Auto-Update-Guide-snom-SIP-to-UC-Edition-for-Lync

Three simple steps to roll out the Lync compatible snom UC Edition to devices with SIP firmware (out-of-the-box)

Contents

Three simple steps to roll out the Lync compatible snom UC Edition to devices with SIP firmware (out-of-the-box) 1

Intro 3

Notes and limitations: 3

Step 1: Upload the snom CAB files to Lync Update Service 4

Step 2: Store template XML files in Lync server (IIS), optional edit them in advance 5

The firmware XML file, ... 6

The configuration XML file, ... 7

Step 3: Define and configure DHCP vendor specific options 9

Define vendor classes for each device model 10

Set Predefined Options 11

Configure the DHCP Server with Option 43 13

Ready-to-roll: Verify the environment preparation with a few devices 16

Troubleshooting 17

Intro

With this guide the Lync environment already in place can be prepared to perform the software switch from the snom SIP firmware (out-of-the-box) to the Lync compatible UC edition in three simple steps. There is no need for any third party provisioning server or access to the Internet for the snom devices. The steps in this guide are verified as working with standard SIP firmware version 8.2.29 as minimum. Devices equipped with this or higher standard SIP firmware versions will support this upgrade mechanism too.

The overall process is:

1) Upload the snom firmware CAB files to Lync Update service via Lync PowerShell

2) Store template XML files in Lync server (IIS), optional edit them in advance

3) Define and configure DHCP vendor specific options

Please note: when the devices are running UC edition (8.8.1.11 or higher) all further updates can be performed natively via Lync Server Update Server, managed via Lync PowerShell or Control Panel as described in the Apollo documentation available via your personal firmware portal.

Important advice: the snom devices will auto-upgrade from standard SIP firmware 8.2.29 (and higher) to the UC edition as described in this guide only:

- if placed into an environment which is prepared and verified as working following this guide
- and if the devices are unpacked out of the box directly into such environment.

If the devices were unpacked and booted in another network before, a manual factory reset of each device will be necessary to initiate the update process. Do prevent such overhead it is strongly recommended to unpack the devices in mass rollouts only if the preparation phase is complete and the setup is verified as working.

Notes and limitations:

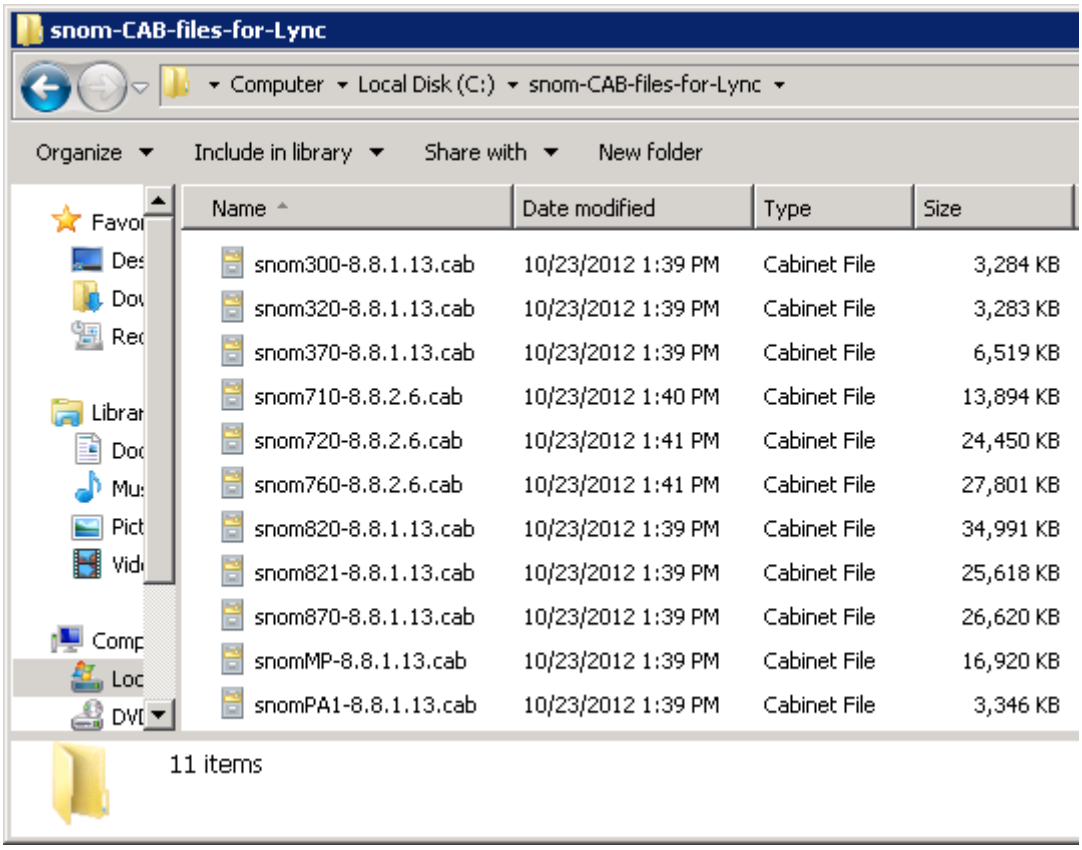
After the switch to UC Edition the snom devices can be signed in to Lync Server instantly via Extension & PIN if the environment supports it. For more details and guidance please refer to our Apollo documentation (available via your personal firmware portal) and the section “Extension and PIN sign". Alternatively the sign in process via SIP address and NTLM (AD-Domain) credentials can be used.

The firmware update mechanisms used here will only allow performing a firmware switch from standard SIP to UC edition inside internal network. When the switch to UC edition (8.8.1.11 or higher) is done further software updates can also run externally via the native Lync update mechanism.

Step 1: Upload the snom CAB files to Lync Update Service

Snom provides Lync Update Service compatible firmware cabinet (.CAB) files in your personal firmware portal. If already registered, the login can be performed with your email address and your password. A new registration can be done via: http://www.snom.com/en/lync.

It is recommended to collect the latest version CAB files for the designated devices in one folder on the Lync server (can be a SE/FE Frontend or Director) like in this example with version 8.8.1.13 and 8.8.2.6:



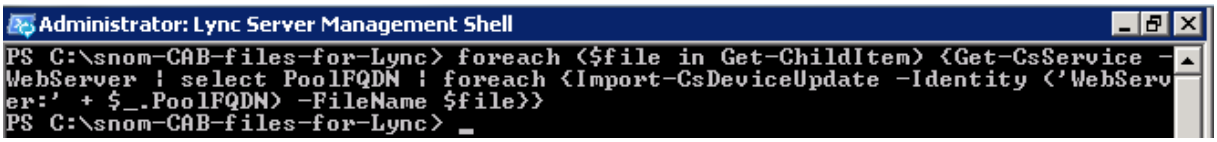
In general the snom firmware cabinet files can be uploaded by using the Lync PowerShell command Import-CSDeviceUpdate as described in TechNet: http://technet.microsoft.com/en-us/library/gg398861.aspx

Hint: To ensure that all update files from the current folder (in CSPowerShell) are uploaded to all Lync Device Update Service equipped IIS-Webservers, run this command.

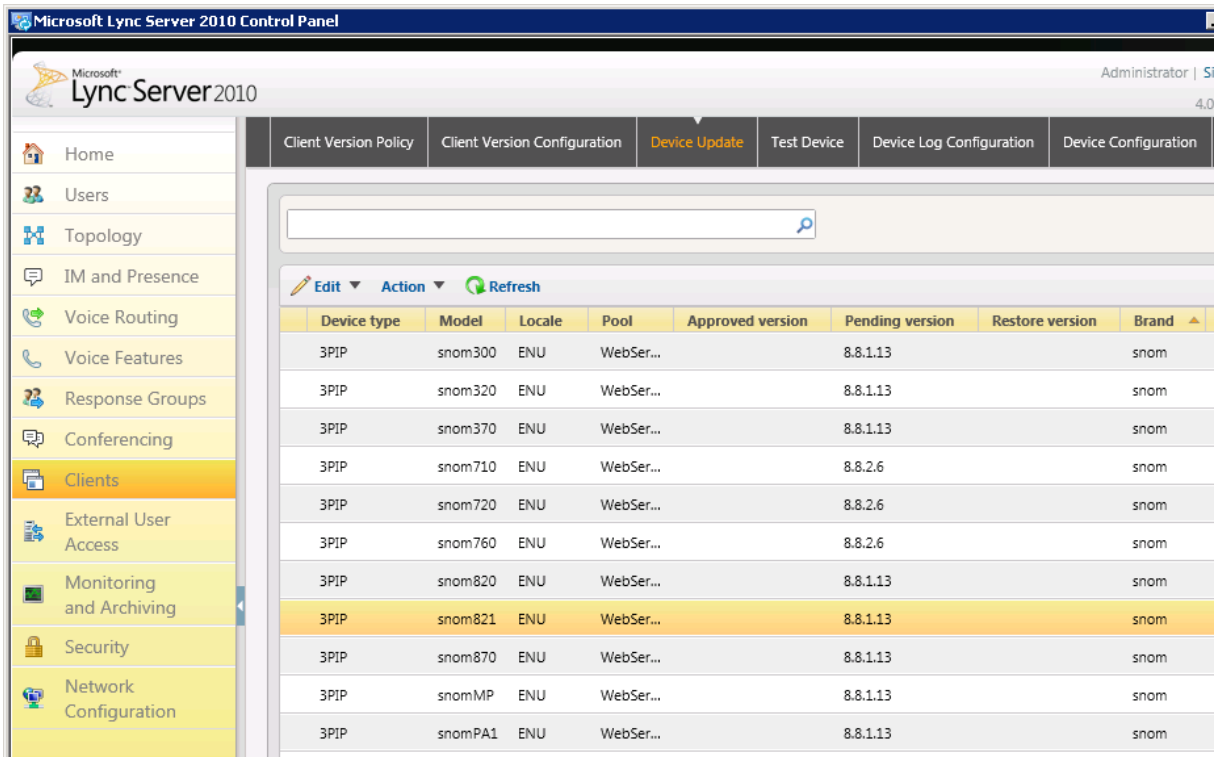
foreach ($file in Get-ChildItem) {Get-CsService -WebServer | select PoolFQDN | foreach {Import-CsDeviceUpdate -Identity ('WebServer:' + $_.PoolFQDN) -FileName $file}}

This command can also be executed in single server installations (Standard Edition, Enterprise Edition), where there is typically only one Lync Device Update Service.

For the example (all files are in the folder C:\snom-CAB-files-for-Lync) the following command would import all files to all services:



In the Lync Control Panel – on the Device Update page, the uploaded version is listed under pending version.



Please note: It is not necessary to approve the uploaded versions for the process described here. With the upload of the CAB files the Lync server (the built-in IIS) becomes the firmware repository the devices will be directed to with the next two steps independent of the approval status in Lync.

Step 2: Store template XML files in Lync server (IIS), optional edit them in advance

In typical Lync deployments just storing the XML template files in Lync server (IIS) as described is enough to complete step 2.

Optional editing should be considered carefully, if it cannot be avoided and with reviewing the comments in the files.

Note: Editing the template XML files can easily lead to typos or creating issues due to line breaks / word wrap and similar. Please never copy example XML content from this guide in an XML file and review the content of the XML files carefully if the process seems to be broken during verification.

A couple of a firmware XML file and a configuration XML file need to be stored for each device type to Lync server.

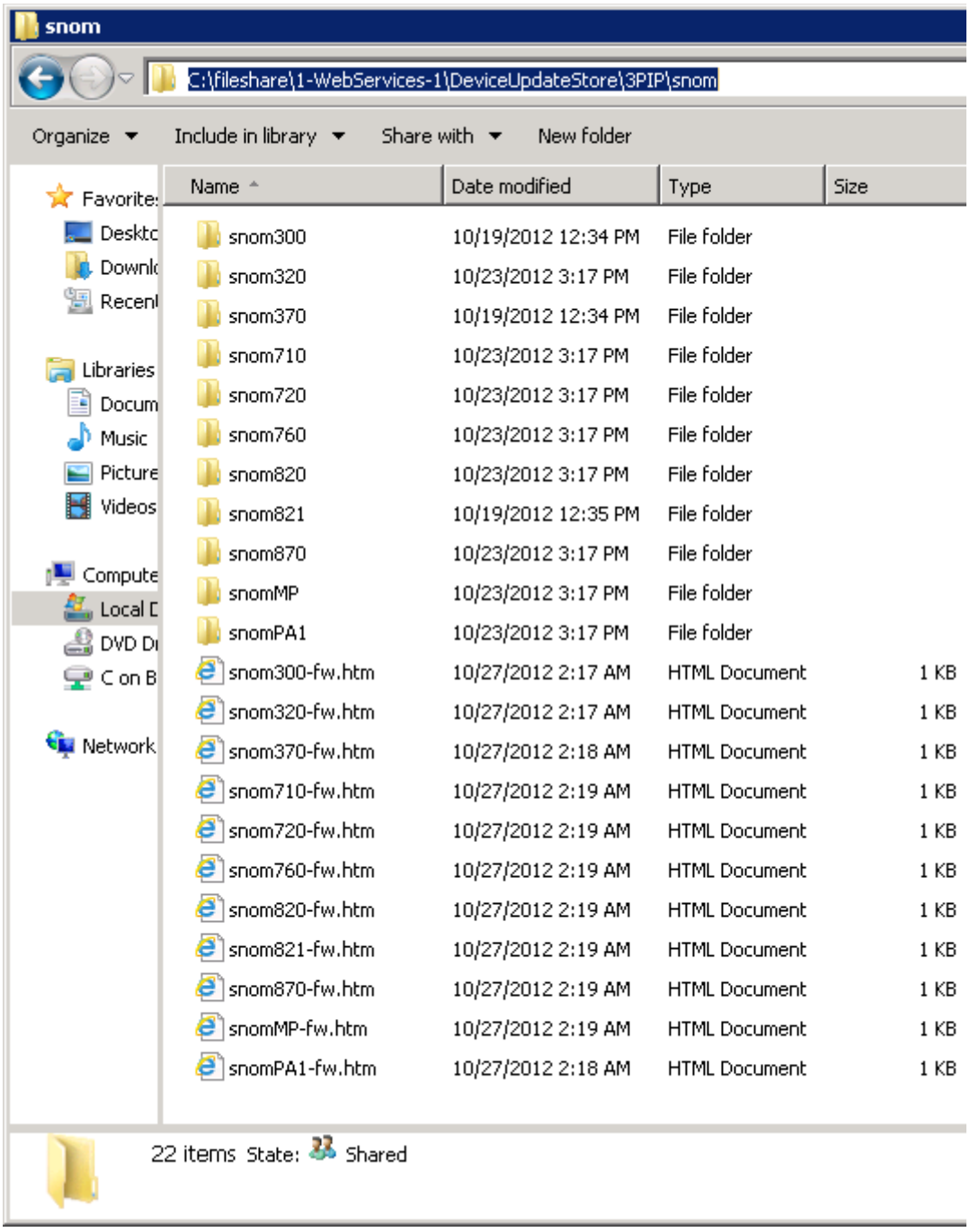
The firmware XML file,

directs the devices to the UC edition firmware stored into Lync server in step 1. Snom provides a collection of such XML files as templates that can be easily adapted via:

http://downloads.snom.com/snomuc/documentation/snom-Lync-firmware-XML-templates.zip

It is recommended to download the ZIP file and extract its content in this folder on Lync server:

C:\fileshare\1-WebServices-1\DeviceUpdateStore\3PIP\snom\



Please note: this is a default path available after snom CAB files are already uploaded via Lync PowerShell. If it does not exist, please check if the upload was not performed or the path / folder names were customized during Lync deployment and adapt your repository location accordingly. The root folder “C:\fileshare” above is just an example, that can have a custom name, but correlating folder structures like “\1-WebServices-1\DeviceUpdateStore\” are hard-coded in a Lync environment.

This is an example of the content of one of those templates, this case for a snom 300 (filename snom300-fw.htm):

```
<!-- Please do not edit this file, before you read the comments for each section! -->

<?xml version="1.0" encoding="utf-8" ?>
<firmware-settings>

<!-- Following settings will direct the device to the UC edition firmware stored in Lync Server-->
<!-- The variable {prov_host} represents the server FQDN the device detects via DHCP vendor specific option 66 (encapsulated in 43). -->
<!-- Please edit {prov_host} to an FQDN or the path to the firmware CPE.nbt file only, if it is not stored as documented and adapt it to your designated repository! -->

<firmware perm="$">http://{prov_host}/RequestHandler/Files/3PIP/snom/snom300/AB/ENU/8.8.1.13/CPE/CPE.nbt</firmware>
</firmware-settings>
```

It is optional to edit the highlighted parts in the firmware URL according to the Lync environment in use and (or) the firmware version uploaded to Lync server via the CAB files in step 1.

a) The variable for the Lync server (EE / SE Frontend or Director) named {prov_host} here only needs to be adapted to your designated Lync FQDN as described in the XML comments. In large Lync deployments / network infrastructures it is recommended to direct to a Lync Update service equipped server that’s close and fast connected from the device network perspective. So a mass rollout of firmware must not occupy a WAN connection for example.

b) The placeholder for the UC edition firmware version, here 8.8.1.13 needs to be adapted to match the version you uploaded via CAB files (only if a higher or lower version was used).

It is recommended to edit such values as needed and save the file without changing the filename. If the filename is changed, it needs to be changed accordingly in the next XML file that contains the URL directing to it.

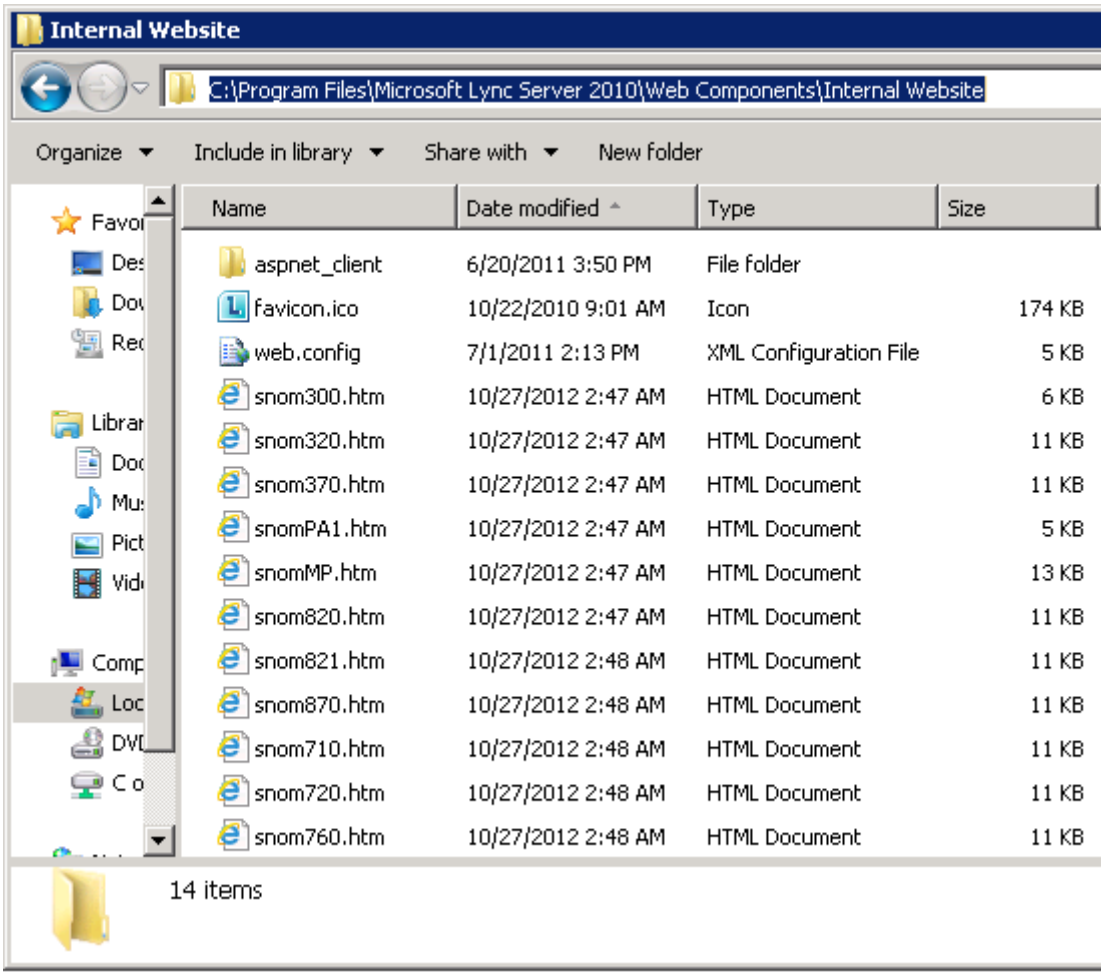
The configuration XML file,

directs the devices to the corresponding firmware XML file. Snom provides a collection of such XML files as templates that can be easily adapted via:

http://downloads.snom.com/snomuc/documentation/snom-Lync-configuration-XML-templates.zip

It is recommended to download the ZIP file and extract its content in this folder on Lync server:

C:\Program Files\Microsoft Lync Server 2010\Web Components\Internal Website\
(for Lync **2013**: C:\Program Files\Microsoft Lync Server **2013**\Web Components\Internal Website\ )



Please note: this is a default path available after a standard Lync installation. If it does not exist, please check if it was customized during Lync deployment and adapt your repository location accordingly.

This is an example excerpt of the content of one of those templates, this case for a snom 300 (filename snom300.htm):

```
<!-- Please do not edit this file, before you read the comments for each section! -->

<?xml version="1.0" encoding="utf-8" ?>
<settings>
<phone-settings e="2">

<!-- Following two settings will allow the SIP firmware auto-switch to UC Edition stored in Lync Server-->
<!-- The variable {prov_host} represents the server FQDN the device detects via DHCP vendor specific option 66 (encapsulated in 43). -->
<!-- Please edit {prov_host} to an FQDN or the path to the firmware XML file only, if it is not stored as documented and adapt it to your designated repository! -->
```

<update_policy perm="$">auto_update</update_policy>
<firmware_status perm="$">http://{prov_host}/RequestHandler/Files/3PIP/snom/snom300-fw.htm</firmware_status>

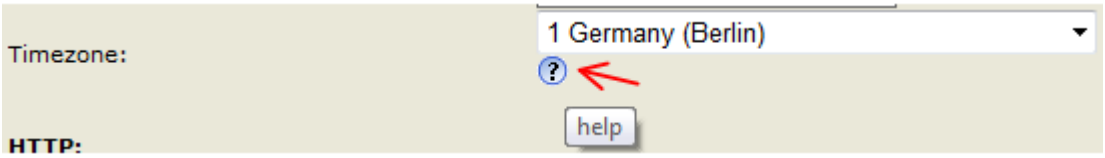
<!-- Following setting section contains the default phone settings for UC edition -->
<!-- This allows the firmware switch to UC edition without an additional factory reset. -->
<!-- Please edit or extend such settings only if you are 100% sure about the consequences! -->

Again, it is optional to edit the highlighted variable {prov_host} in the firmware URL according to the Lync environment in use. Editing it according to the location of the firmware XML file created and stored before is only needed if it deviates from this guidance.

It is recommended to edit such values as needed and save the file without changing the filename. A changed filename can be used, but is beyond the scope of this guide, especially step 3 (define and configure vendor specific DHCP options). The configuration XML file can be stored on any web server available as long as unauthenticated read access is possible. If the location of the configuration XML file is customized, the DHCP vendor specific options in the next step need to be adapted accordingly.

Please note: the configuration XML template file per design can be extended to provision more, in fact close to all device settings (like time zone, tone scheme, call waiting indication etc.). Such custom provisioning is out of scope of this document. The snom wiki (http://wiki.snom.com) provides the most current and complete documentation for the device settings, including guidance how to manage each in the XML configuration file.

Hint: Every setting in the device web server is linked to a wiki subpage explaining details, possible values and how to configure it, like in this example the time zone:



For your convenience the question mark alongside each setting offers the corresponding link.

Step 3: Define and configure DHCP vendor specific options

A DHCP vendor specific option created for each device type in this step will direct the snom devices to the configuration XML file. This configuration file directs to the firmware XML file and this one finally directs to the download resource location for the UC edition firmware.

Important advice: In large Lync deployments / network infrastructures it is strongly recommended to carefully consider this logical chain before setting the value for the DHCP vendor specific options in the DHCP servers designated to serving the devices in each location / subnet. Ideally the described logical chain should direct to a Lync Update service equipped server that's close and fast connected

from the device network perspective. So a mass rollout of firmware must not occupy a WAN connection for example. If a site or branch has the need to rollout the firmware locally, but has no Lync Update Service in place (like in case of a Lync SBA site) it is recommended to make the firmware files (.bin or .nbt) available via any local or public accessible web server and update the URL in the firmware XML file accordingly. This way a WAN or VPN connection to the Lync FE's (Data Center) must not be occupied with massive firmware downloads to the branch locations / remote sites.

This guide assumes that an NTP time server is already provided via DHCP option 42 to the DHCP clients. Configuration of that setting is out of scope of this guide.

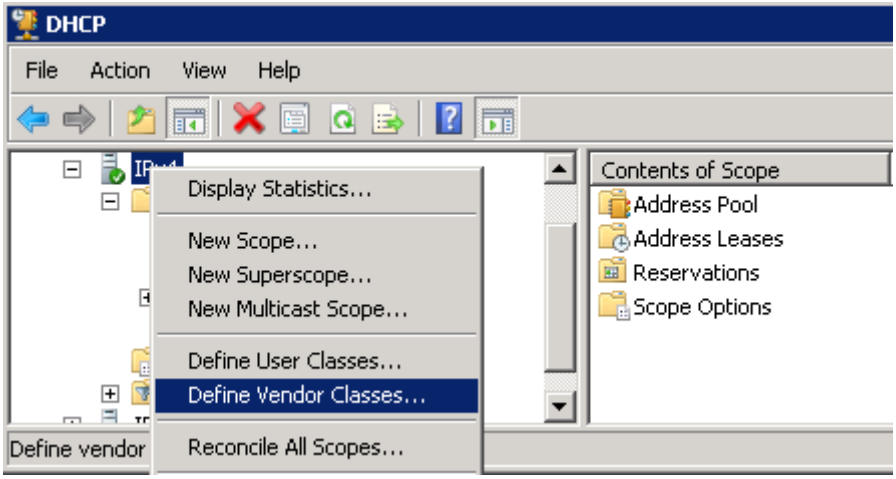
Define vendor classes for each device model

Note: The following instructions are based on Windows Server 2008 R2. If you are using a different server, the procedure may differ.

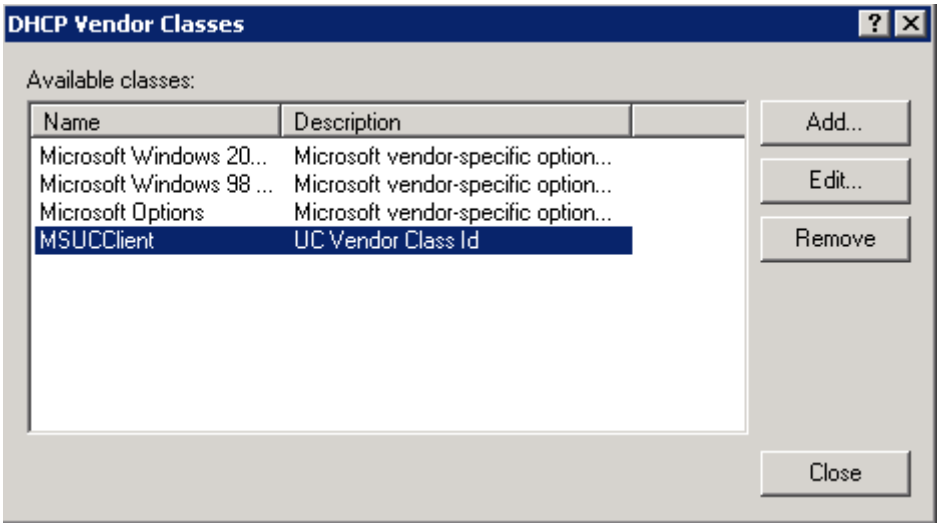
1. Access the DHCP server management console via Start > Administrative Tools > DHCP

2. Select the DHCP server and right-click IPv4.

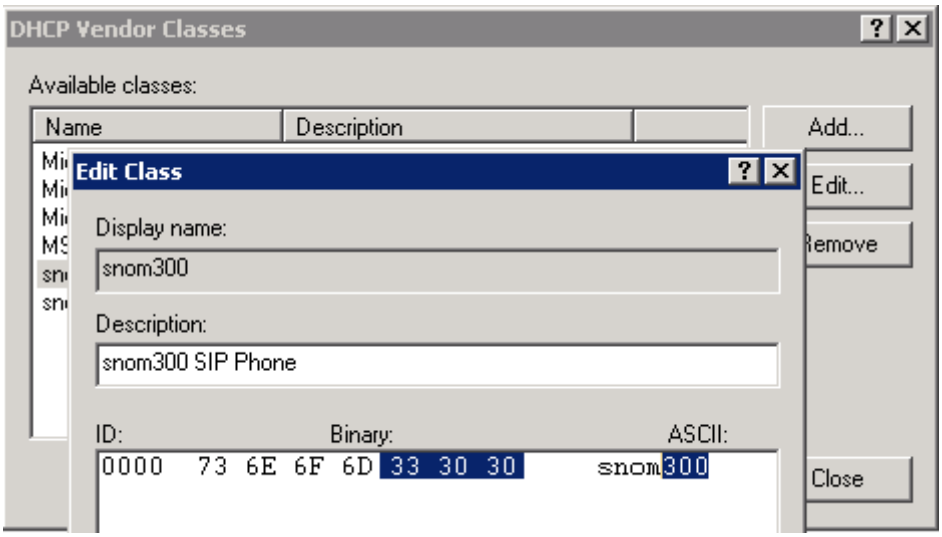
3. From the dropdown menu, select Define Vendor Classes...



4. When the DHCP Vendor Classes window opens, click Add...



5. In the Display name field, enter the name of the device model (e.g.snom300, snom821).



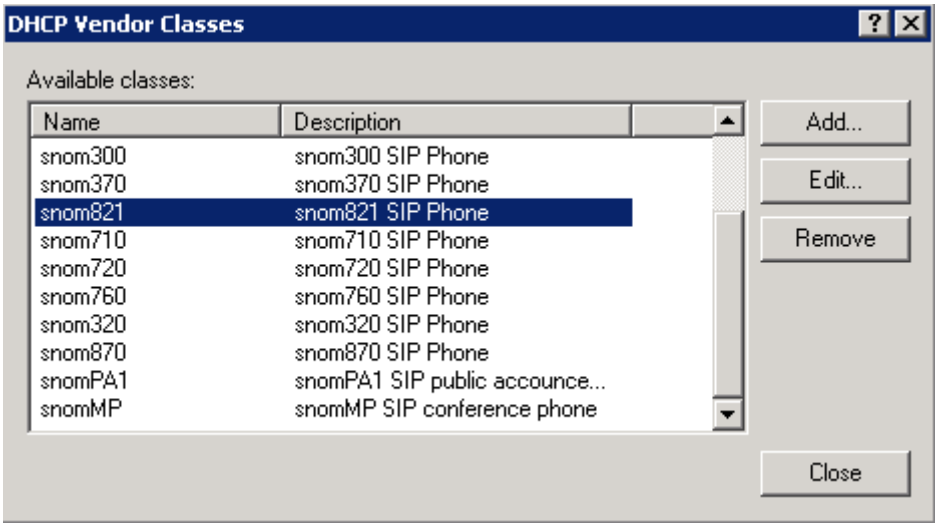
6. In the Description field, enter a description for the device model (e.g. snom300 SIP Phone).

7. Enter data to be used by the DHCP Server service for matching the class ID provided by DHCP clients (e.g. snom300, snom821). Click the right side of the text box (ASCII:) and enter the data as American Standard Code for Information Interchange (ASCII) text character values.

8. Click OK.

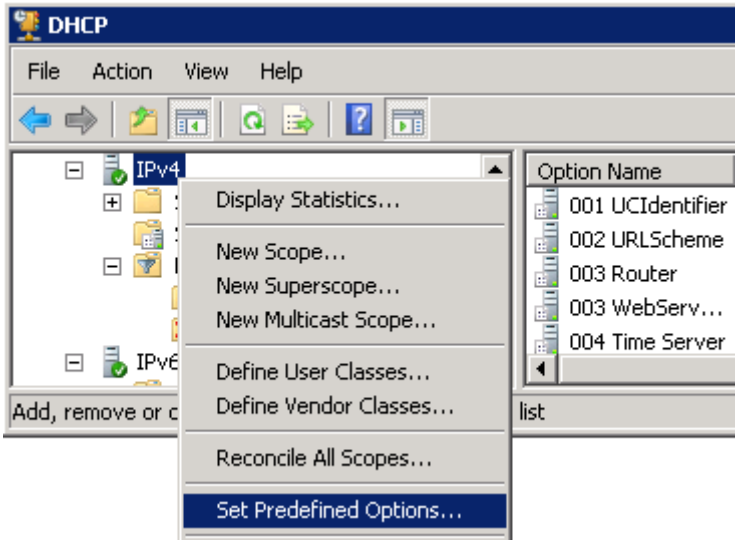
9. Repeat 4. through 8. for each device model in your environment.

10. Click close when all desired models are listed in the DHCP Vendor Classes window.

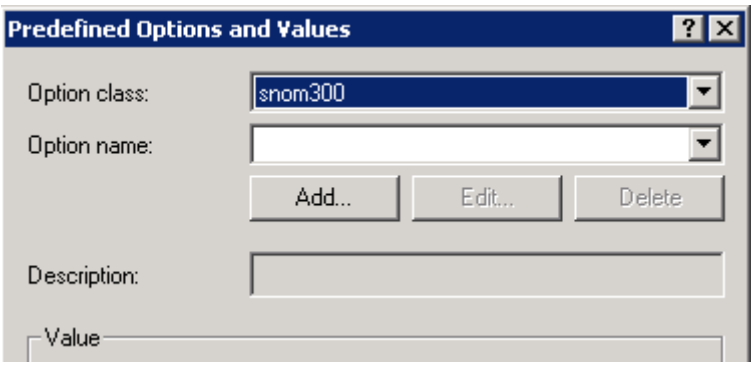


Set Predefined Options

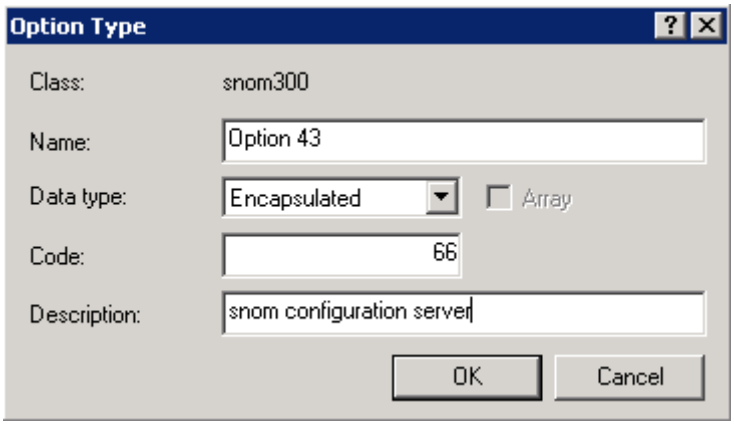
1. Right-click IPv4 again and select Set Predefined Options…



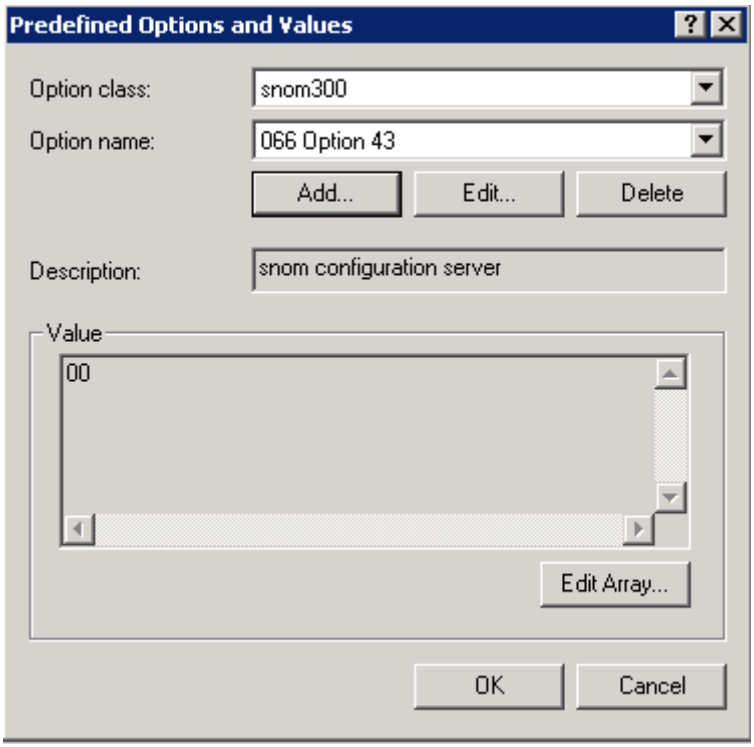
2. From the Option class dropdown menu, select the device model and then click Add:



3. In the Options Type window, populate the fields as shown below:

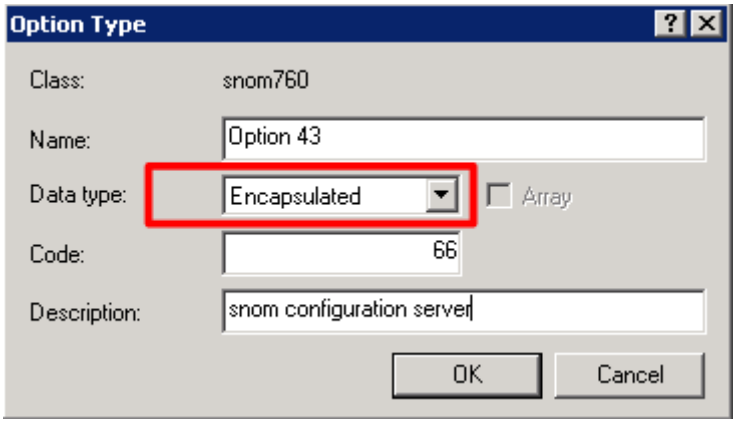


4. Click OK.



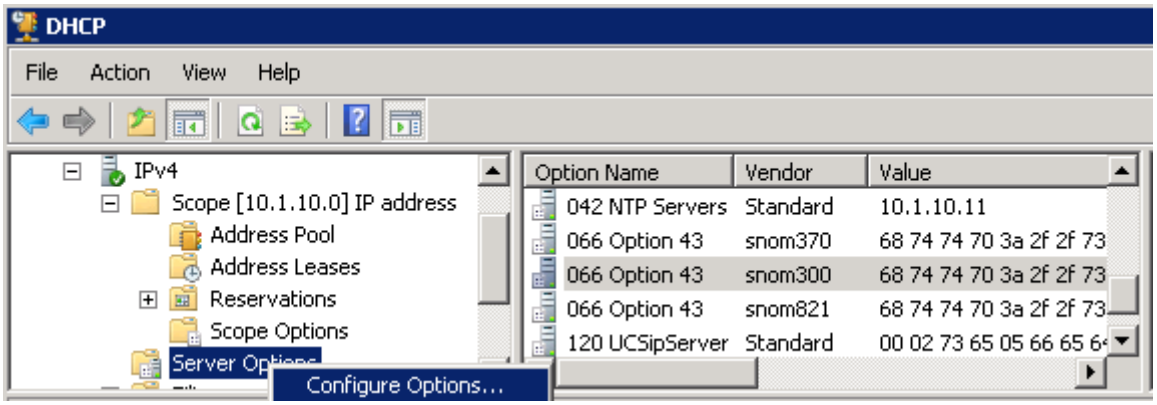
Repeat 2. through 4. for each option class defined before (each device type in your environment).

Note: during repeating please make sure that the Data type is always set to Encapsulated!



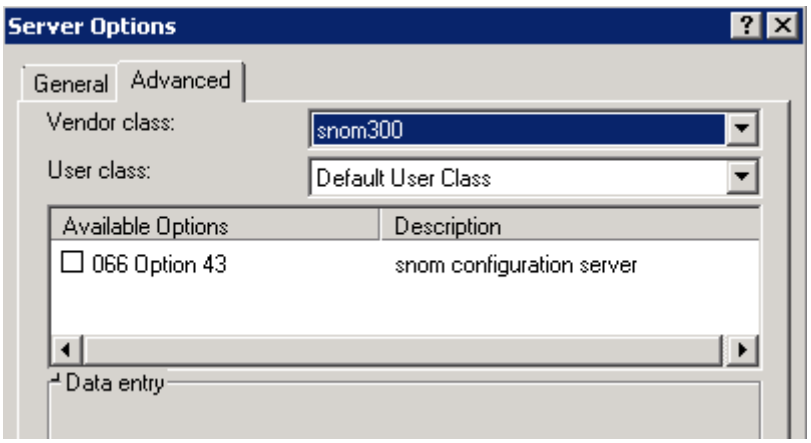
Configure the DHCP Server with Option 43

1. In DHCP management console right-click Server Options and select Configure Options…

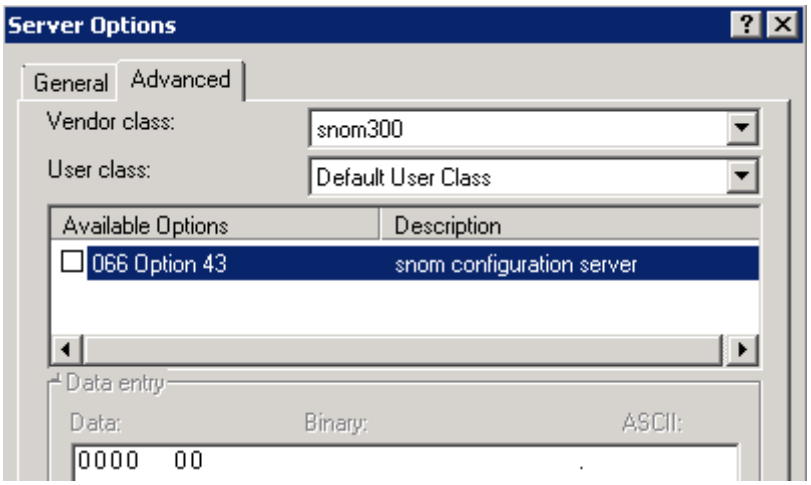


2. In the Server Options window click the Advanced tab.

3. From the Vendor class dropdown, select the device model.

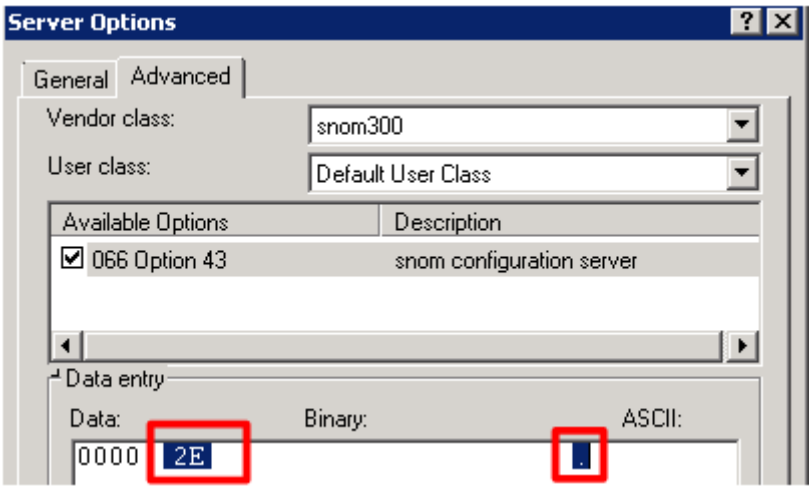


4. Select 066 Option 43 from the Available Options list.

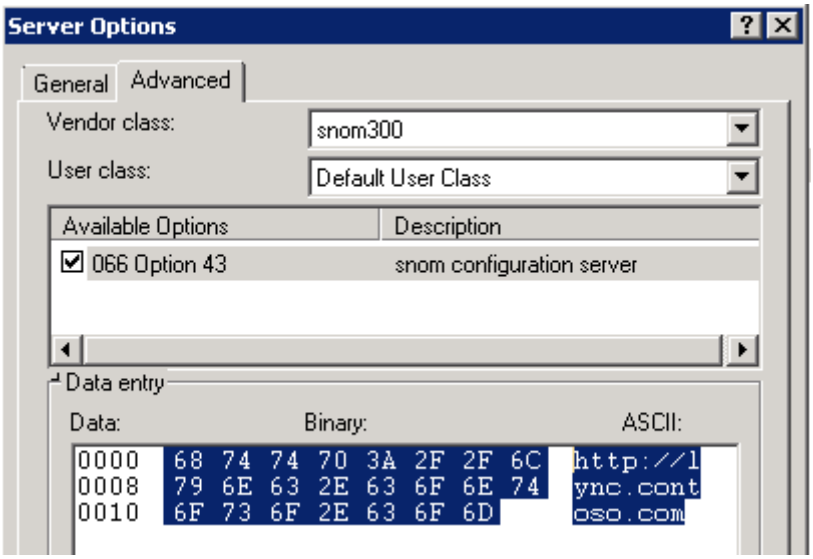


5. Click 066 Option 43, and enter the http-URL of your Lync server as a continuous string. This can be a little tricky. Place your cursor into the space below ASCII and begin typing.

   Note: If an asterisk (or dot) is in the ASCII field, backspace a few times to delete it:



   When you are finished, you may notice that the address wraps to more than one line.



This example uses http://lync.contoso.com as the URL to the Lync server (webserver) where the configuration files are published and available to the devices in their specific site / location. Adapt this value to the URL according to the designated Lync server in place by considering the recommendation in the intro of Step 3.

6. Repeat 3. through 5. for each Vendor Class according to the device types in your environment.

Note: During repeating 3. to 5. you can easily mistype the value for the URL, as copy & paste won't work. Therefore it is recommended to carefully review the value for each device / Vendor Class when finished. The server options list sorted by device type can be a help here be comparing the HEX value listed for each model:

Option Name	Vendor	Value
066 Option 43	snom300	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snom320	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snom370	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snom710	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snom720	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snom760	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snom820	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snom821	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snom870	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snomMP	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
066 Option 43	snomPA1	68 74 74 70 3a 2f 2f 6c 79 6e 63 2e 63 6f 6e 74 6f 73 6f 2e 63 6f 6d
003 Router	Standard	10.1.10.1

Typically they should all present the same value.

Ready-to-roll: Verify the environment preparation with a few devices

Select at least two devices of each model and unpack them. If available, verify that according to the box label the device was equipped during production with a standard SIP firmware version called 8.2.29 or higher.

Connect the devices to your environment / network and let them boot. Typically the devices will be served with an IP address by the DHCP server configured in step 3 and the snom vendor specific options. During boot up the display will show the obtained IP address.

Important note: Do not disconnect the device from the network or power off the device during the process! It may brick the device.

If the device successfully received and parsed the vendor specific options it will instantly start downloading the configuration and firmware XML files from the desired web repository. By using the URL to the CPE.nbt file found in the firmware XML file it will start downloading the UC edition firmware. If available the device display will show progress messages like:

> Software Update
> Downloading Firmware, Verifying Firmware (Successful), Checking Update Type (System Update)
>
> System Update
> Extracting Scripts, Extracting Update, Check for Kernel Update…, Update Successful

After the message “Update Successful” the device will restart, but this time with showing the UC edition logo or at least the desired UC edition firmware version number on the boot screen, shortly after the DHCP IP address assignment dialog.

When the boot process is completed the device will typically offer the standard dialogs for language selection, time zone, and tone scheme. After answering the dialogs the “Welcome! Press a key to log on.” screen will be shown. Depending on your environment preparation for sign in options to Lync the next dialog will allow ask you for your Extension and PIN or at least for your NTLM login information: sip-address, domain\username and password.

At this point the verification of the environment preparation for the Auto-Update to the UC edition firmware is completed. Please note that the registration/logging in process to Lync is out of scope of this guide. If you need information regarding the sign in options please refer to the Apollo guide (section: snom Extension and PIN sign in support with Lync Server) offered in your personal firmware portal!

After you successfully performed the described verification with at least two of each device model you can plan or immediately start the mass roll out of the UC edition for all remaining devices.

Troubleshooting

Troubleshooting the update process as described in this guide should start with the basics by analyzing the boot sequence first. It is important to verify if the device is really connected to the network as intended. Even if it seems correctly physically connected, it may be directed into another VLAN than intended, for example by an LLDP-MED configured Voice-VLAN on a certain network switch. If you experience the devices are booting into another network than intended, due to your productive network configuration, it is recommend to consider a kind of staging network segment without VLAN provisioning. Alternatively the VLAN in which the devices boot up can be prepared for the update process as described in this guide.

The next step is to verify if the phone received the correct update server URL via the vendor-specific DHCP option. To review the URL found and used by the device, access the device web server via its IP address and select “Settings” from the “Status” section (http://device-ip-address/settings.htm). At this page check the URL value for the setting: “update_server!:”. Please make sure it matches your configuration and environment as described in this guide. If it doesn’t match, it is recommended to review and correct the URL value at the DHCP server inside the vendor-specific options. If the setting seems to be not set, its recommend to troubleshoot the DHCP communication from and to the device with usual network tracing tools and by carefully reviewing the DHCP server side configuration (e.g. for typos).

After the setting “update_server!:” is verified as correctly set, the value for the setting called “firmware_status!:” should be reviewed. If it’s empty / not set most likely the attempt to access and download the model specific configuration XML file (e.g.: snom300.htm, snom760.htm) failed. This can be caused for example by a temporally outage at the web server repository (IIS in Lync server if used as described) or if the access to the file is blocked by any (none-default) additional authentication or a proxy / firewall challenging the device. It is recommended to check if the download of the model specific configuration XML file is currently possible (without authentication) from the device network location perspective. This can be performed e.g. by using a browser (no proxy / credentials pre-configured) on a none-domain joined machine being connected to the device network location. With the browser the access to the XML file, e.g. via the URL http://lync.contoso.com/snom760.htm according to the case described in the guide must be possible without any credential challenge. If the access is not possible at all, carefully check the service availability of the web server repository in use. If the access attempt is facing a credential challenge, consider to allow (maybe temporally) unauthenticated access for the update process or a kind of staging network segment without proxy / authentication. In the unexpected case the device still fails to download the configuration XML file, even all mentioned prerequisites are met and verified its recommend to troubleshoot the HTTP communication from and to the device with usual network tracing tools.

Such troubleshooting steps described for investigating issues by accessing the model specific configuration XML file, are strongly recommended for a rerun if access to the model specific firmware XML file or the CPE.nbt firmware file fails.

Typically you will find the update process related settings filled with values like in this (the described) example:

update_server!: http://lync.contoso.com

- given by DHCP vendor specific option 66

update_policy!: auto_update

- retrieved from the model specific configuration XML file (snomXXX.htm), for an example refer to page 8

firmware_status!: http://{prov_host}/RequestHandler/Files/3PIP/snom/snomXXX-fw.htm

- retrieved from the model specific configuration XML file (snomXXX.htm) while XXX represents the device model, {prov_host} is the place holder for the server FQDN value found in setting: “update_server!:”

firmware!: http://lync.contoso.com:80/RequestHandler/Files/3PIP/snom/snomXXX/AB/ENU/X.X.X.X/CPE/CPE.nbt

- retrieved from the model specific firmware XML file (snomXXX-fw.htm) while XXX represents the device model and /X.X.X.X/ represents the UC edition firmware version

A final note: Before starting extended troubleshooting beyond the scope of this document, it is recommended to carefully review the values mentioned above, the related XML files, and the network (DHCP, DNS) configuration especially regarding typos. In addition it can save a lot of time and effort to review the steps in this guide again and by comparing it to the present environment, with a focus on the web repository (XML and firmware file store) configuration and availability.