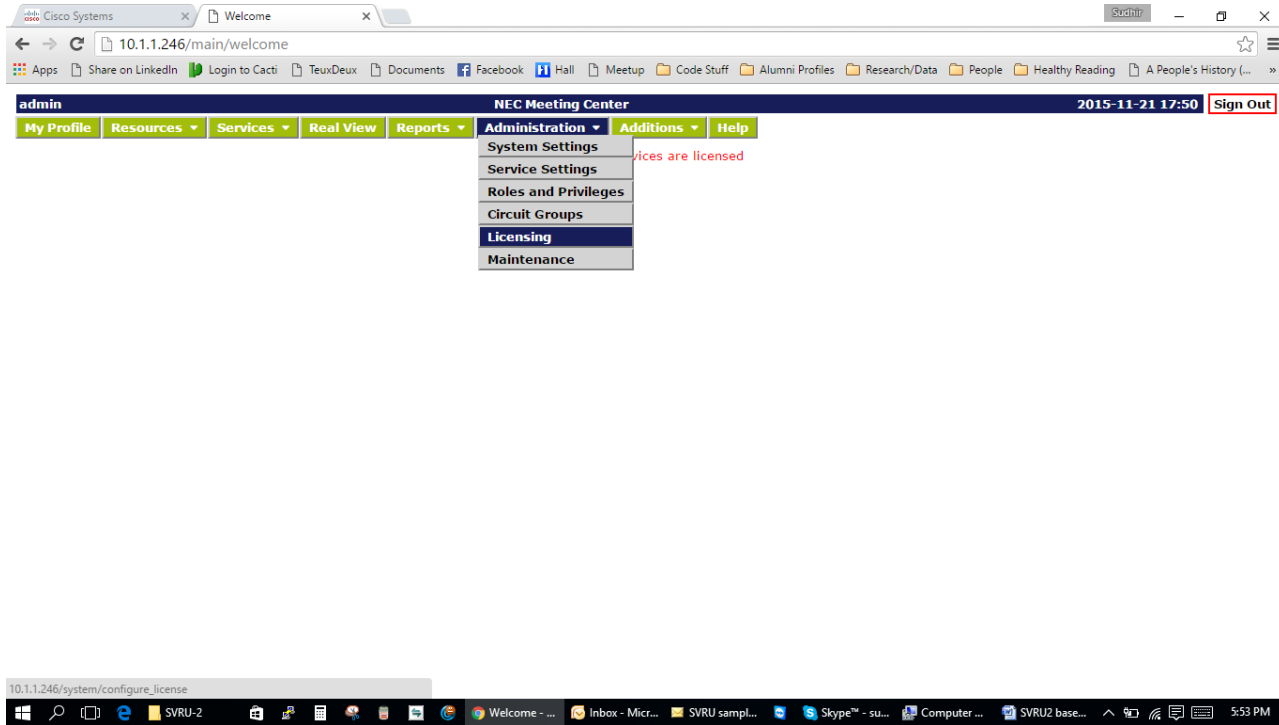
Figure 4: NMC Licensing Portal Access

Next, use 'Choose File' to point to the license file on your PC and then click on 'Upload'.
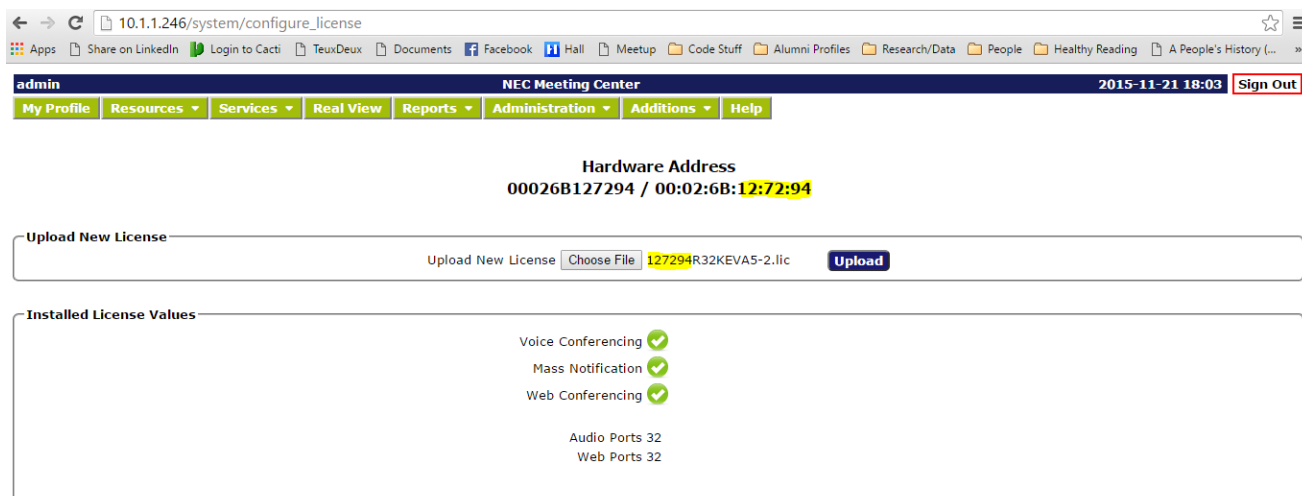
Figure 5: Uploading the License File

NOTE: The NMC's MAC address is also displayed on the web portal. The license file name contains 6 numerals that match the least significant 3 octets of the MAC address of the system. This helps an associate in determining that a correct license file pertaining to the NMC at hand is being loaded.

The upload process takes approximately 3 minutes. After the license is uploaded successfully, the portal will self-refresh and purchased number application ports will be displayed.

Configure NMC System Parameters

Go to the "General Settings" Tab.

Figure 6: System Settings Page

- **System Identification**
  - o **System description:** Any name that you would like to provide to your system
  - o **Server Name:** This should match the Host Name that you setup within the Webmin application under the "Configure Network Integration" section of this document. This is the URL that users will use to access the NMC for administrative purposes or as a "moderator"
  - o **Dial-in Number:** This is the telephone number that is dialed to access the NMC audio conferencing application. This field appears in the iCal file as the number to dial to reach the NMC
  - o **Time Zone:** Specify the default time zone used by the NMC
  - o **Upload New Logo:** If you would like to replace the NEC Logo with your own logo or the customer's, you may do so here. The Logo image to be imported should not be more than 120 pixels tall.
  - o **Upload New Welcome Prompt:** This is the opening welcome prompt that callers hear when calling into the NMC. You can record your own WAV File and upload here to customize for your company.
  - o **Web root page:** This determines the default login page (account login, web conference login etc.)
- **Voice Settings:** Enter appropriate voice settings for your configuration. Default originating number is used to populate the From field in outgoing invites
- **Resource Constraints:** Specify any resource constraints you desire
- **VoIP Settings:**
  - o **Stack Address:** Enter the IP Address of the NMC Server

14

Set up a SIP Trunk between U3C and the NMC

1. Go to "Administration" and select "Circuit Groups". Press the "ADD" button to add a new Circuit Group. The "Edit Circuit Group" screen will appear. Assign a name for this circuit group, select "SIP Trunk" in the Circuit Group Type field and input the IP Address of the UNIVERGE 3C and the port number (e.g., 5070) that you wish to connect with.

Figure 7: Setting Up a SIP Trunk

Circuit Group Type: On UNIVERGE 3C "Circuit Group Type" should be "SIP Trunk". On SV system, "Circuit Group Type" would be "SIP Extension".

Transport: Should be set to "UDP".

Circuit Group Address: This is the IP Address to your communications system, SV or 3C.

Realm: This can be left blank in most cases.

User Name and Password: If your system requires User Name and Password for registration to your SIP Trunks or to your SIP Extensions, input that information here.

15

Set up Administrator Profile

2. Go to "Account Profile" so you can update and change the Administration Login, password, phone number, email and other options available.

Figure 8: System Administrator Profile Page

At a minimum, update the Phone Number, Login and Password and Email address. It is recommended that you update all fields which are applicable. Page Size determines how many rows are presented on a web page such as under conferences or mass notification listings page.

3. If you are connecting NMC to 3C Web Services for purposes of sending Text Messages to NEC IP Phones during a Mass Notification or utilizing the NMC IP Phone Location services for automatic moves of IP Phones within 3C Emergency Groups, continue with Step 8, else you may go to Step 12.

4. Go to "Additions" and select "PBX Synchronization". Here you will define the Web Services user which you set up in Active Directory and in the next section of this document on the 3C system. This configuration is necessary to allow NMC to connect to the 3C system to perform synchronizations to gather information about users, phones, internal zone page groups and emergency groups.

Figure 9: U3C Web Services Synchronization Page

Service Address: This is the 3C UCM IP Address or URL based DNS SRV address.
Data extraction account name: This is the 3C UCM User Name on the 3C system that was setup and enabled for Web Services access. The fully qualified name should be used.
Data extraction account password: This is the Password setup in Active Directory for the 3C Web Services user. This password should be defined in AD as never to change.

5. If you are deploying NMC IP Phone Location services, you need to define the Network Switches that NMC should scan for IP Phone MAC addresses; If you are planning on sending Text Messages to the NEC IP Phones from Mass Notification application, you will need to setup the Push Server on the NEC Phones and point it to the NMC IP Address; Go to "Administration" and select "Network Switches". Here you will define the various network switches to which IP Phones may be connected. You will need to know their IP Address, what their port ranges are and their SNMP Community string required to allow NMC to access these switches to perform MAC Address Table scans. See screen shots on next page. Go to "Administration" Menu and select "Network Switches".

Administration > Network Switches

6. Once you have assigned the network switches and have completed the setup of the 3C as specified in the next section, you will want to have performed a synchronization of your 3C system to your NMC system. This is necessary before you can associate your defined switches to your 3C Emergency groups. Once this is done, go to "Resources" and "Groups". Here you will identify your 3C Emergency Groups, which will have a "Type" of "PBX Emergency". NMC will also discover 3C Internal Zone Page Groups and they will have a "Type" of "PBX Paging" (note, that in order for NMC to discover these groups, the Paging Address that you assigned under the Number Tab within the 3C Administrator must be input within the extension range to page within the 3C Address Group. This will be covered in more detail in next section). Refer to screen shot below. Go to "Resources" menu item and select "Groups".

7. If you are planning on sending **Text Message to the NEC IP Phones**, you must enable the Push Server on each phone to receive text messages and point the Push Server to the NMC IP Address. This can be done manually from each phone or it can be done in "mass" by creating a customer config file for the phones. Note, this requires that you have purchased the IP Phone Location Manager application. To set this up manually, go to each phone and do the following:
    a. Press the Menu Key and go to "Admin Settings"
    b. Input the NEC Phone Password (Default is 6633222)
    c. Go to "Application Settings" option
    d. Go to "Push Server" option
    e. Ensure that "Push Server Access" is enabled
    f. Go to "Server IP Address" and input the IP Address of the NMC server

Note: The NEC IP Phone must be reachable on the Local Area Network to which the NMC is located in order to receive text messages.

To configure the Push Server and the IP Address of the NMC server on the NEC Phones via the Customer Config File, please follow the instructions as found in the Appendix under, "Push Server Setup on NEC IP Phones from Phone Configuration File".

8. You can now proceed to setup and customize other elements of your NMC Solution. Refer to the online Help documentation. The steps above complete the necessary requirements to provide integration to your UNIVERGE 3C system, at least from the NMC side. Please continue to the next section to configure the UNIVERGE 3C system.

STEP 4: UNIVERGE 3C Integration Configuration

The following steps are to be performed within the UNIVERGE 3C Administrator application. This will setup the SIP Trunk and extension number which will connect to the NEC Meeting Center application.

1. Login into the UNIVERGE 3C Administrator
2. Go to the Trunks tab and right click within this screen to add a "soft-trunk" as shown below.
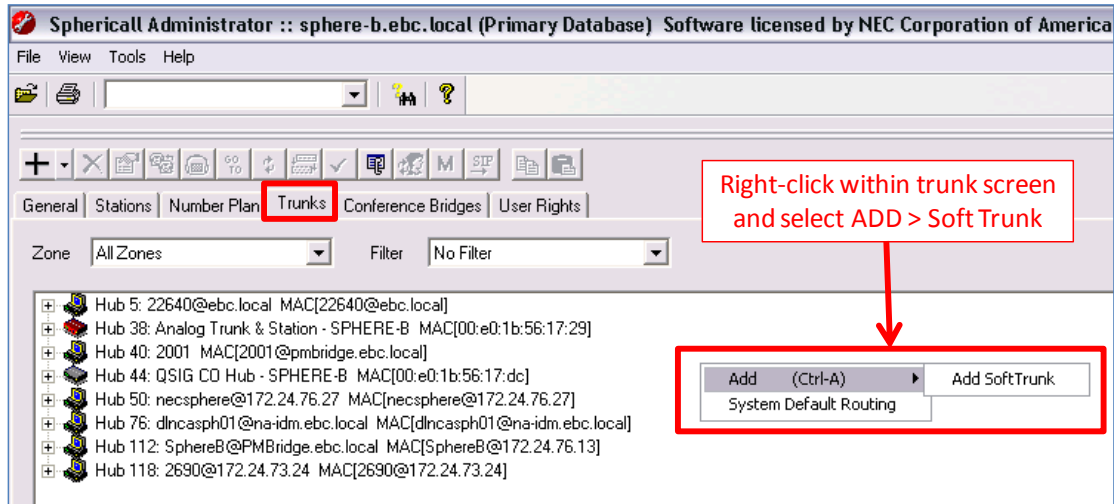
3. Once the soft-trunk dialog is opened, input the following information:
   - **Description:** Enter a name for this soft-trunk
   - **Account:** This can be the same name you entered above
   - **Service Provider Domain:** Enter the Domain Name of the network where the NEC Meeting Center is installed
   - **Outbound Proxy:** Leave blank
   - **Port:** This should be set to "5060"
   - **Registration Type:** Set this to "None"
   - **Primary MGC:** Input the "name" or the IP Address of the Primary UNIVERGE 3C media gateway controller
   - **Secondary MGC:** Input the "name" or the IP Address of the Secondary UNIVERGE 3C media gateway controller
   - **Preferred Transport:** Select "UDP" from the dropdown box.
   - **User Agent:** Select "Generic SIP Trunk" from the dropdown box if your 3C version is prior to 8.5.3.10. If your 3C version is 8.5.3.11 or higher, you must define a User Agent according to the user agent that the NMC is sending. Refer to next page for information on defining the User Agent on 3C Versions 8.5.3.11 or greater.

Define SIP Trunk User Agent on 3C Systems v8.5.3.11 or greater

1. Go to the General Tab within the 3C Administrator, right-click and select System Properties.
2. Go to the SIP Tab within System Properties
3. Press the Add Button and define the user agent fields as shown in the screen shot below (Dialogic SIP, All, Trunk, NMC User Agent)

4. Open up the SIP User Agent that you have created by double clicking on it. This applies to versions prior to 3C 8.5.3 and to versions later than 3C 8.5.3. In order for the NMC to see Caller ID information and for Service Selection rules to operate properly within the NMC, you must set the "SIP header number format" to "Internal". Once you have set this, press Apply and OK. Proceed to Assign Trunk Properties.

Assign Trunk Properties

1. Once you have clicked "OK" on the "Configure Service Provider" screen in "Step 3" above, double click on the "Port 1" or right-click and select "View Properties" on the Port 1. Go to the "General" tab and complete the information as shown in the screen shot below:

Assign "Name", Hardware ID (could be same as name), Select Telephony Area, Zone and input the total quantity of connections over this SIP Trunk (this would correspond to the quantity of TAL licenses you purchased to connect to the NEC Meeting Center
Make sure you have checked the box "In Service"

2. Go to the "Outward Routing" tab to setup the extension-number/DID-number that will be used for accessing the Audio Conferencing of the NEC Meeting Center.

When adding an "Extension" select either from an already defined extension or select "New Extension"

3. If you assigned a "New Extension" in Step 5 above, input the following information on the dialog that appeared under the General Tab (no other tab settings are required):

4. If you selected a pre-existing extension number in Step 5 above, go to the "Number" tab within the UNIVERGE 3C Administrator and right click on the extension you selected, select "View Properties" and make sure naming, etc. is setup as you desire and as specified in Step 6 above.
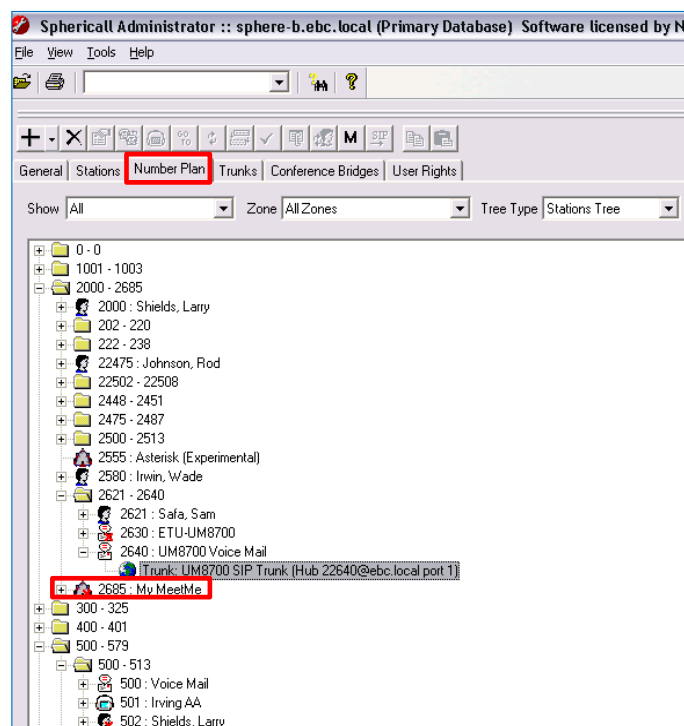
8. If you are doing Mass Notification and are planning on sending Text Messages to NEC IP Phones, you must create a Web Services user that the NMC can utilize to access the 3C Web Services for discovery of NEC IP Phone IP Addresses and internal Zone Paging Groups. Additionally, if you are utilizing the NMC IP Phone Location Services, you must have a 3C Web Services user created that NMC can utilize to access 3C Web Services for purposes of discovering IP Phone MAC Addresses and 3C Emergency Groups. A user must first be created in Active Directory. The Active Directory user should be setup so that the user cannot change their password and their password never expires. Once a user is created in AD, you now need to create the user in 3C. Go to the 3C Administrator and to the "Number Plan" tab. All users must have an address (dummy extension), so right-click in the Number Plan area and select "Add Extension".

9. Once the user has been added, and you have clicked on "Apply" from above, open up the user "Properties" dialog and go to the "General" tab. Make sure the settings are as shown below.

10. On the "Addresses" tab, make sure the "dummy extension" assigned is set as the "Preferred" address of the user. On the "User Rights" tab make sure that rights are granted to all "Zones" on the 3C system with "Full" privileges. This is to allow

25

the NMC to move stations from one Emergency Group to another when necessary and when using the NMC IP Phone Location Services.

11. If sending text messages to NEC IP Phones via 3C internal zone paging groups, you will need to make sure that the "Paging Address" that you assigned under the 3C Number Plan tab is also included in the "Address List" of the "Address Group" you created on 3C for the paging group. If the Paging Address is not included, NMC will not discover the paging group during synchronization.

Conclusion

This completes the initial integration of the NEC Meeting Center with the UNIVERGE 3C system. For additional information refer to the online help within the NMC system. Technical certification is required in order for NEC Partners to obtain support from NEC Technical Assistance. Certification training is available within www.myNEClearning.com. Refer to "Training" section at the beginning of this document for more information.

Appendix

Push Server Setup on Individual NEC IP Phones

1. If you are planning on sending **Text Message to the NEC IP Phones**, you must enable the Push Server on each phone to receive text messages and point the Push Server to the NMC IP Address. This can be done manually from each phone or it can be done in "mass" by creating a customer config file for the phones. Note, this requires that you have purchased the IP Phone Location Manager application. To set this up manually, go to each phone and do the following:
   a. Press the Menu Key and go to "Admin Settings"
   b. Input the NEC Phone Password (Default is 6633222)
   c. Go to "Application Settings" option
   d. Go to "Push Server" option
   e. Ensure that "Push Server Access" is enabled
   f. Go to "Server IP Address" and input the IP Address of the NMC server

   Note: The NEC IP Phone must be reachable on the Local Area Network to which the NMC is located in order to receive text messages.

Push Server Setup on NEC IP Phones from Phone Configuration File

1. Using the U3C Admin tool, open the desired station's properties window. In the station properties window, select **Create File**. The button's name will change to **Delete File**, and an entry will be made in the Custom File Parameters field indicating that you can add your custom settings to a file named dt-<MAC>-customer.cfg. Then press **OK**.

   NOTE: This procedure will create a file in the ftproot\necsdt700 folder with the name dt-<MAC>-customer.cfg. It will also modify the station's dt-MAC>.cfg file to include the name of the new file to be included for download by the station.
   You can now close the admin tool.

2. Open Windows Explorer and navigate to the Sphere\ftproot\necsdt700 folder.

3. In that folder find the file that was created above (dt-<MAC>-customer.cfg, where MAC is the MAC Address of the NEC phone you had created the cfg file on in Step 1). See next page for graphics.
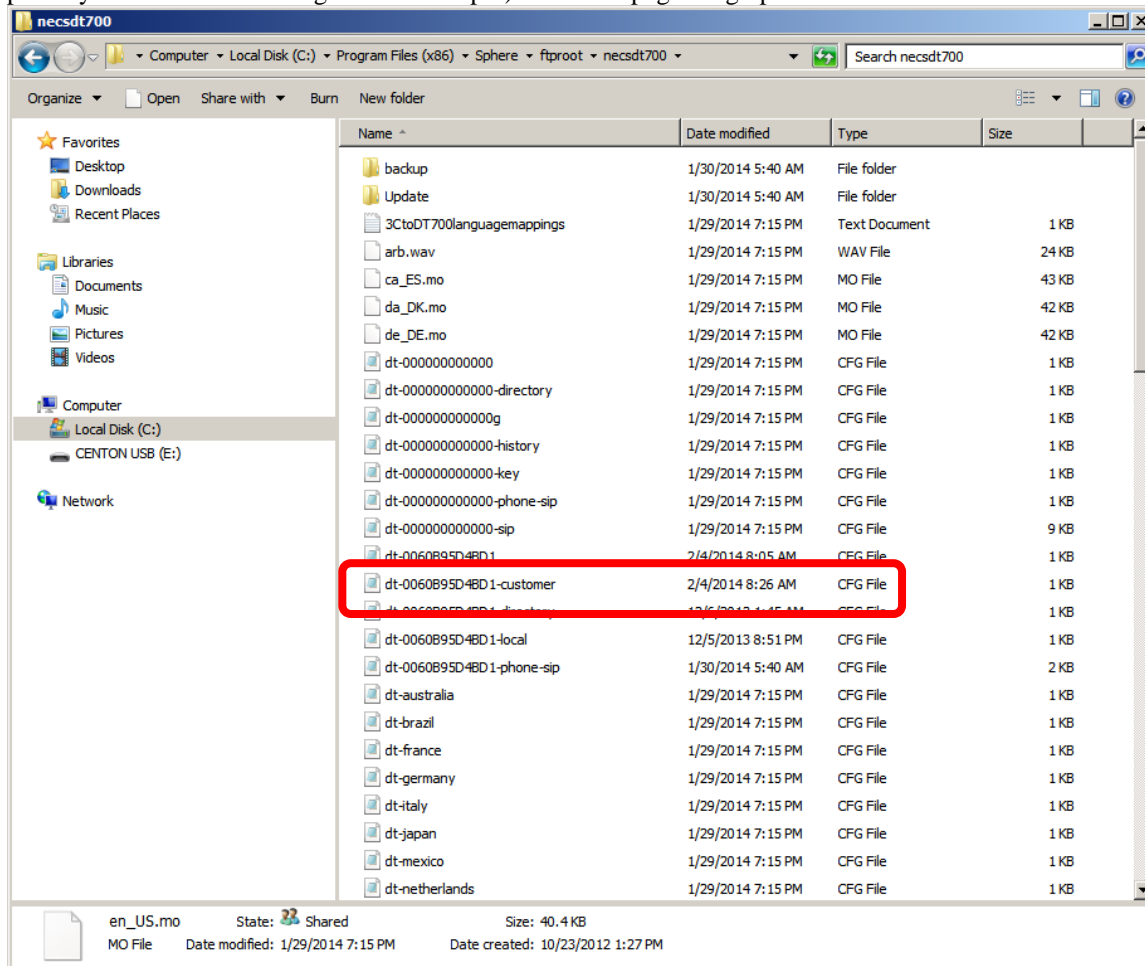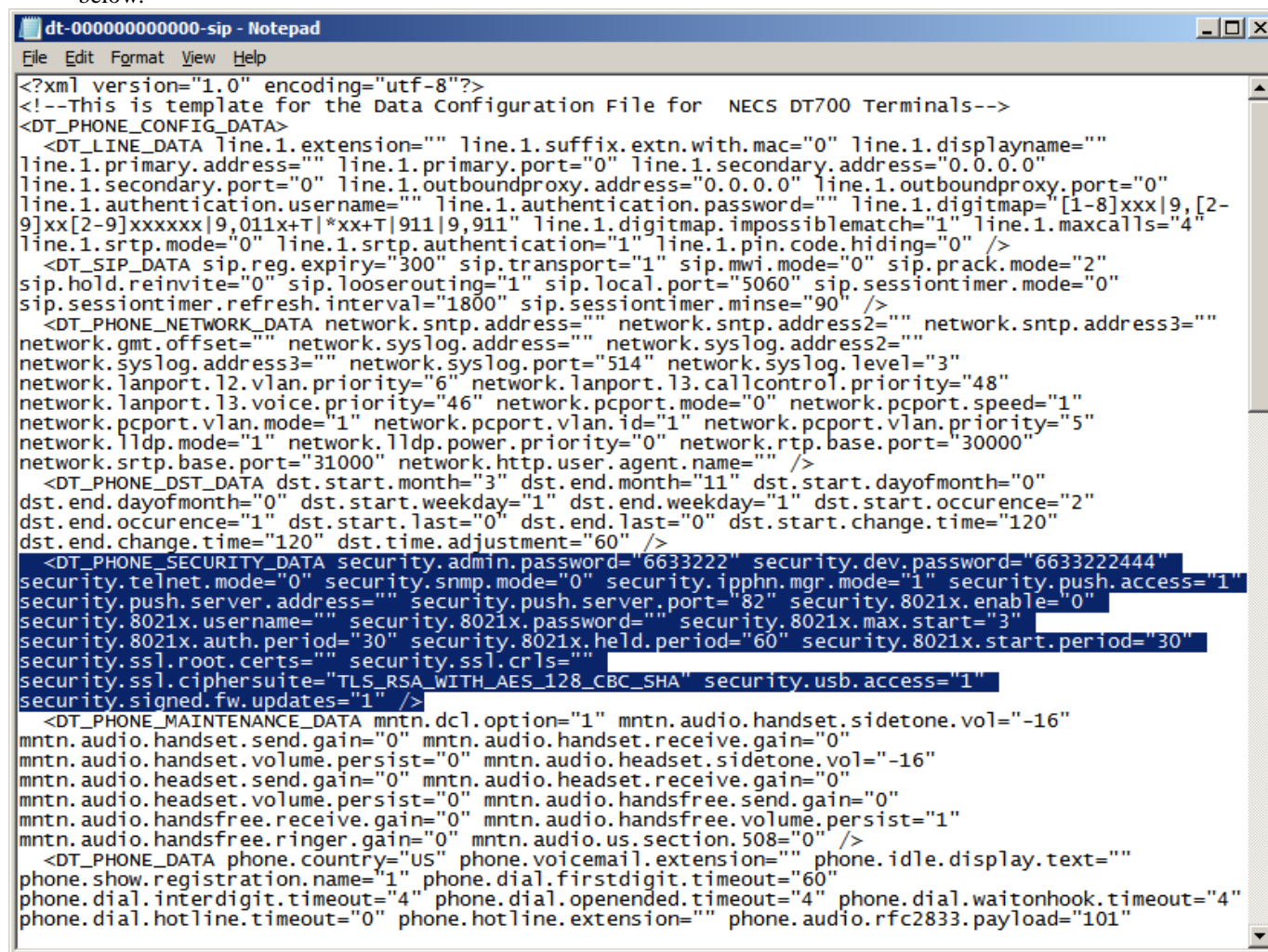
4. Open this file in a text editor.
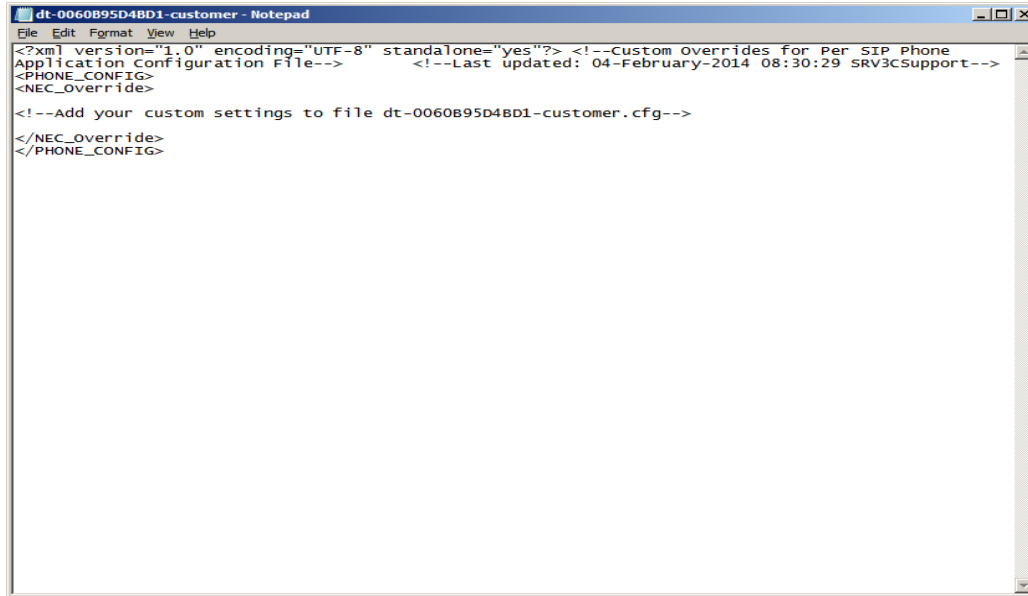
You will see that a blank file has been created with comment fields inserted in it. (I have entered carriage returns in the file to make it easier to read. Carriage returns do **not** affect the files ability to function as an xml config file.)
Since the file has no actual XML parameters, you will copy the parameters you want from one of the template files.

5. Minimize the existing file and with Windows Explorer, find the dt-000000000000-sip.cfg file in the ftproot\necsdt700 folder.

6. In that file you must find and highlight the desired parameters, in this case, the DT-PHONE_SECURITY_DATA section. See below.

7. Once you have highlighted the desired parameters, right click and COPY the highlighted section.

8. Now open the original dt-<MAC>-customer.cfg file and insert (Right-click > Paste) the new section, in between the "<NEC_Override>" and the "<!- - Add your custom settings to file dt-<MAC>-customer.cfg - - >" comment section. See below.

9. Once you have pasted the information, you can clean up the file by doing three things:
   A. Delete the comment "<!- - Add your custom settings to file dt-<MAC>-customer.cfg - - >".
   B. Delete all security settings not needed for this customer/station. For example: the Push server only needs three settings:
      1. The security.push.access = "1"
      2. security.push.server.address = "x.x.x.x"
      3. security.push.port = "82"
   C. Finally, make sure to add any setting that may be black that is needed, such as the real IP Address of the Push server.

10. See below for final version of the file.

   NOTE: Depending on the customer's needs, other parameters may be included as needed as long as they follow the standard xml format with headers (including start headers and end headers for sections).

   For more detailed information on the various configuration files that can be used when setting up SIP Phones, refer to the U3C documentation, "DT700 Administrator Guide – 3C" and especially the "DT700 Administrator Guide – Core". You can search in both of these PDF's by doing a Control F for find and inputting the key words of "Configuration File".

```
dt-0060B95D4BD1-customer - Notepad

File  Edit  Format  View  Help

<?xml version="1.0" encoding="UTF-8" standalone="yes"?> <!--Custom Overrides for Per SIP Phone
Application Configuration File-->        <!--Last updated: 04-February-2014 08:30:29 SRV3CSupport-->
<PHONE_CONFIG>
<NEC_Override>
  <DT_PHONE_SECURITY_DATA security.push.access="1" security.push.server.address="192.168.0.6"
security.push.server.port="82"  />
</NEC_Override>
</PHONE_CONFIG>
```

11. You must now save this file back into the Sphere\ftproot\necsdt700 folder.

12. Once saved, you must reboot the phone to force it to download the new set of config files.

   NOTE: You can confirm the settings in the UNIVEERGE 3C server by returning to the station Properties window for that station and looking in the NEC tab. In the Custom File Parameters field you will see the changes that were made to the file.

   You can confirm the settings in the telephone by going to Menu>> Admin Settings. Log in as Admin, password = 6633222. Then go to 5 – Application Settings followed by 1 - Push Server. Both Push Server Access (Enable/Disable) and the IP Address can be confirmed. The Push Server port cannot be verified via the telephone.