Extension and PIN sign with snom phones for Microsoft Lync 2010

Introduced in “snom UC edition” Version 8.8.1.1

Version 1.0 Jan boguslawski 2012-05-22

snom Extension and PIN sign in support with Lync Server 2010:

Starting with Version 8.8.1.1 snom introduces the new feature “Extension and PIN sign in support with Microsoft Lync Server 2010”. This feature is based on the same mechanisms used to sign in phones running the Lync Phone Edition 2010 available from other vendors. In an environment set up to support these devices, snom phones are able to sign in with extension and PIN automatically.

As an alternative to authentication via NTLM (full AD – Active Directory credentials, Domain\Username and Password), snom UC edition devices can now authenticate via TLS-DSK (TLS with Derived Session Key) in SIP and HTTP(S). This kind of client certificate is provisioned by the Lync Server 2010 web service when a valid combination of a user’s extension (optional: complete phone number) and PIN is provided. Using a Derived Session Key the snom devices operate independently of any Active Directory password changes, or even changes to the telephone number, extension or PIN.

Notes and limitations:

Easy Hot-Desking

With the support of Extension and PIN sign in, snom devices introduce “easy Hot-Desking”. Signing in and out multiple user accounts[1] on one device using extension and PIN becomes a quick and intuitive task. For details please refer to the section “Easy Hot-Desking in configuration”.

TLS-DSK and SBA support

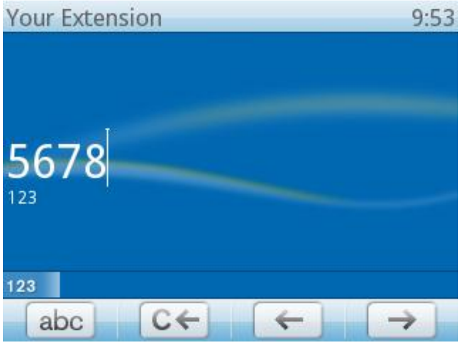
With Version 8.8.1.1 and beyond, snom UC edition devices will use TLS-DSK as the primary authentication mechanism for SIP and HTTP(S), regardless of whether or not the new extension & PIN or NTLM authentication is used. This is a basic requirement in Survivable Branch Appliance (SBA) scenarios, which are also now natively supported by the snom UC edition (min. 8.8.1.1). This includes user interface notifications during an outage and the underlying failover mechanism related to primary and backup registrars in Lync infrastructures.

[1] Currently, this feature is officially supported for up to two user identities – additional identities are not recommended but can be added.

Signing in with Extension and PIN:

If the snom device detects (via DHCP responses – covered in detail later in this document) it will provide users with the option to login with extension and PIN (visible in the top line of the user interface). If the phone continues to ask for NTLM credentials (SIP-URI) because it could not detect the prerequisites for this sign in method, please refer to the prerequisites section of this document.

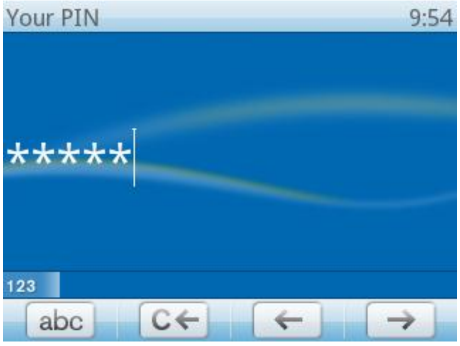
When an Extension and PIN



Your Extension 9:53

5678

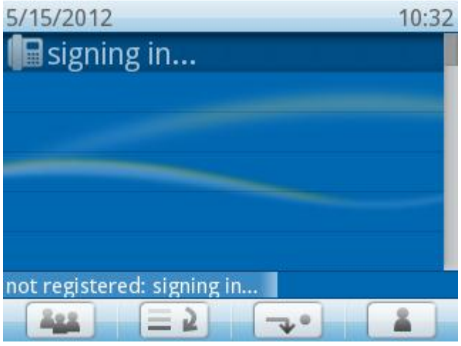
123



Your PIN 9:54

*****

is provided by the user the device will contact Lync’s certificate provisioning web service by using the URL received via the DHCP server’s response (if configured - not per default - the DHCP response can also be sent by Lync Registrar via the built-in stripped down DHCP server – more details in the section about configuration prerequisites). By design, the login process with extension and PIN takes more time than the login with NTLM credentials. As long as the process is running, the device will indicate this on the user interface.

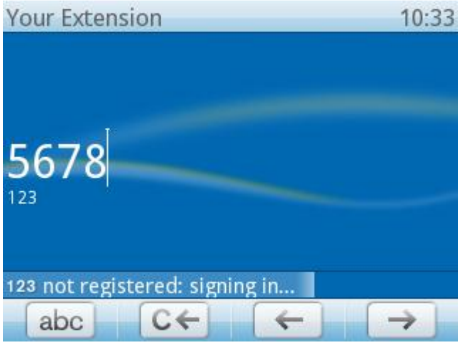


5/15/2012 10:32

signing in...

not registered: signing in...

If the login fails, for example because of an invalid or non-existent extension, a request will be made for a valid extension and PIN combination, with a note (not registered: signing in…).



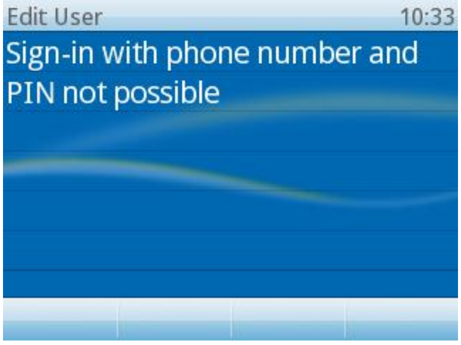
Your Extension 10:33

5678

123

123 not registered: signing in...

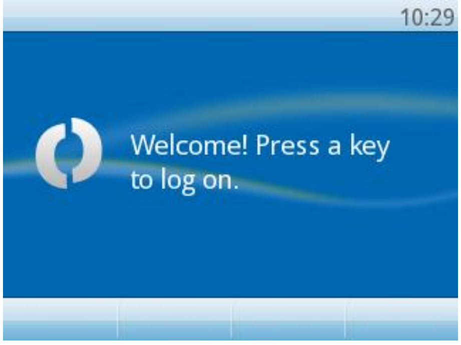
If the sign-in fails completely, the device will display a corresponding message.



Edit User 10:33

Sign-in with phone number and PIN not possible

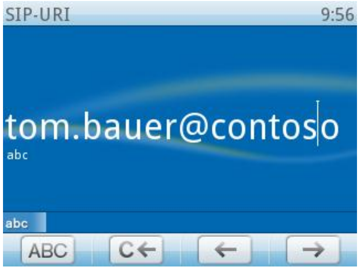
By returning to the “Welcome!” screen



10:29

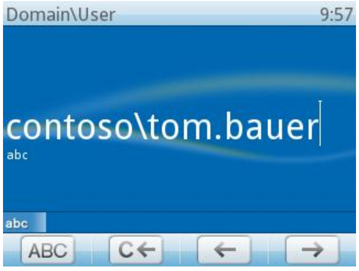
Welcome! Press a key to log on.

the device now returns to the authentication message for NTLM (full credentials: SIP-address, Domain\Username and Password).



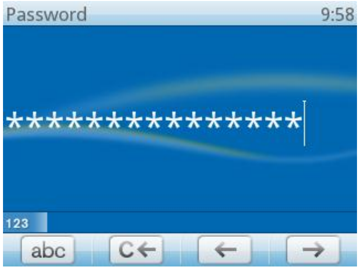
SIP-URI 9:56

tom.bauer@contoso



Domain\User 9:57

contoso\tom.bauer

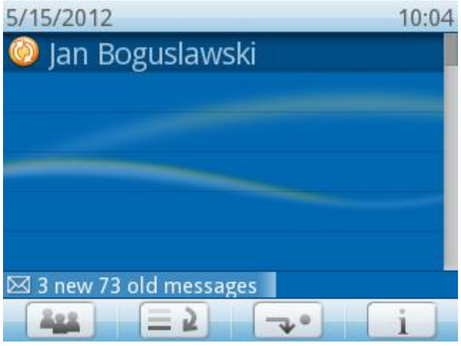


Password 9:58

****

Please note: Every time a login is canceled (phone returns to the “Welcome!...”-screen), the phone will toggle between Extension & PIN sign in and NTLM..

A successful extension and PIN sign-in finishes with the same idle screen when performing NTLM authentication.



5/15/2012 10:04

Jan Boguslawski

3 new 73 old messages

Configuration

The possibility to sign in devices with extension and PIN is not available by default after Lync Server 2010 is deployed. Please follow Microsoft's guidelines on how to setup extension and PIN sign-in. Consequently, snom recommends carefully reviewing related TechNet articles, blog posts and whitepapers.

Prerequisites

- Please verify that extension and PIN authentication is enabled on the Lync Server as described in TechNet:

  Setting Up (PIN) Authentication on the New IP Phones
  http://technet.microsoft.com/en-us/library/gg412902

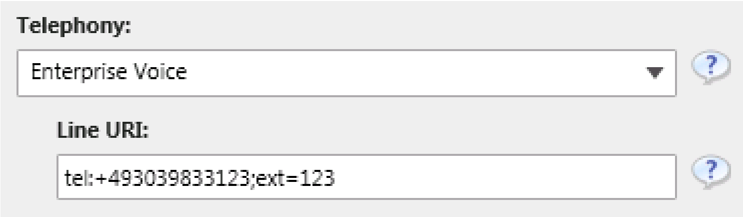
  Please also verifiy that Certificate Authentication (TLS-DSK) is enabled via the Lync PowerShell command:

  Get-CsWebServiceConfiguration | select usecertificateauth | fl

  More details are available in TechNet

  Get-CsWebServiceConfiguration: http://technet.microsoft.com/en-us/library/gg425751
  Set-CsWebServiceConfiguration: http://technet.microsoft.com/en-us/library/gg398396

- User accounts that should be logged in via Extension/PIN need to be Enterprise Voice enabled in Lync Server 2010 and be configured with a Line URI that has its extension defined via the " ;ext= suffix ".
  Example: A user has the E.164 telephone number +493039833123 and the extension is 123. The Line URI should be configured thus: tel:+493039833123;ext=123

  Telephony:
  Enterprise Voice
  Line URI:
  tel:+493039833123;ext=123

  (Configuring the Line URI is possible via Lync Server Control Panel or Lync PowerShell)

  If the extension is not defined via the " ;ext= suffix " in the Line URI, the login can be performed by using the full telephone number without the leading plus sign. For the example above (Line URI would be only: tel:+493039833123), the user can provide 493039833123 and Lync 2010 will accept it as well.

- As no PIN is configured by default, it must be set by the user or the Lync Server administrator once before a login can be executed successfully. To set an initial PIN for all users, execute this Lync PowerShell command:

Get-CsUser | Set-CsClientPin -Pin 12345

This will set the same PIN for all users found in the Lync infrastructure and may conflict with your security policies!

For more details and background information about the Lync PIN, lock and unlock a PIN, and the options on how to set or reset it as an administrator or a user please carefully review the following online information:

- From the CS PowerShell team - CSCP Haiku 095: http://blogs.technet.com/b/csps/archive/2011/04/22/haiku095.aspx

- Office Online Help Topic - Join a meeting or conference call by phone – section “Set my dial-in conferencing PIN”: http://office.microsoft.com/en-us/communicator-help/join-a-meeting-or-conference-call-by-phone-HA102041504.aspx

- The DHCP server that operates the network segment where the devices will be used needs to be configured with a set of vendor specific options. With the URL information provided by the DHCP server, snom devices will be able to locate the Lync Server certificate provisioning service (extension/PIN sign-in required).

  - For Windows based DHCP servers a pair of handy tools called DHCPutil.exe and DHCPConfigScript.bat is available, typically stored in common files of the Lync Server installation folder: …\Program Files\Common Files\Microsoft Lync Server 2010

    This TechNet article will guide through the steps to configure Windows based DHCP servers with by using these tools:

    Using DHCPUtil: http://technet.microsoft.com/en-us/library/gg412988.aspx

  - For DHCP servers other than Windows DHCP server please refer to these TechNet articles:

    Configuring DHCP Options on DHCP Servers other than Windows DHCP Server
    http://technet.microsoft.com/en-us/library/gg412828.aspx

    A whitepaper that compliments the previous article on how to configure DHCP servers from the following manufacturers: BlueCat, Cisco, Linux, Infoblox, and QIP:

    Configuring DHCP Options to Enable Sign-in for IP Phones
    http://www.microsoft.com/en-us/download/details.aspx?id=27138

- For network segments without a DHCP solution that supports the necessary vendor specific options (e.g. a router device) using the built in Lync Server DHCP component (a stripped down DHCP server provided with the Registrar) might be an option.

  To enable the built in Lync Server DHCP component, which is disabled per default this Lync PowerShell command needs to be executed:

  set-CsRegistrarConfiguration -EnableDHCPServer $true

  More details: http://technet.microsoft.com/en-us/library/gg398764.aspx

  Please note that this DHCP component will not lease IP addresses. It just listens to the device’s DHCP broadcasts and responds with the appropriate DHCP INFORM packets containing the URL to Lync certificate provisioning web service.

For more information about configuring DHCP servers, the Lync Server DHCP component, and parallel usage please refer to the TechNet article:

Setting Up DHCP for Devices
http://technet.microsoft.com/en-us/library/gg398369.aspx

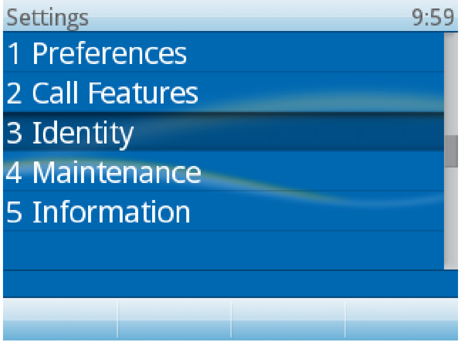
Easy Hot-Desking

Signing in multiple accounts within a Lync infrastructure on a single snom device now becomes an easy and quite straight forward task.

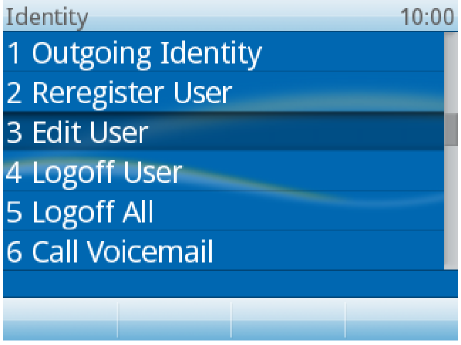
Please note: Depending on account activity, the amount of usable accounts on a phone can be limited, snom supports up to 2 Identities on one phone. Additional Identities can be added but are not recommended

The following example, on a snom 821, explains the major steps required.

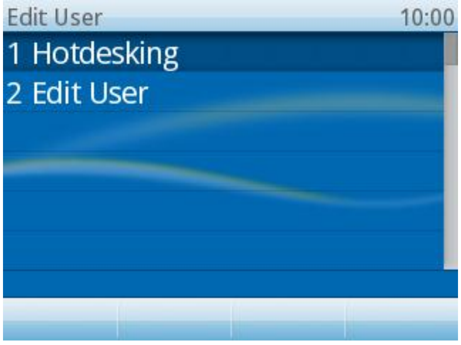
On a snom device already signed in to Lync with one or more accounts, the user can enter the settings menu, via the menu button. Selecting and confirming the optional identity



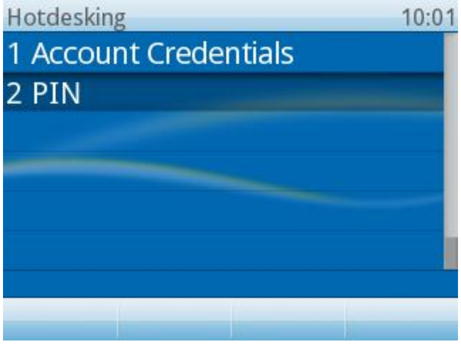
will lead to the Identity submenu.



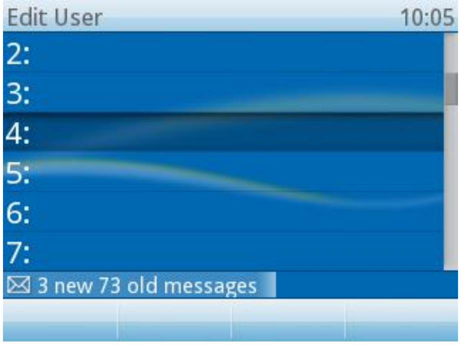
By selecting and confirming 'Edit User' the Hotdesking option is displayed.



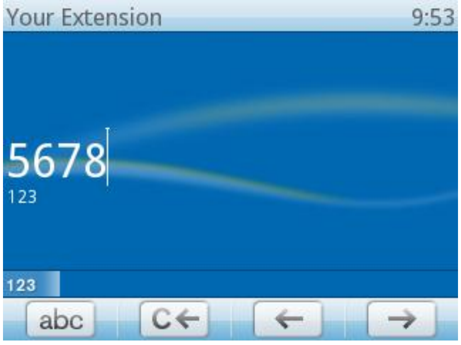
Inside Hotdesking menu a new option called PIN is available.



When PIN is selected and confirmed all phone accounts (maximum is 12 in case of snom 821) not in use are displayed.



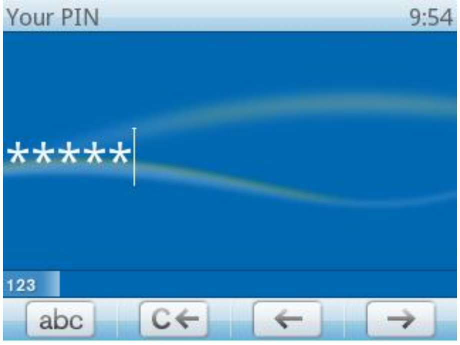
For the selected account the device will request the user's extension and PIN in the same way it does when the Welcome! Screen is passed.



Your Extension 9:53

5678

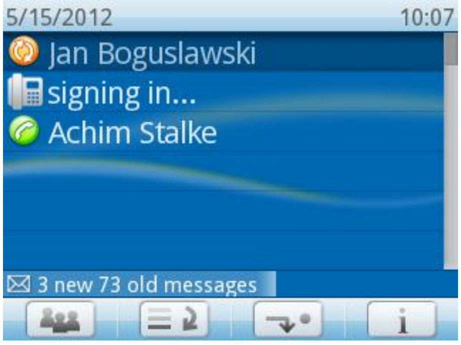
123



Your PIN 9:54

*****

Once the sign-in starts, the display will return to the idle screen indicating the process.



5/15/2012 10:07

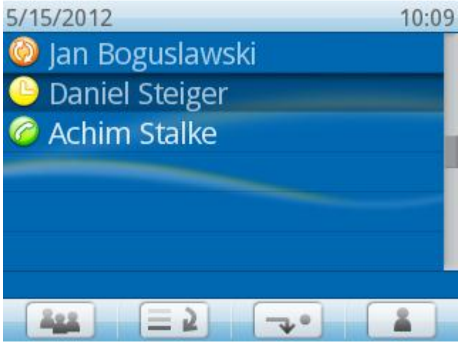
Jan Boguslawski

signing in...

Achim Stalke

3 new 73 old messages

After successfully signing in, the additional account is ready for use with the same feature set as the first account: Presence, contact list, voicemail, etc.



5/15/2012 10:09

Jan Boguslawski

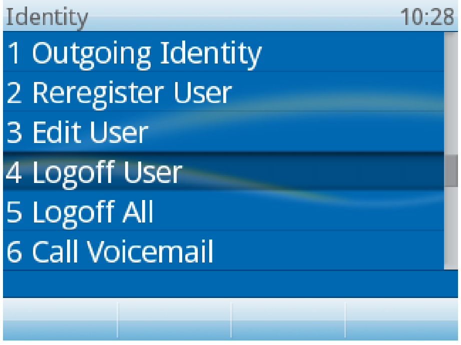
Daniel Steiger

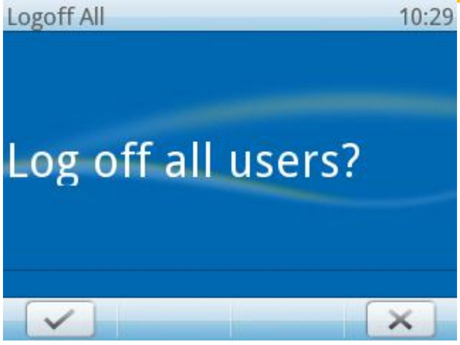
Achim Stalke

The menus for presence, contact list, etc. will dynamically switch their context according to the current active identity selected (highlighted) via the Navigation button on the device.

Please note: The device is able to receive all incoming calls for the accounts logged in. Outgoing calls will be performed with the active identity.

Logging off one or all users can be performed via the Identity submenu by choosing the option Logoff User or Logoff All.





Log off all users?

Troubleshooting

The key information the devices need to have, to start offering the Extension and PIN sign in dialog is the URL for the Lync Server certificate provisioning web service. This information should be provided within a vendor specific DHCP inform response.

For troubleshooting, it is essential to review the network infrastructure and components in use, while considering the nature of DHCP protocol and transport layer. Please verify if it is in general possible for the snom device to successfully send out a DHCP inform request to a desired DHCP server (or the DHCP component in a Lync Registrar if enabled). In addition, the response from the DHCP server or component must reach the device in the opposite direction. Besides Firewall rules, DHCP - Denial of Service protection in use might be another obstacle blocking the DHCP packets.

How to verify if the device detected the URL to Lync Certificate provisioning web service

- If the devices successfully obtain a URL, it is stored under the setting called "cert_provisioning_service". For example:

  cert_provisioning_service!: https://ls.contoso.com:443/CertProv/CertProvisioningService.svc

  The setting and its value can be found on the device "/settings.htm" page. This page can be reviewed by logging into the device web server with administrative access that unlocks the advanced settings and submenus. For example, if a device has the IP address 10.10.10.42 then "settings.htm" can be accessed under https://10.10.10.42/settings.htm

  For details about logging in to the device web server and accessing advanced mode, please refer to the appendix: How to login to the device web server – Automatic device web server protection

- **Setting cert_provisioning_service is empty**
  If the value of the setting "cert_provisioning_service" is empty the device did not receive the DHCP inform response or did not parse it successfully for the Lync Certificate provisioning web service URL. In case the setting has no value, the login dialog screen for Extension and PIN authentication will not offered by the device. Please analyze your DHCP configuration.

- **Setting cert_provisioning_service is set**
  If the value is set to a valid URL to a Lync Certificate provisioning web service but login with

extension and PIN fails, it is recommended to carefully review the prerequisite steps under section configuration. Ensure communication between the device and the web service is not blocked by any network protection, such as a firewall, and also check that DNS is working in the network location of the device. Try to request the URL from a web browser in the same network segment – the browser should ask for credentials (this would indicate that communication is possible).

- **Manually setting the Certificate Provisioning Service:**
  When troubleshooting it can be helpful to set the value for "cert_provisioning_service" manually on the phone by accessing the device web server in Admin mode. This can be performed by using a web browser to open the so called "/dummy.htm" and providing the URL with a command such as in this example:

  - The IP address of the device is: 10.10.10.42

  - The Lync Certificate provisioning web service is available under the URL:

    https://ls.contoso.com:443/CertProv/CertProvisioningService.svc

  ➔ This URL needs to be opened in a browser if the device web server is already accessed in Admin mode:
  https:// 10.10.10.42/dummy.htm?settings=save&cert_provisioning_service=https://ls.contoso.com:443/CertProv/CertProvisioningService.svc

  - After setting the value manually it is recommended to review the "/settings.htm" page again (refresh it in browser) to see if it's configured correctly.

  - A subsequent reboot (not just power off/on) performed via the phone's user interface using Menu → Maintenance → Reboot is recommended.

  - When rebooted the device should start offering the login dialog for Extension and PIN authentication if the Welcome! Screen is passed. If not, please refer to the section "Setting cert_provisioning_service is set"

Appendix:

How to login to the device web server – Automatic device web server protection

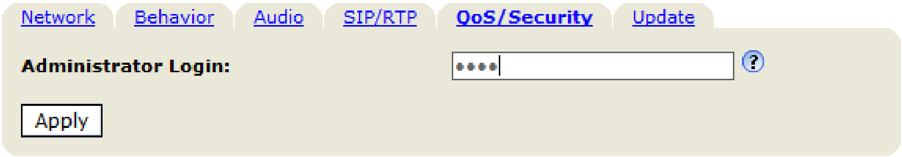
In the UC edition firmware, snom's built in web server is enabled to only be accessible via HTTPS by default. The device IP address can be obtained whilst booting..

As access to the web server is restricted to HTTPS you need to open a web browser and enter the device IP address in the address bar prefixed with https (not just http).

Please note: most browsers will display a warning message regarding the certificate presented by the snom device web server. The warning can be safely ignored.

- Access the web server on devices not registered

  By default, the web interface will be in User-Mode. Unlocking the "Advanced" menu and Administrator-Mode is possible via clicking "Advanced" in "Setup" and by entering the Administrator Login (0000 by default). If the Webserver requires Username and Password confirmation, please read below.



Administrator Login: ••••

- Access the web server on devices already registered

  If the device is already registered to the Lync infrastructure, its web server is automatically protected by default with an account and password in line with security and privacy considerations. The values for a valid account and password are always related to the first Lync user account logged in, but depend on the authentication mechanism that was used.

  - By signing in with SIP-address, username and password via UC Account Data wizard (in snom device web interface) or on the device user interface e.g. with:

    Domain\User: Snom\Tom.Bauer

    Password: MyP@sswort1234

    the snom webserver account name will become:

    Snom\Tom.Bauer

    the snom webserver account password:

    MyP@sswort1234

Sum:

1. The domain and \ becomes part of the account name value.
2. Both account name and password are CASE sensitive!

It is necessary to enter the exact values to gain access to the snom web server again.

- By signing in with extension and PIN on the phone e.g. with:

Extension: 5678

PIN: 12345

the snom webserver admin account name will become:

5678

The snom webserver admin password:

12345

Unlocking the Advanced menu and Administrator-Mode can be performed the same way as described in “Access the web server on devices not registered”

By signing out the first user, the web interface can be unlocked.