Configuration Note

snom 360 Phone with VX for Branch Survivability

Release 1.0

CONFIGURATION NOTES: VX SERIES

Trademarks

The N.E.T. logo, PanaVue, PrimeSwitch, Promina, SCREAM, Service Creation Manager, SHOUTIP, CellXpress, FrameXpress, Frame Relay Exchange, IPNX, LAN/WAN Exchange, Network Equipment Technologies, netMS, PortExtender, PrimeVoice, SCREAMvue, and SHOUT are trademarks of Network Equipment Technologies, Inc.

SunOS and Solaris software copyright is held by Sun Microsystems, Inc. Sun Microsystems is a registered trademark and Sun, SunOS, OpenWindows, Solaris, and Ultra are trademarks of Sun Microsystems, Inc. UNIX is a registered trademark of The Open Group.

All other trademarks and registered trademarks are the sole property of their respective owners.

This document constitutes the sole Specifications referred to in N.E.T.'s Product Warranty for the products or services described herein. N.E.T.’s Product Warranty is subject to all the conditions, restrictions, and limitations contained herein and in the applicable contract. N.E.T. has made reasonable efforts to verify that the information in this document is accurate, but N.E.T. reserves the right to correct typographical errors or technical inaccuracies. N.E.T. assumes no responsibility for any use of the information contained in this document or for any infringement of patents or other rights of third parties that may result from the use of this document. Networking products cannot be tested in all possible uses, configurations or implementations, and interoperability with other products cannot be guaranteed. The customer is solely responsible for verifying the suitability of N.E.T.'s products for use in its network. Local market variations may apply. This document is subject to change by N.E.T. without notice as additional information is incorporated by N.E.T. or as changes are made by N.E.T. to hardware or software.

U.S. Government Rights, Government Users

The software accompanying this documentation is furnished under a license and may only be used in accordance with the terms of such license. This documentation is "commercial computer software documentation" as that term is used in 48 CFR 12.212. Unless otherwise agreed, use, duplication, or disclosure of this documentation and any related software by U.S. Government civilian agencies is subject to restrictions as set forth in 48 CFR 52.227-14 (ALT III) and 48 CFR 52.227-19, and use, duplication, or disclosure by the U.S. Department of Defense is subject to restrictions as set forth in 48 CFR 227.7202-1(a) and 48 CFR 227.7202-3(a) or, if applicable, 48 CFR 252.227-7013(c)(1)(ii) (OCT 1988).

Released

October 2009

Network Equipment Technologies, Inc.
6900 Paseo Padre Parkway
Fremont, CA 94555 U.S.A.

http://www.net.com

Contents

Document Overview

Content

This document includes configuration examples for:

- snom 360 with OCS
- snom 360 with VX Registrar Fallback
- snom 360 TLS with VX Registrar
- eyeBeam TLS with VX Registrar

Note: This document does not necessarily describe accurately the design or operation of any NET product or service and it does not create any express or implied warranty. NET's sole warranty is contained in its Product Warranty. The End User Documentation shipped with NET's products constitutes the sole Specifications referred to in the Product Warranty. NET assumes no responsibility for any use of the information contained in this document or for any infringement of patents or other rights of third parties that may result. Networking products cannot be tested in all possible uses, configurations or implementations, and interoperability with other products cannot be guaranteed. The customer is solely responsible for verifying the suitability of NET's products for use in its network. This document and NET's specifications are subject to change without notice.

Intended Audience

This document is intended for Systems Integrators with significant telephony knowledge.

Configuring snom 360 and VX with TLS

Use the steps in this section to configure the snom 360 (snom) and VX with Transport Layer Security (TLS).

Step 1: Install VX Root Certificate onto the snom Phone

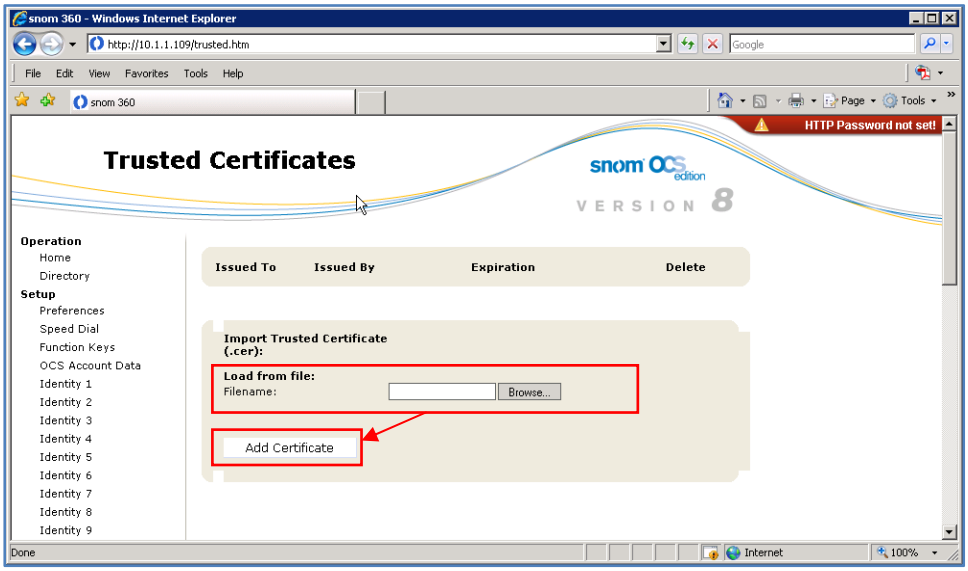
If VX is using a Certificate Authority (CA)-signed trusted certificate, the VX root certificate file can also be installed directly onto the snom phone to allow TLS.

1. FTP the VX root certificate file to your PC from VX. You can locate the VX root certificate file by entering **`sho cert root`** at the command prompt on VX.

```
UCdemo# sho cert root
Issued To                    Issued By                    Type        Generation          Expiration
---------------------------- ---------------------------- ----------- ------------------- -------------------
                        vxca                         vxca self-signed  1/18/2009 04:02:55  1/18/2014 04:12:53
```

2. From the snom Trusted Certificates view, browse the **Load from file:** and locate the root certificate file.

3. When you have located the VX root certificate, click **Add Certificate**. The VX root certificate is now added to your snom phone.



Note: The VX root certificate may take a few moments to load and/or display on your snom phone. If the TLS is still working, the certificate should be available.

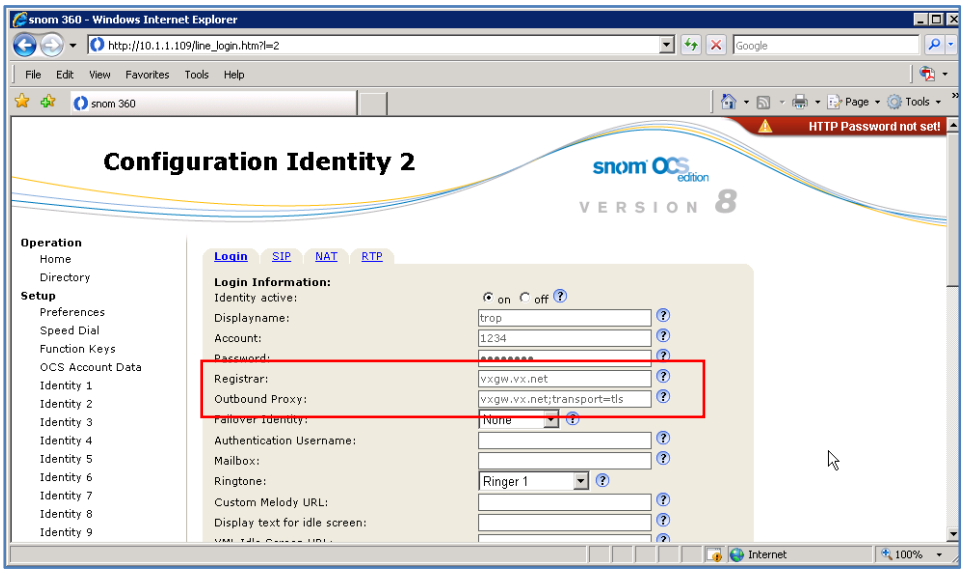
Step 2: Enter the Configuration Identity

1. On VX, locate the certificate name by entering **sho `cert`** at the command prompt. The VX CA-signed certificate **Common Name** is **`vxgw.vx.net`**.

```
UCdemo# sho cert
Issued To                    Issued By                    Type        Generation          Expiration

----------------------------- ----------------------------- ----------- ------------------- -------------------
                  vxgw.vx.net                              vxca    CA-signed  4/27/2009 20:05:28  4/27/2011 20:15:28

UCdemo#
```

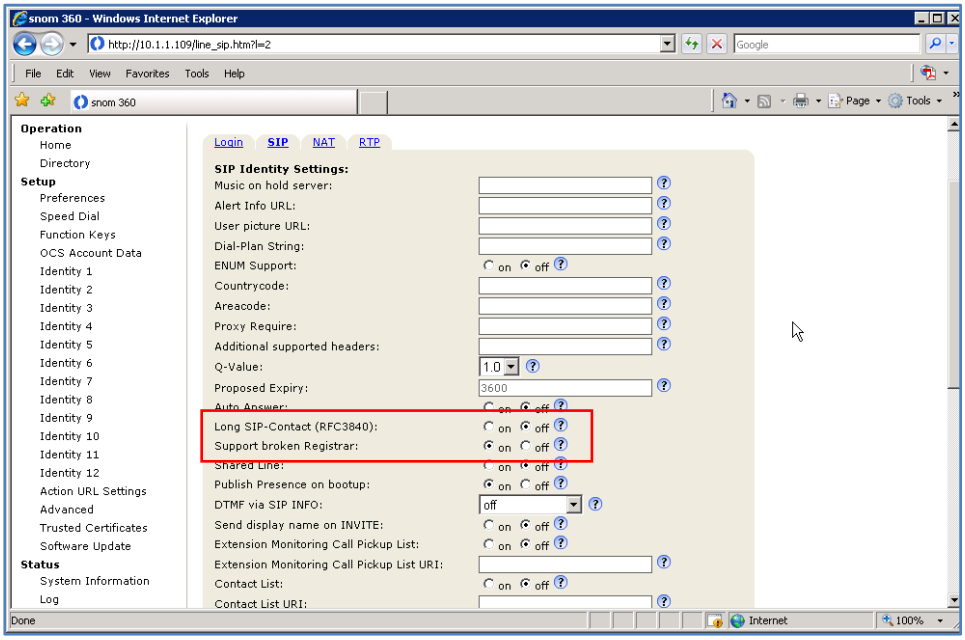
2. On the snom Login Tab, the common name also applies to the **Registrar** and **Outbound Proxy**. The Outbound Proxy includes **`;transport=tls,`** which enables TLS on the snom phone.

   Note: The Fully Qualified Domain Name (FDQN) must be resolvable by a Domain Name System (DNS).



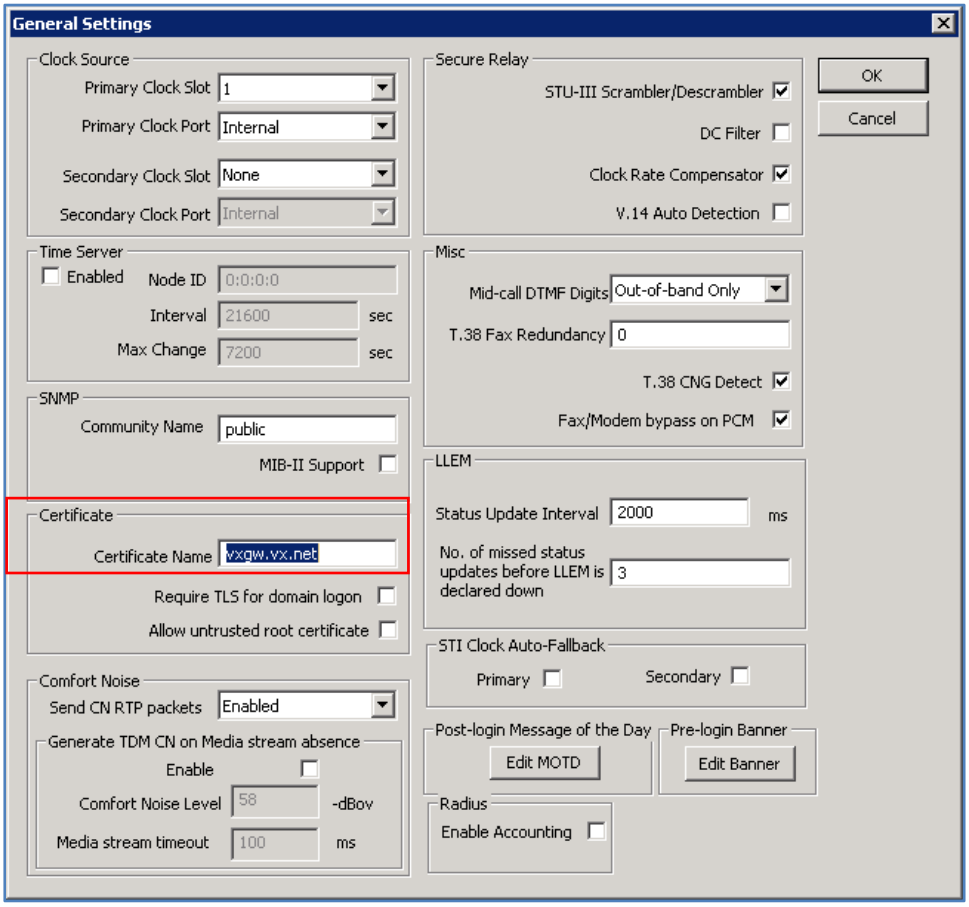
Step 3: SIP Settings

On the snom SIP Tab, set **Long SIP-Contact (RFC3840)** and **Support broken Registar** to **OFF**.



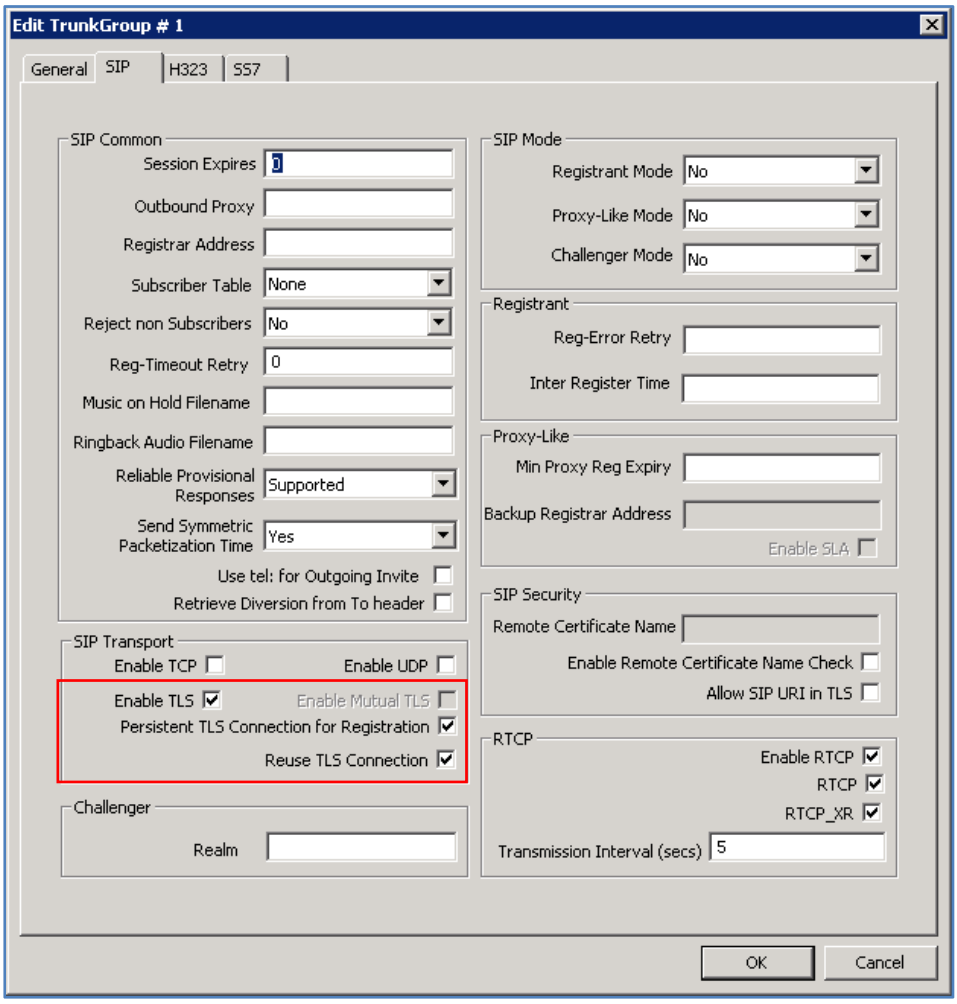
Step 4: VX Settings

On the VX General Settings view, enter the **Certificate Name.**



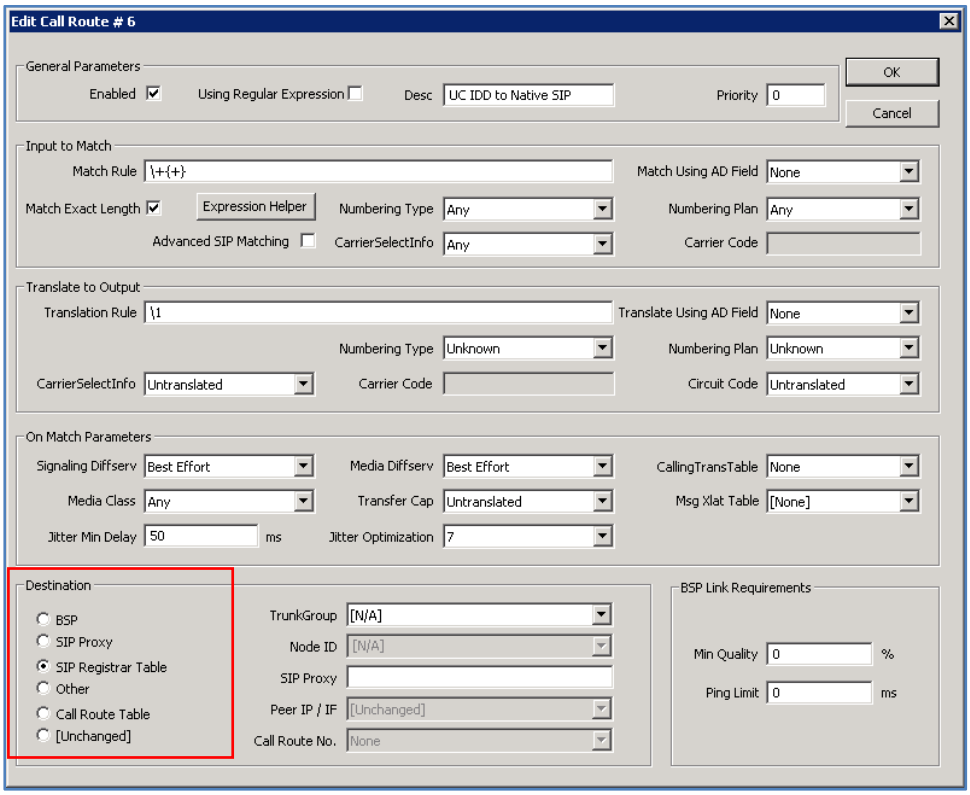
Step 5: Trunk Group Settings

On the VX Edit TrunkGroup # 1 view, SIP Tab, select **SIP Transport>Enable TLS**, **Persistent TLS Connection for Registration**, and **Reuse TLS Connection**.



Step 6: Call Route

On the VX Edit Call Route #6 view, select **Destination>SIP Registrar** to evaluate the SIP Registrar for matches.



Step 7: snom SIP Registration

On the VX, enter **sho reg** at the command prompt to confirm the snom SIP registration.

```
UCdemo# sho reg

Item TG# Address of Record   Contact Address                NAT Address           Expires   TransportType
====== === ================ ============================== ===================== ========= ============
1    1   1234               1234@10.1.1.109:2084             0.0.0.0               3618s          TLS
```

Generating a Self-Signed Certificate

If you do not have a DNS server or Certificate Authority, you must use a self-signed certificate. You can create the self-signed certificate on VX, as described in the steps below, and the certificate will automatically install itself.

Step 1: Generate the Certificate

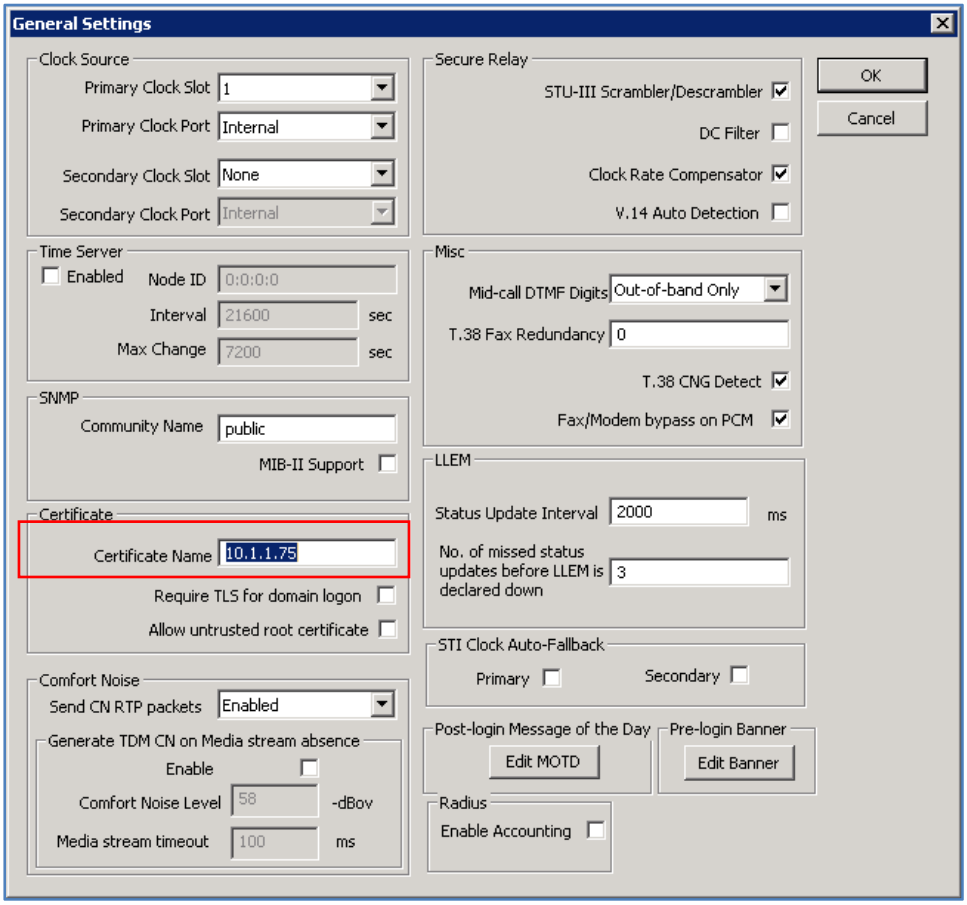
1. From the VX command prompt, enter **`gen cert sel`**. A dialog displays asking for general information to generate the certificate.

2. Enter the requested information, noting the **Common Name** of the certificate must be the IP address of the system.

```
UCdemo# gen cert sel
Please input the following information to create a certificate with.
Common Name should be provided at the minimum.

Enter the Common Name (Subject Name): 10.1.1.75
Enter your email address: trop@hls.com
Enter the Organization Name: NET
Enter Locality: Fremont
Enter the State: CA
Enter the Country: US
Generating a certificate was successful.

UCdemo# sho cert
Issued To                    Issued By                    Type        Generation          Expiration

---------------------------- ---------------------------- ----------- ------------------- -------------------
                  10.1.1.75                    10.1.1.75 self-signed  7/17/2009 17:13:44  7/17/2010 17:13:44
```

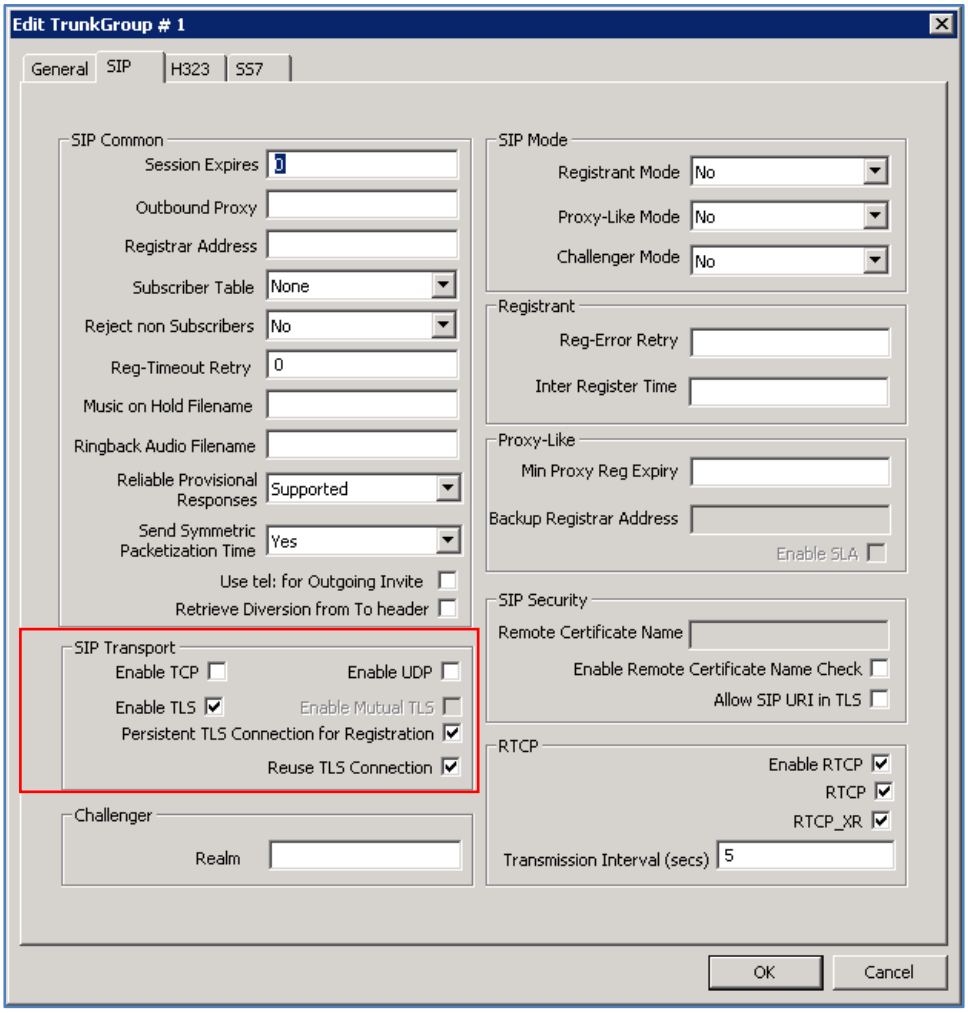
Step 2: VX Settings

On the VX General Settings view, enter the **Certificate Name**.



Step 3: Trunk Group Settings

On the VX Edit TrunkGroup # 1 view, SIP Tab, select **Enable TLS**, **Persistent TLS Connection for Registration**, and **Reuse TLS Connection.**

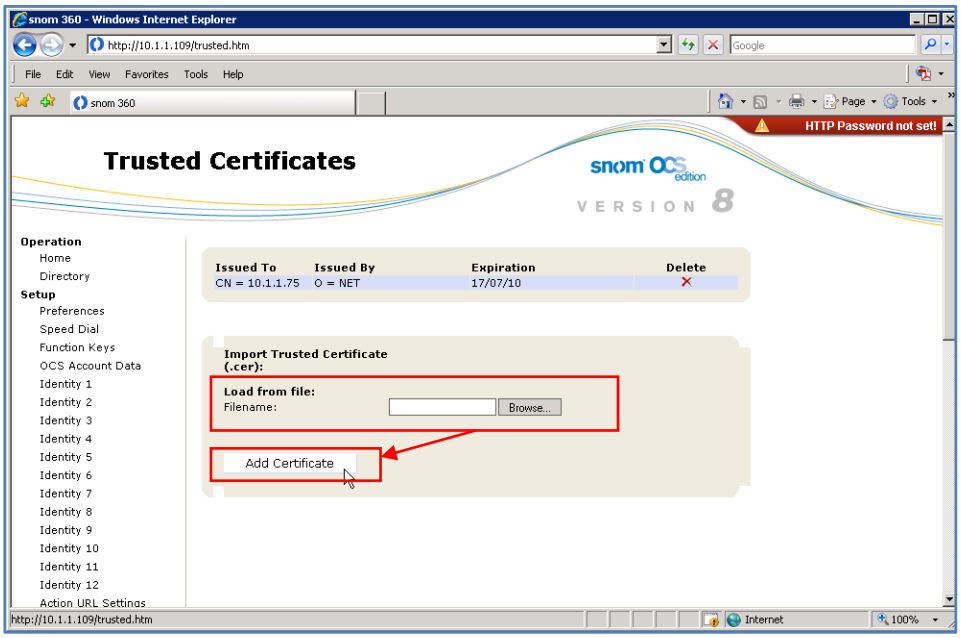


Step 4: Export the Self-Signed Certificate

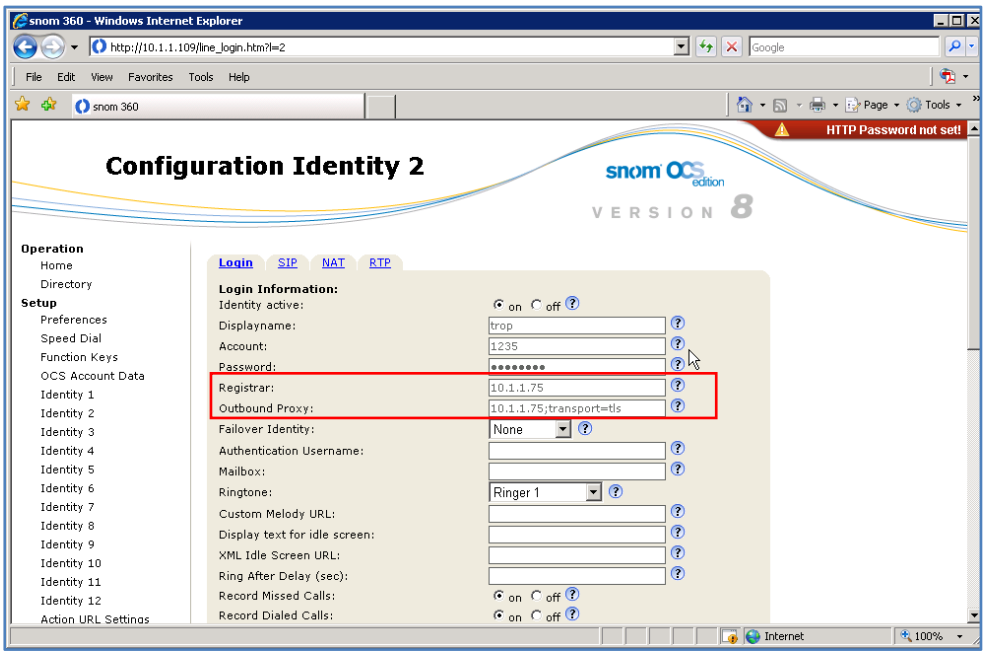
1. Use VXbuilder's Manage File or FTP to move the file to your PC.

2. From the snom Trusted Certificates view, browse the **Load from file:** and locate the self-signed certificate file.

3. When you have located the VX self-signed certificate, click **Add Certificate**. The certificate is now added to your snom phone.



4. On the snom Login Tab, the certificate Common Name is 10.1.1.75. This applies to the **Registrar** and **Outbound Proxy**, with the Outbound Proxy also including **`;transport=tls`** which enables TLS.



Configuring OCS Mediation snom with VX Registrar Fallback

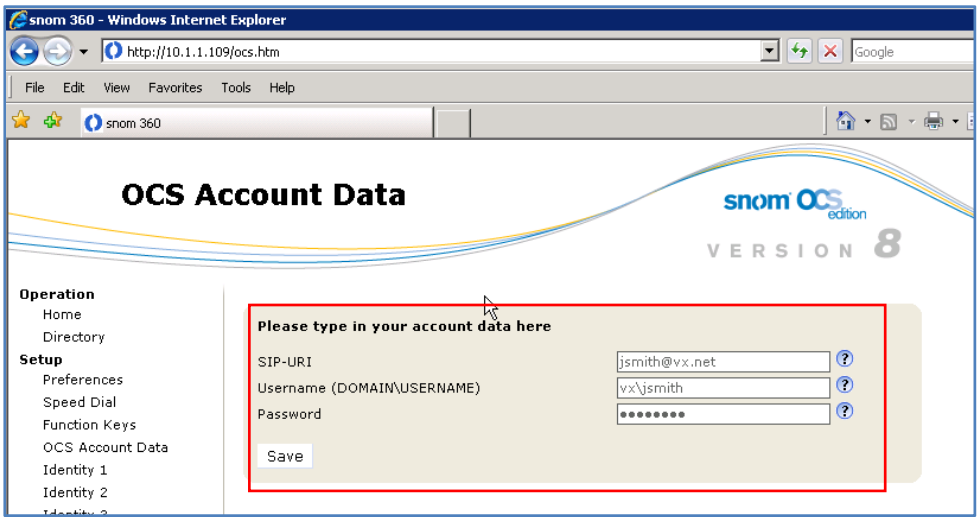
Note: Switchover is slow on the loss of OCS Mediation. The snom phone seems to take some time to perform the switchover, although calls will still attempt to use mediation until the actual failover on the phone occurs.

Note: Previous versions of snom software have been known to have issues. Always have the latest version of software updates to avoid potential problems.

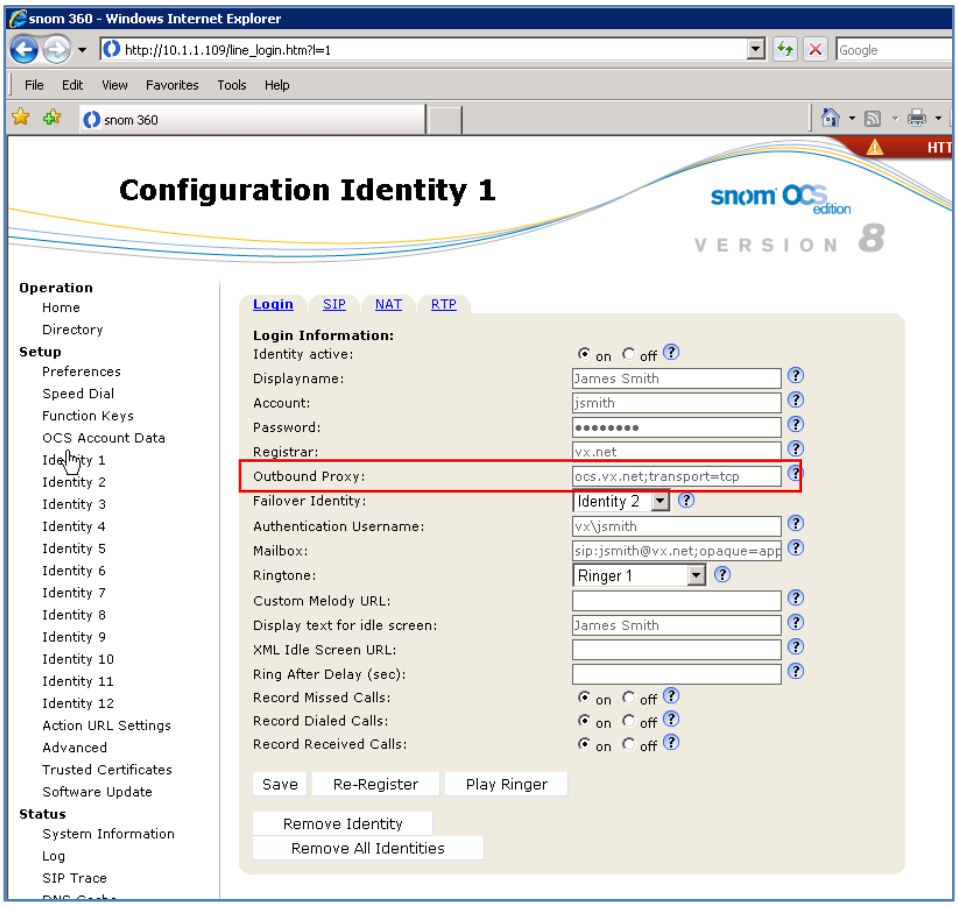
Step 1: Setting Up the snom Phone

1. Start-up your snom phone application. The **Welcome to Your Phone!** view displays.

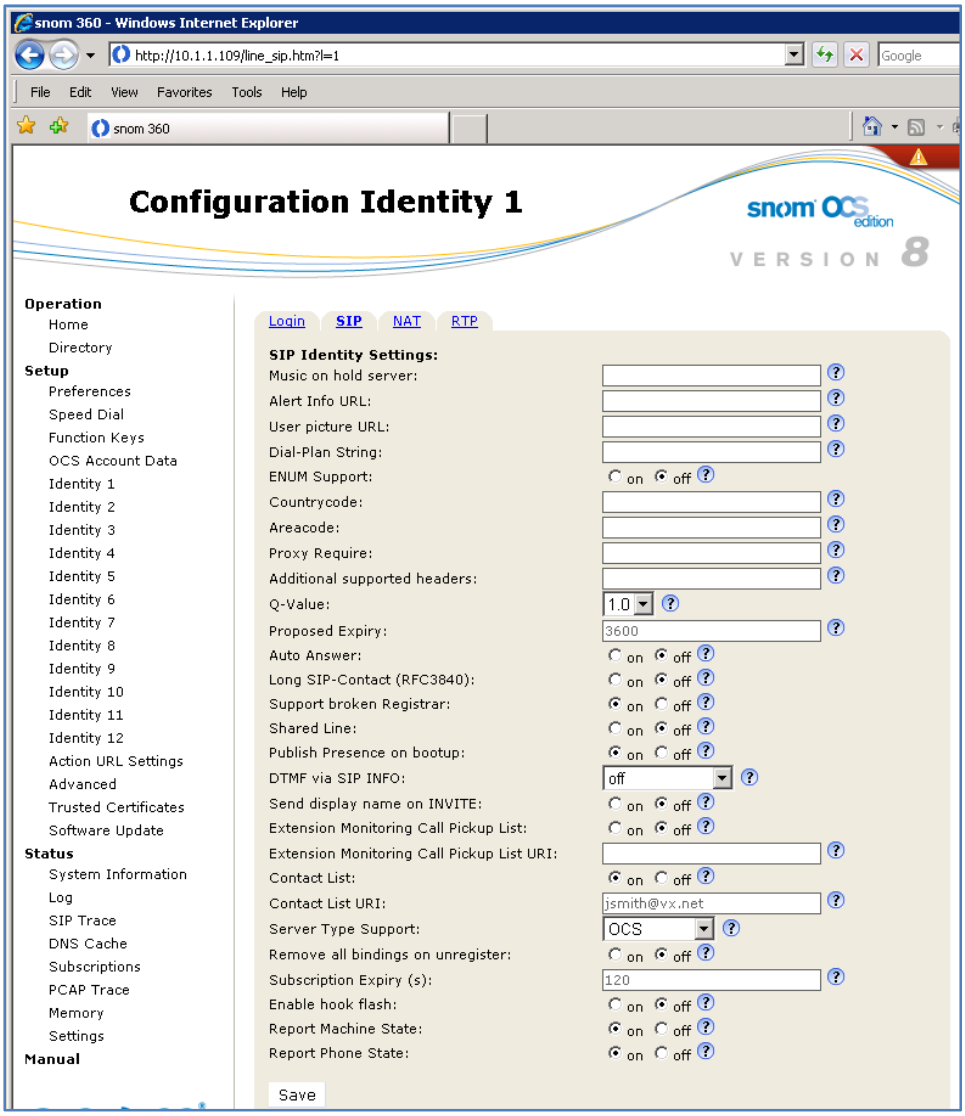
2. To configure the phone for OCS, from the navigation tree located in the left pane select **Setup>OCS Account Data**. The OCS Account Data view displays showing the OCS Identity with the SIP Registrar backup identity**.** Click **Save** to continue.



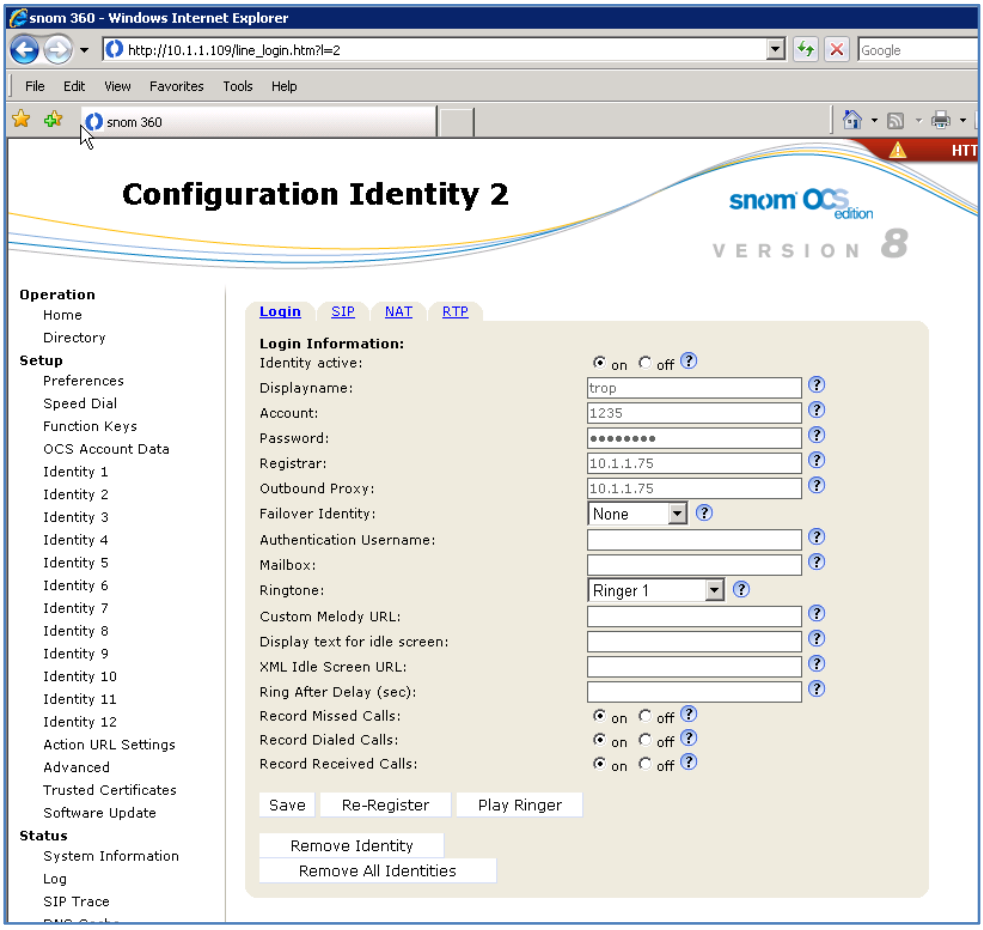
3. From the navigation tree select **Setup>Identify 1** and in the right pane select the **Login tab**. The **Configuration Identity 1** view displays. Listed under **Login Information** is the **Outbound Proxy**: **ocs.vx.net;transport=tls**, which shows it has been tested and found to be working.



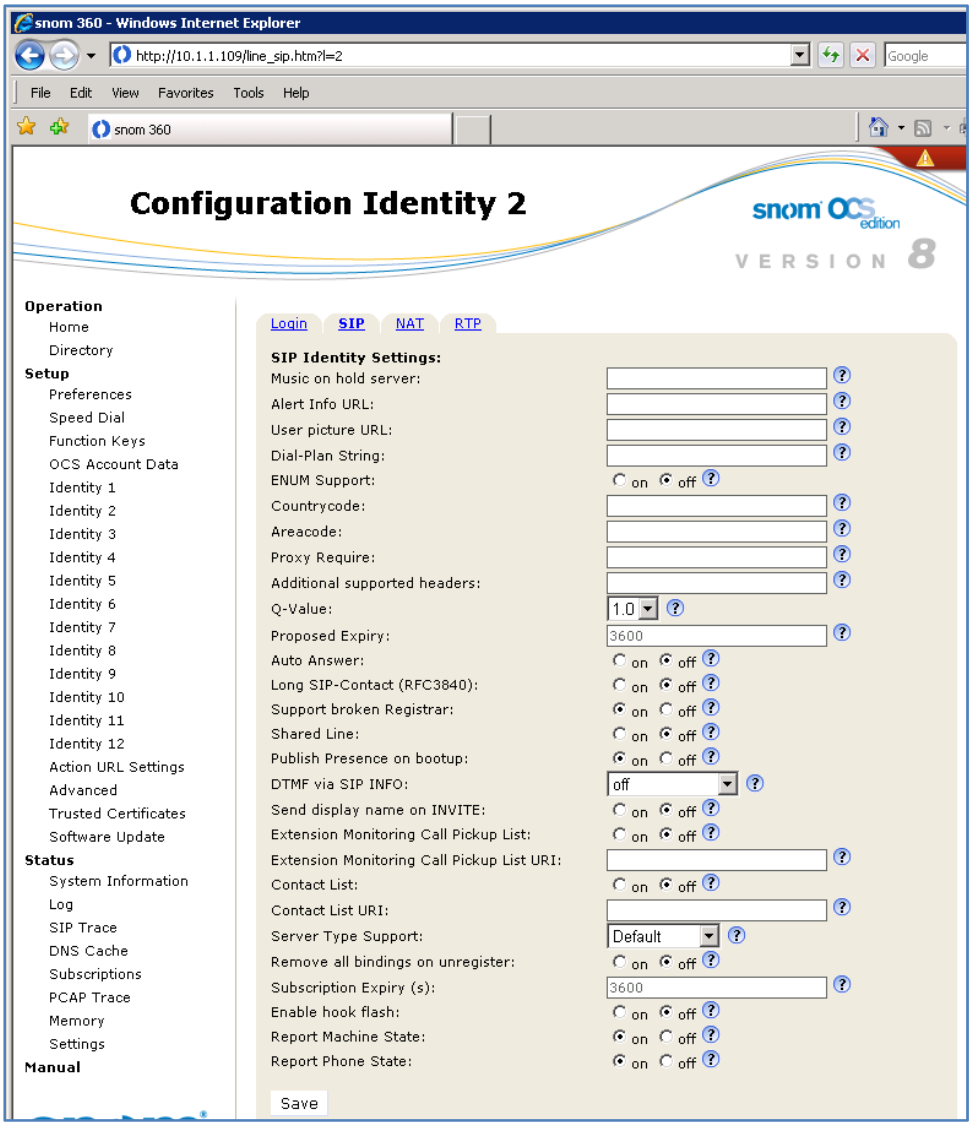
4. In the right pane, select the **SIP tab** to display the SIP configuration settings for Identity 1. This configures the phone to login as a communicator to OCS.



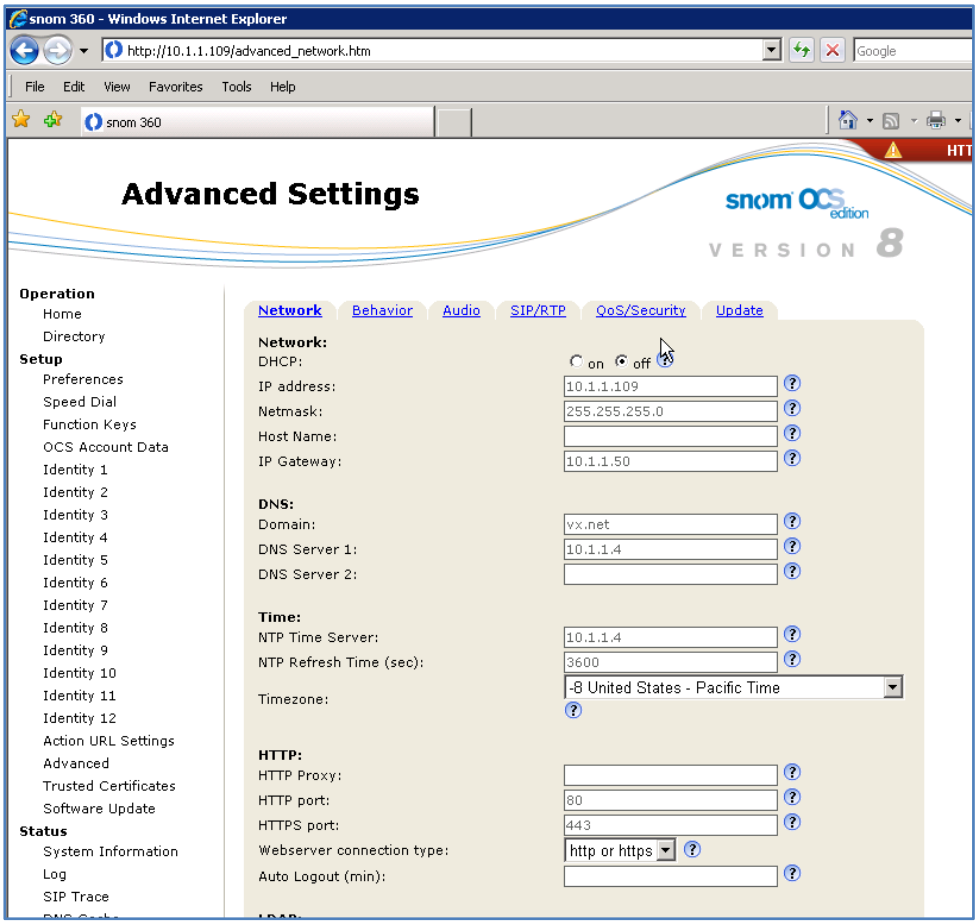
5. Configure Identity 2 as a backup in case of OCS failure. From the navigation tree, select **Identity 2** and the **Login tab**.



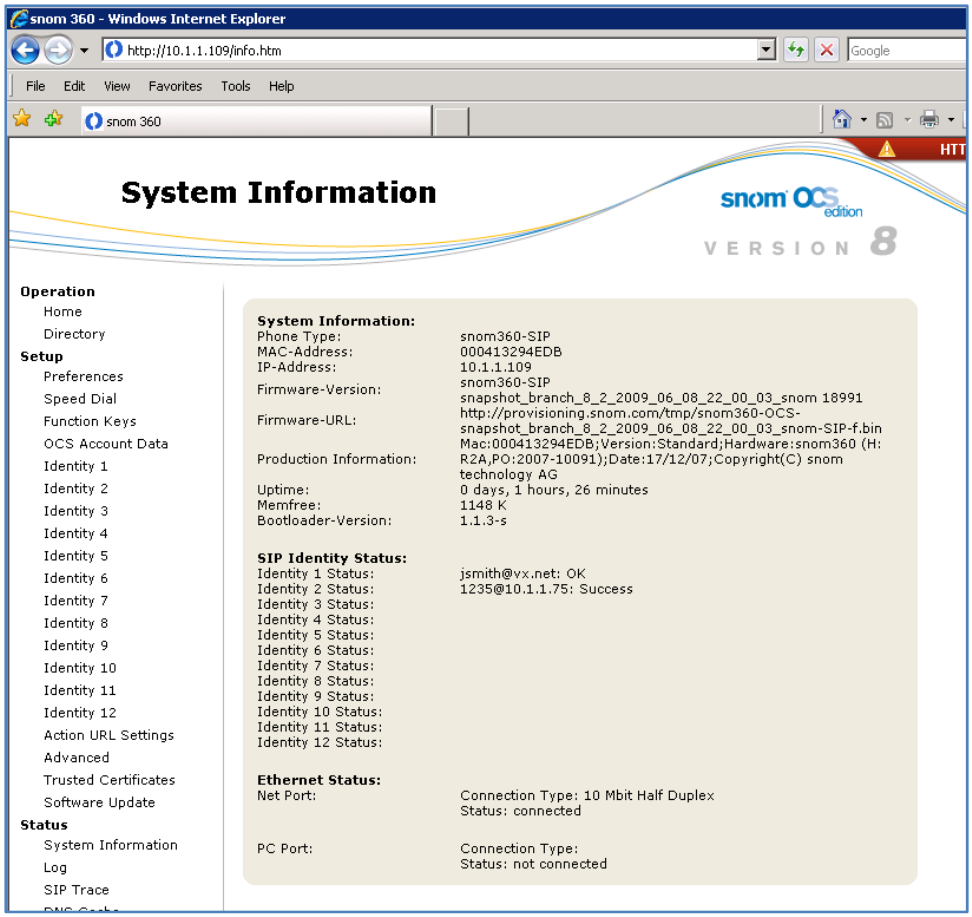
6. In the right pane, select the **SIP tab** to display the SIP configuration settings for Identity 2. This configures backup for the phone to login as a communicator to OCS.



7. In the navigation tree, select **Advanced** and the Advanced Settings dialog displays.

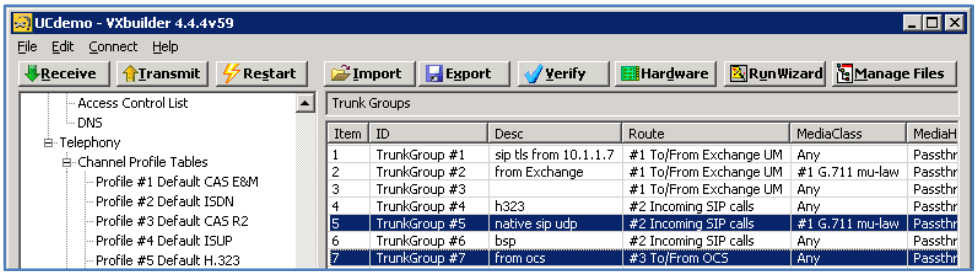


8. View System Information to confirm your settings.

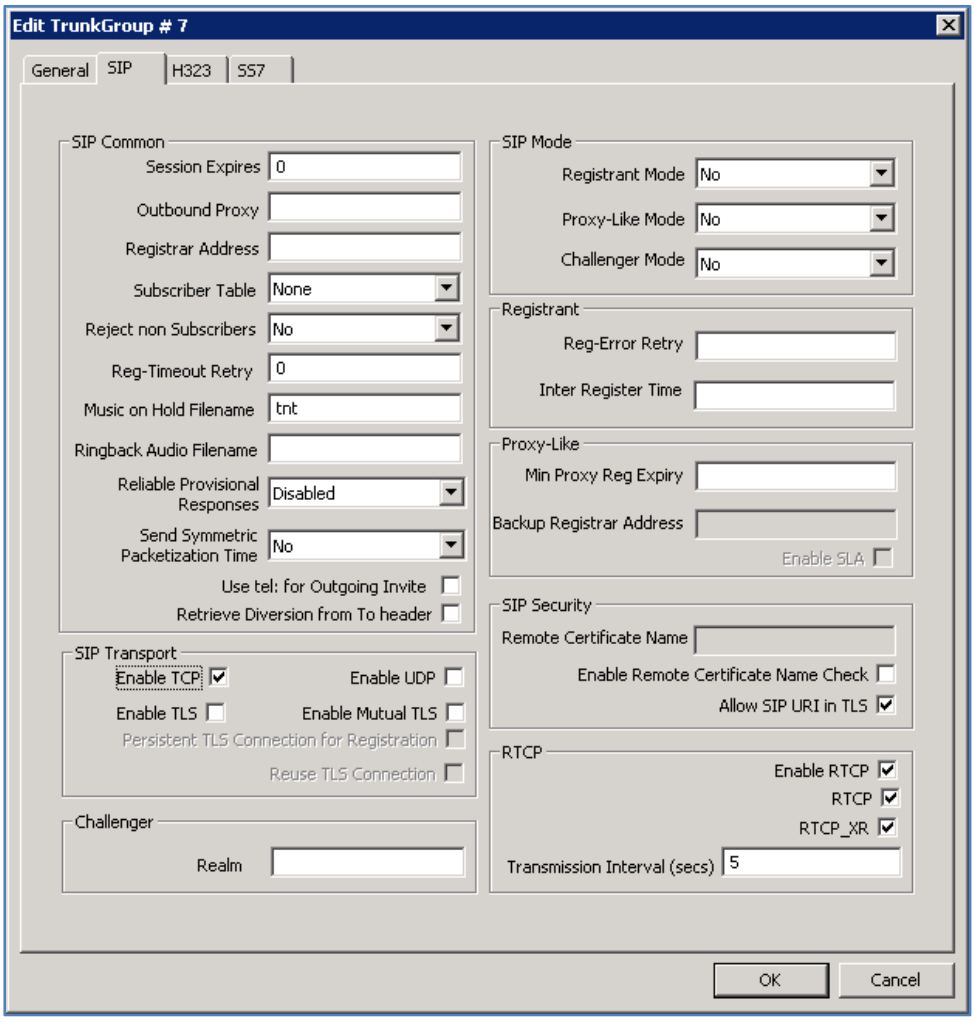


9. Your snom phone is now ready to use.

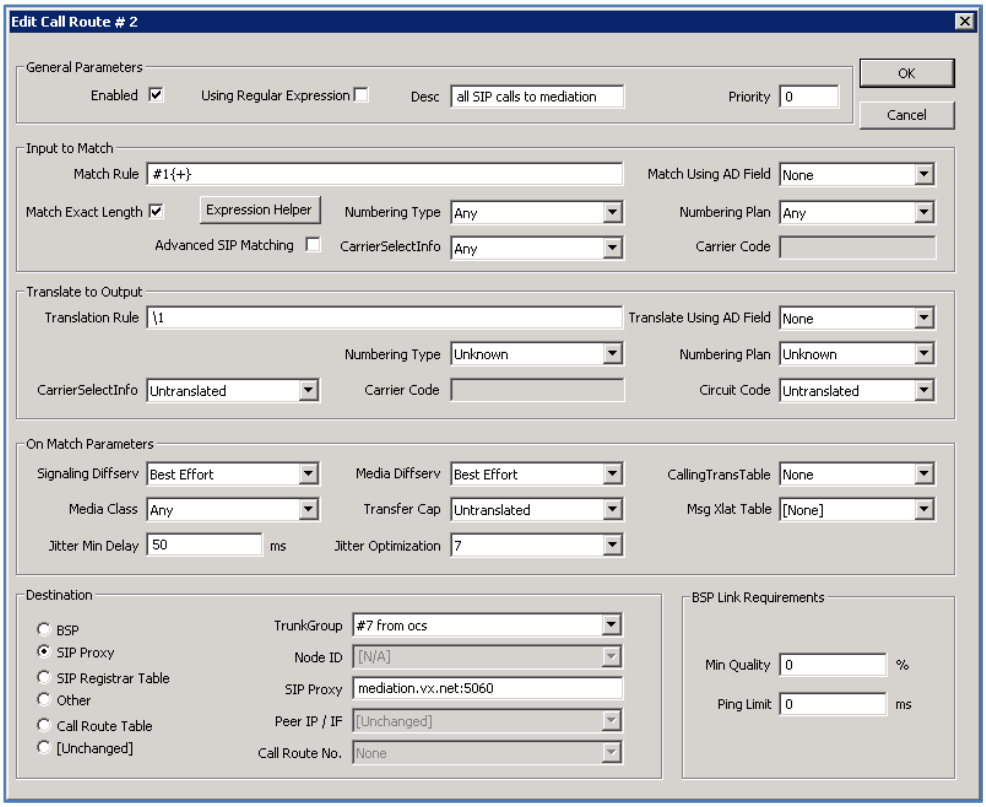
10. On VXbuilder, you can view the Trunk Groups and Calls from the snom MOC/OCS/Mediation to eyeBeam.



11. Mediation via TCP Transport .

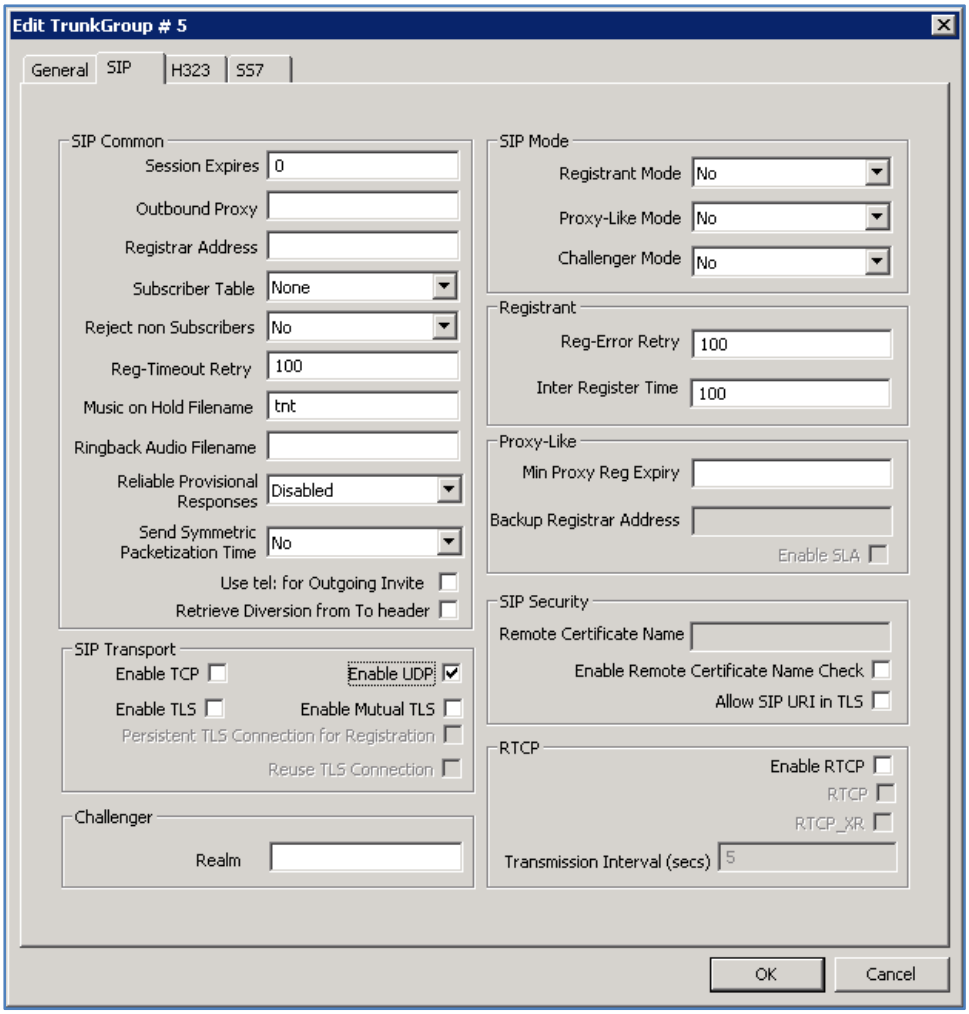


12. Call Route to Mediation from Eyebeam.

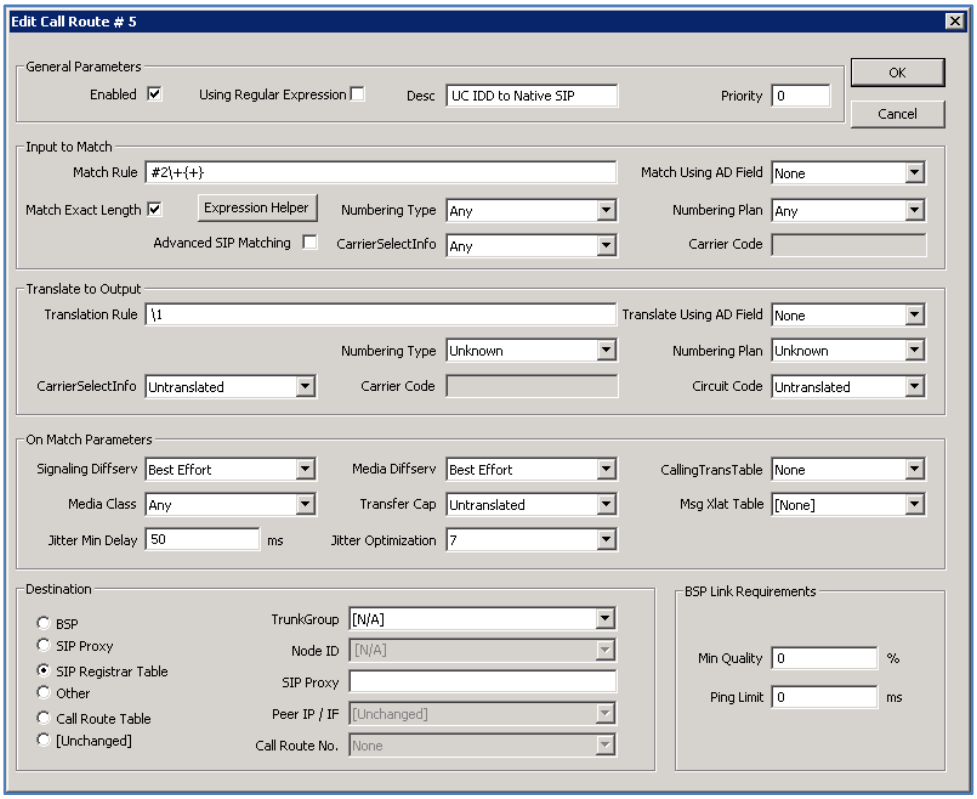


Note: #1 is prepended to the called number by the VX AD integrated scripts. Calls routes without AD integration do not require a prepend prefix.

13. SIP Registrar Trunk Group.



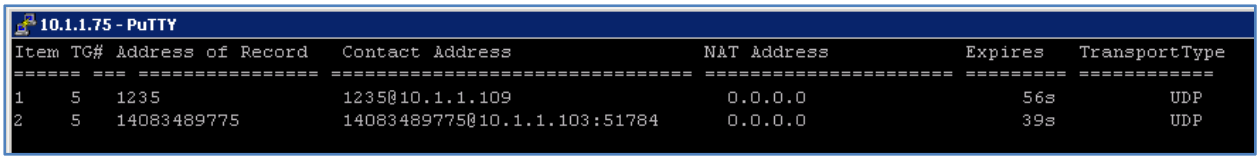
14. Call Route to SIP Registrar.



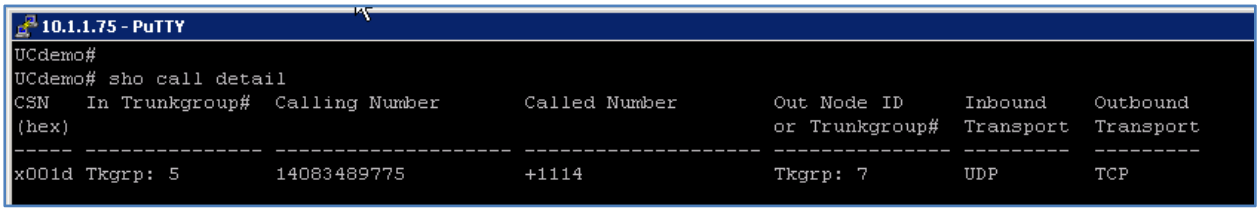
Note: #2 is prepended to the called number by the AD integrated scripts. It may be removed for calls not employing the scripted AD integration.

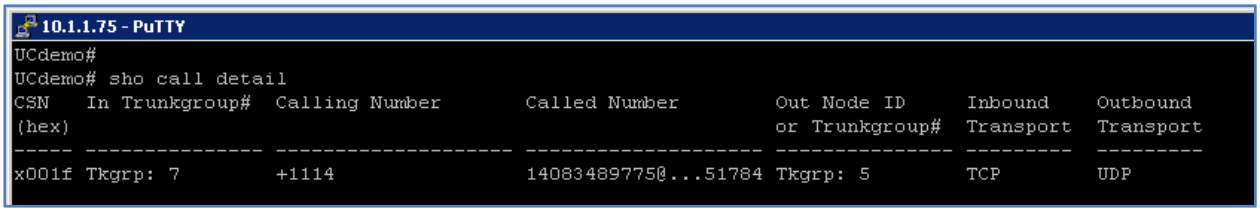
Examples

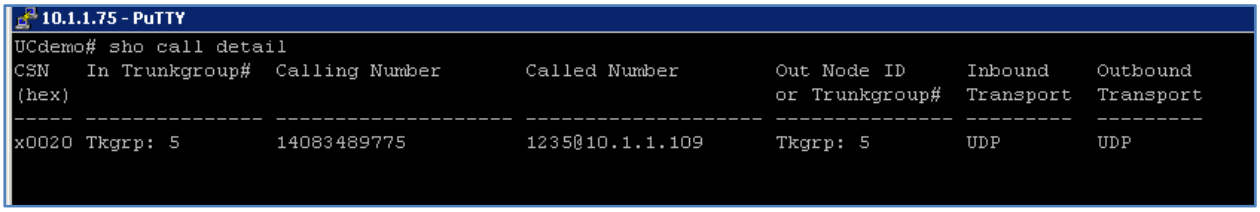
VX Registrar

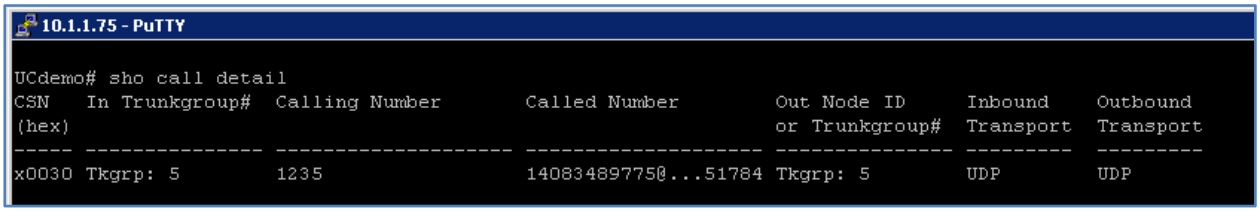


Calls between snom Phone <> eyeBeam



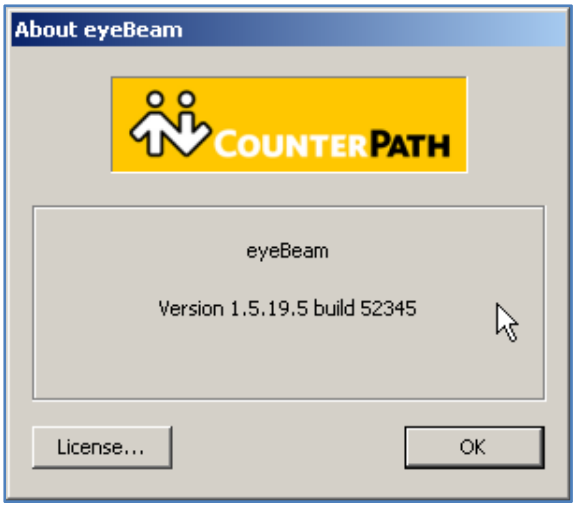






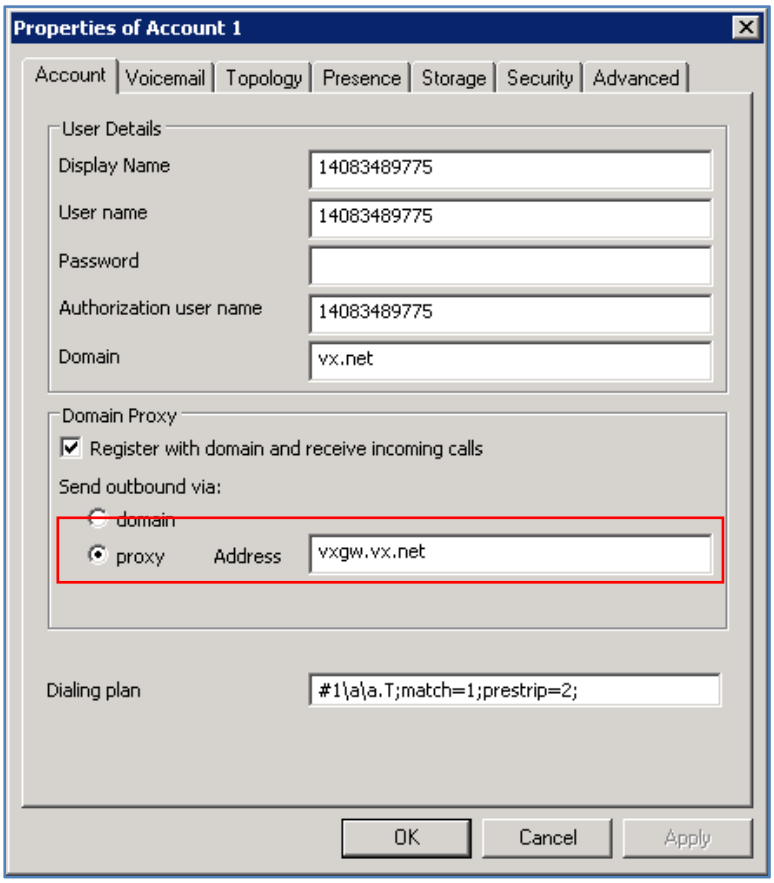
Configuring TLS on eyeBeam

eyeBeam with TLS is similar to other TLS clients. The most important task is to import to the PC the **root certificate** from the Certificate Authority that signed the VX certificate.

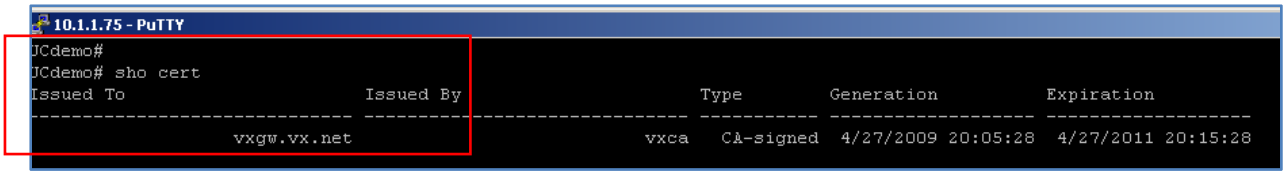


Step 1: eyeBeam SIP Account Configuration

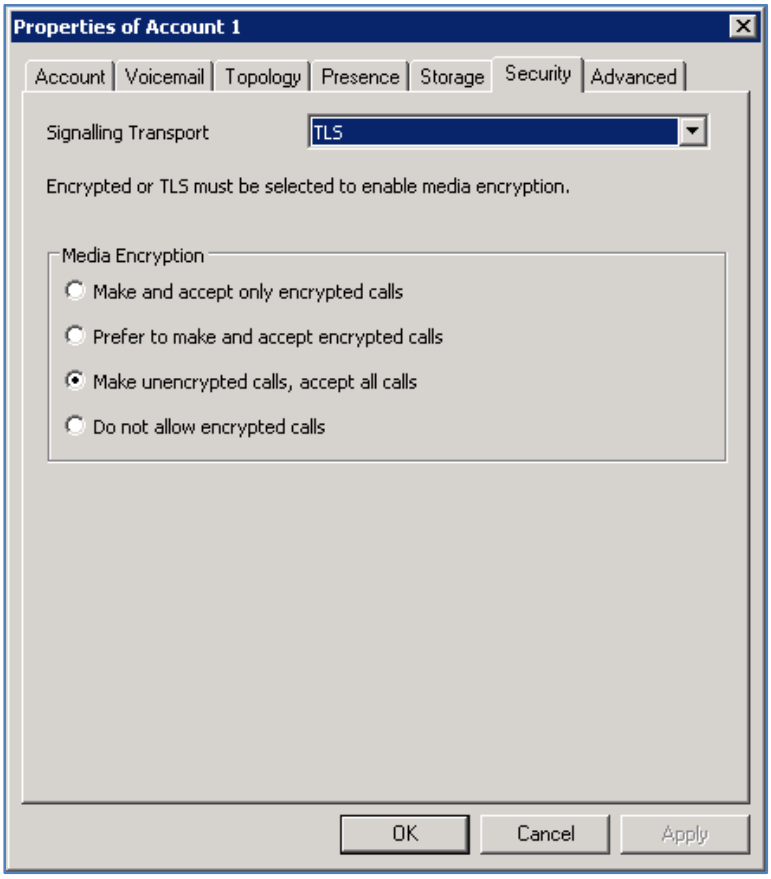
1. Note the **vxgw.vx.net** address to the proxy. This entry must be the same as the Common Name of the certificate installed on the VX.



2. You can also display the certificate name by entering **sho cert** at the VX command prompt.



Step 2: eyeBeam Security Settings

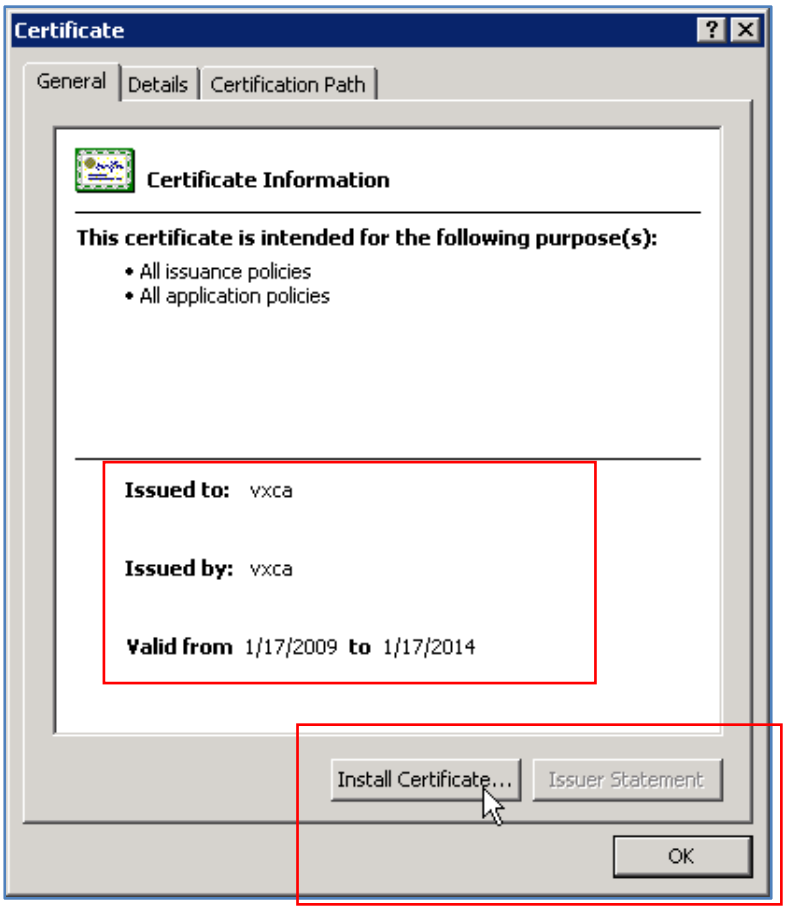


Step 3: Importing the Root Certificate to the eyeBeam PC

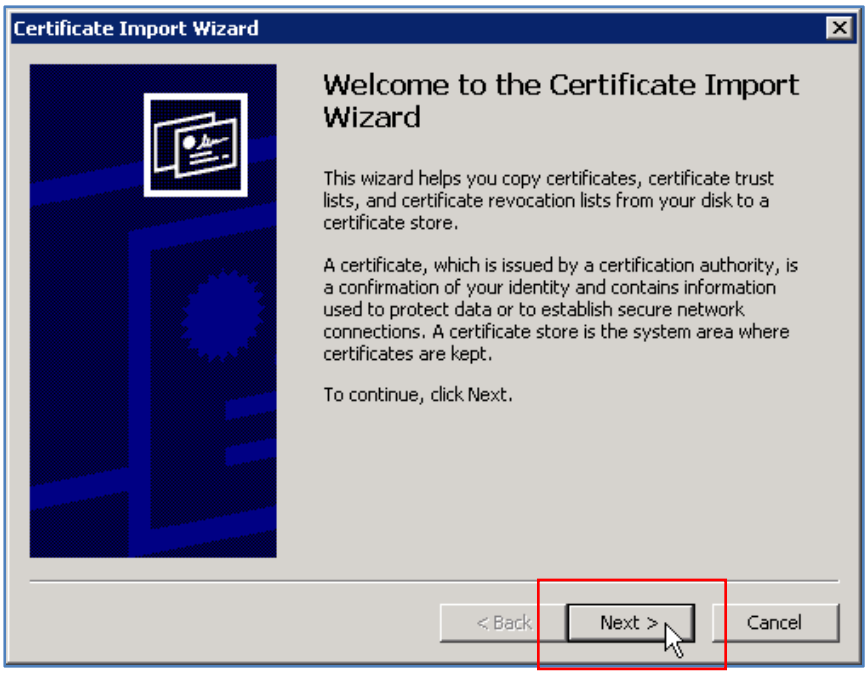
1. Transfer to the PC the **root certificate** of the Certificate Authority that signed the **vxgw.vx.net** certificate.

2. On the Certificate view, General Tab, Double click **Install Certificate** to install the certificate using the following instructions.

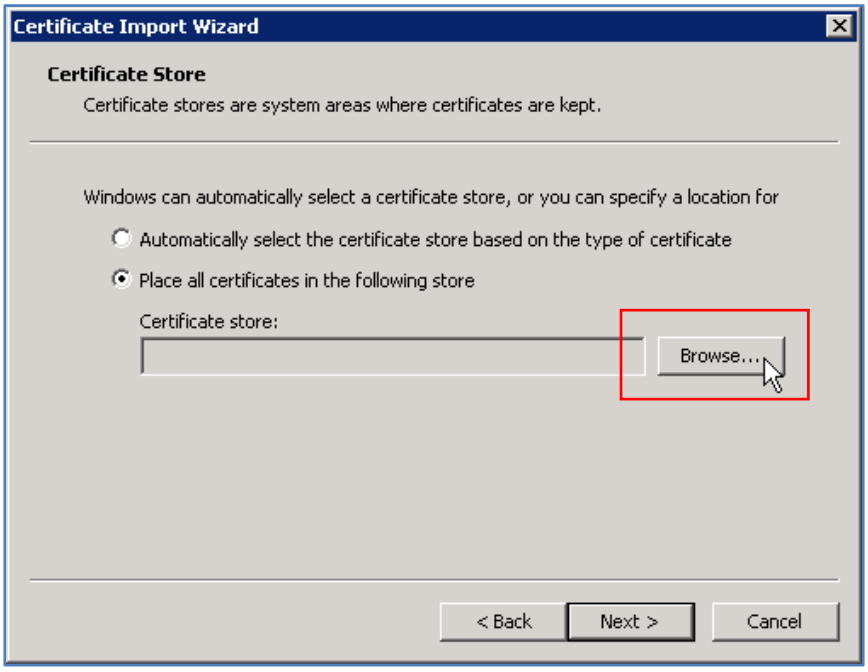
   a. **vxca** is the root certificate from the Certificate Authority used to sign the vxgw.vx.net certificate.



3. The **Certificate Import Wizard>Welcome to the Certificate Import Wizard** view displays. Read the text and click **Next** to continue.

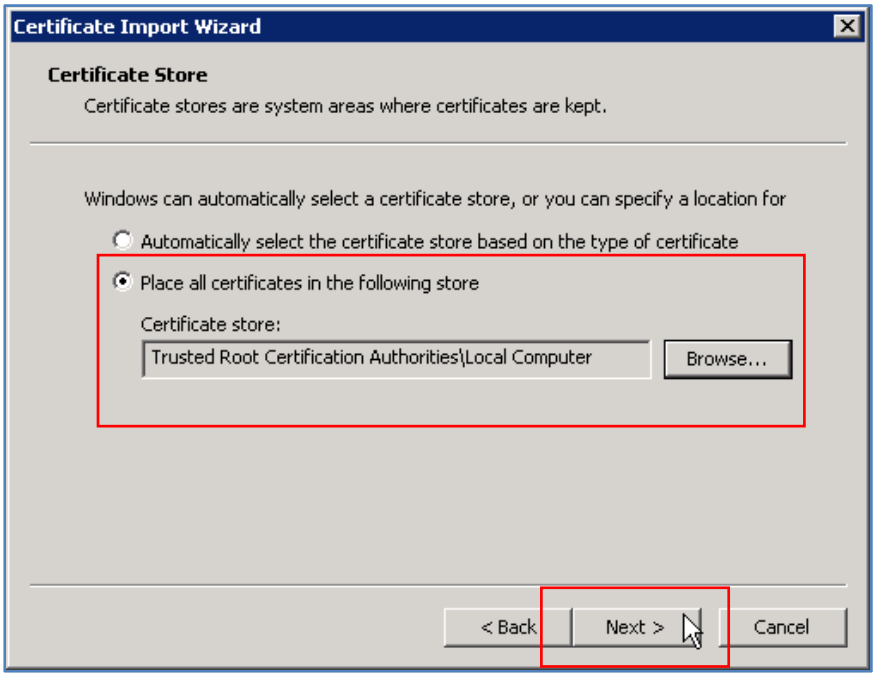


4. **Browse** the Certificate Store to select certificate storage location. Click **Next** to continue.

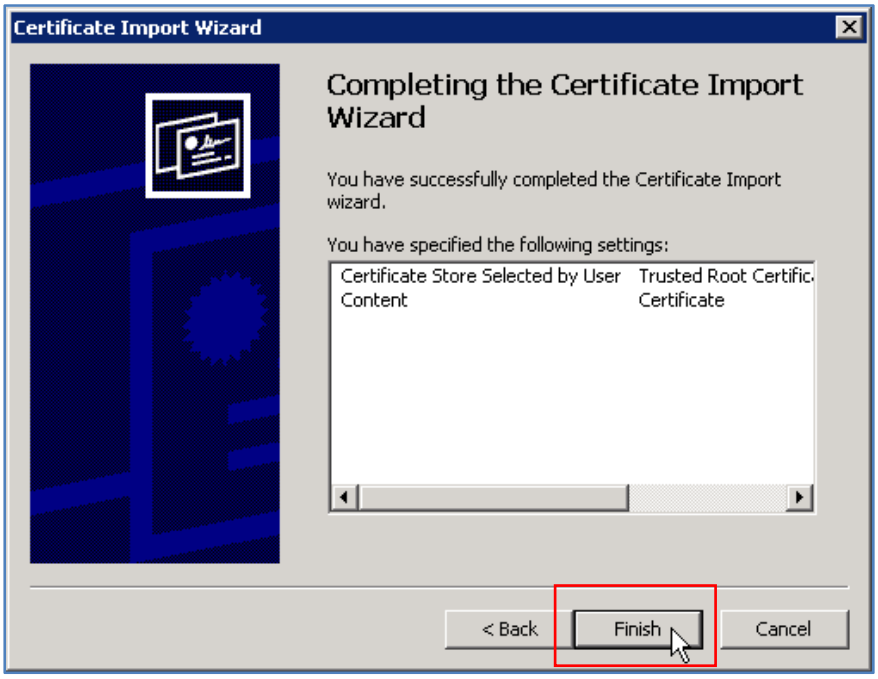


5. Select the **Certificate Store** and click **OK**.

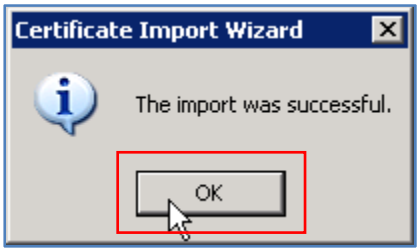
6. Confirm the Certificate Store you have selected, which displays in the **Certificate Store** entry, and click **Next** to continue.



7. Confirm your completion of the Certificate Import Wizard by clicking **Finish**.



8. Acknowledge the import was successful by clicking **OK**.



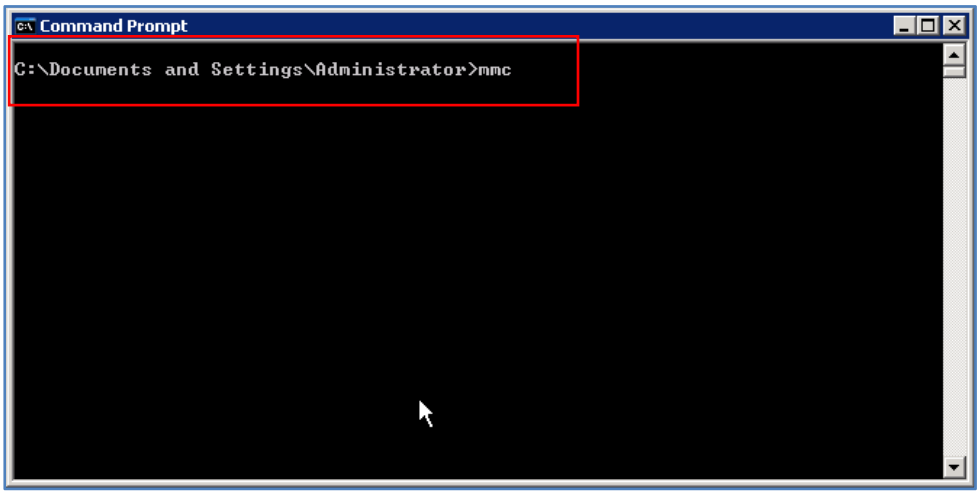
9. You must now **REBOOT your PC** to complete the process. This is a required step to complete the process.

Note: Failure to reboot your PC will invalidate the Certificate Import Wizard steps.

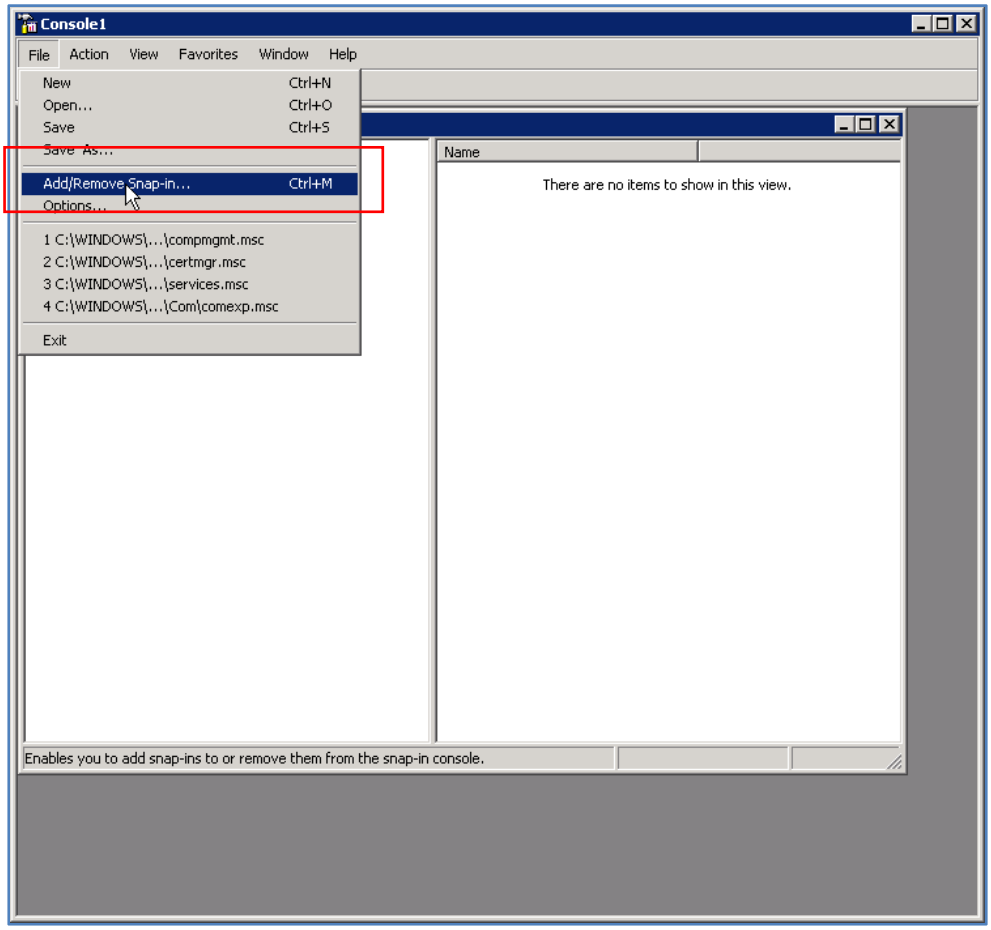
Step 4: Verify Certificate Installation

After rebooting your PC, verify that the root certificate is properly installed. Use the Certificates Snap-in to verify the certificate.

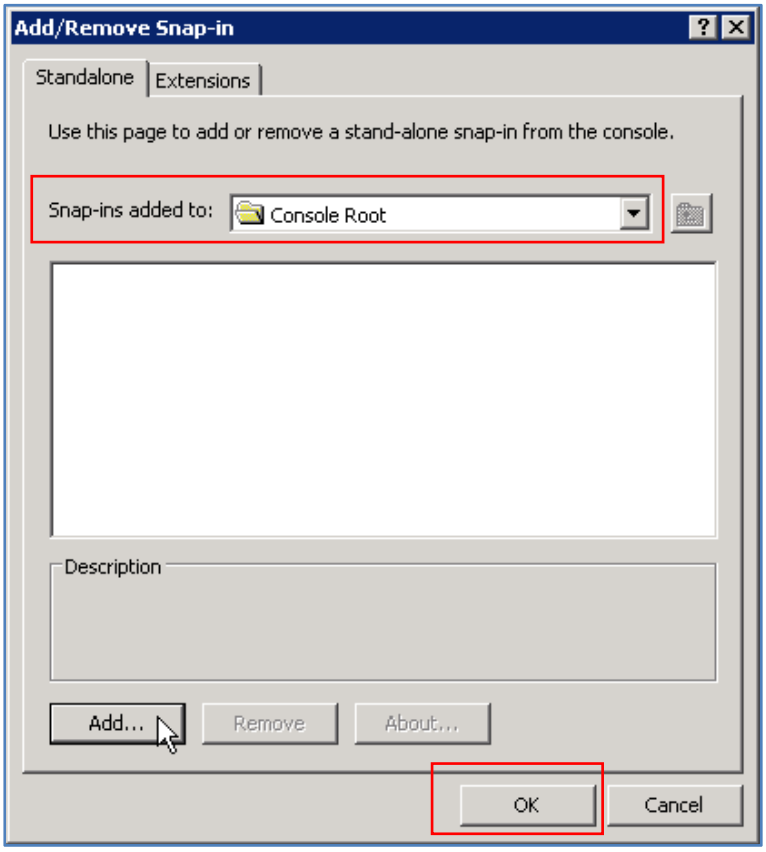
1. At the command prompt, enter **mmc**



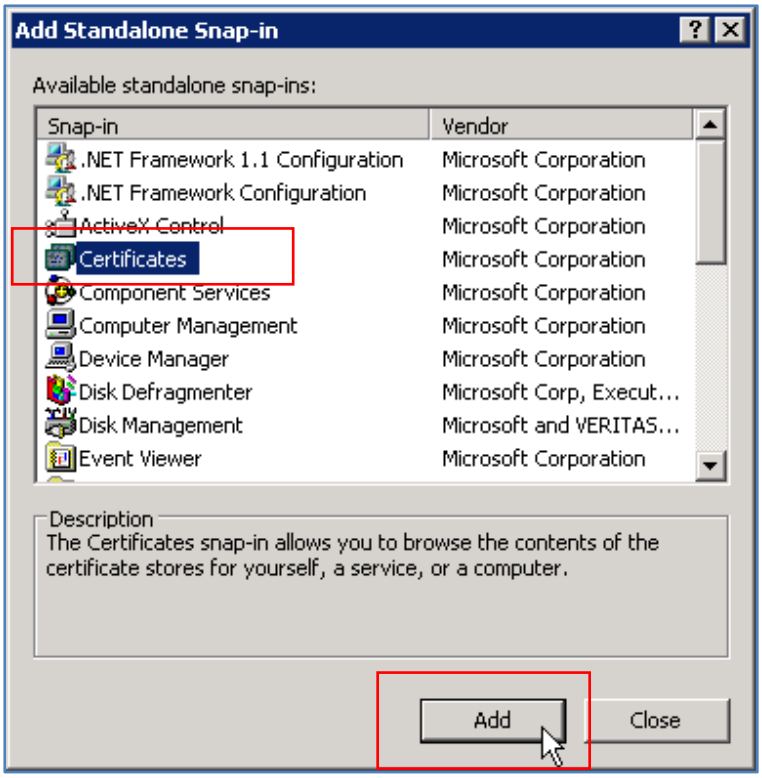
2. At the Console 1 view, select **Add/Remove Snap-In…**



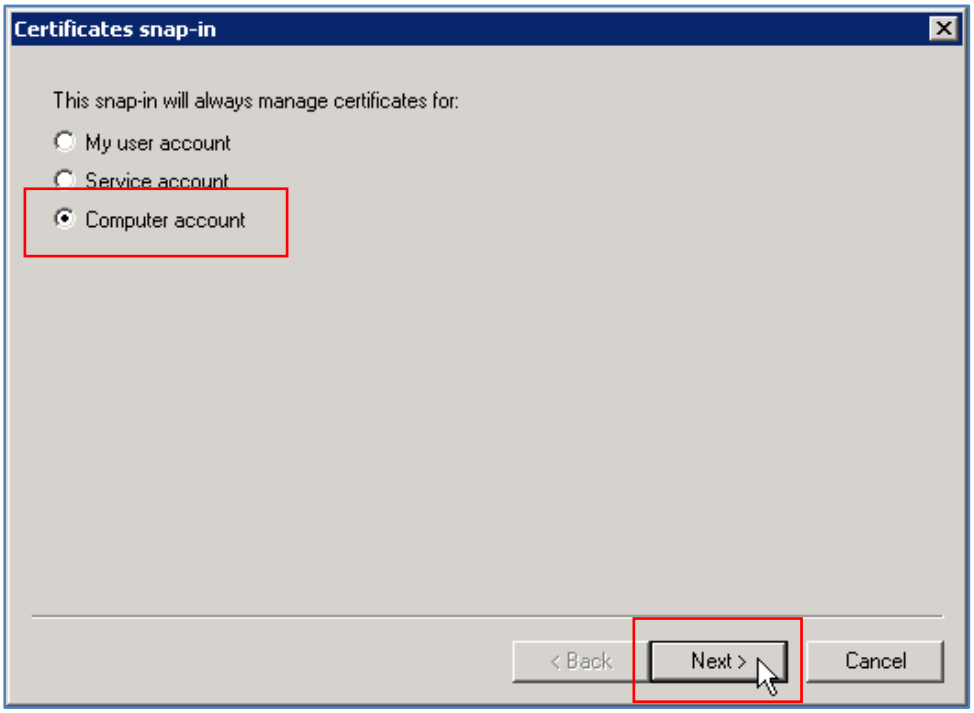
3. From the Standalone Tab, select the **Console Root** folder from the **Snap-ins added to** field. Click **Add** and then **OK**. The Add Standalone Snap-in view displays.



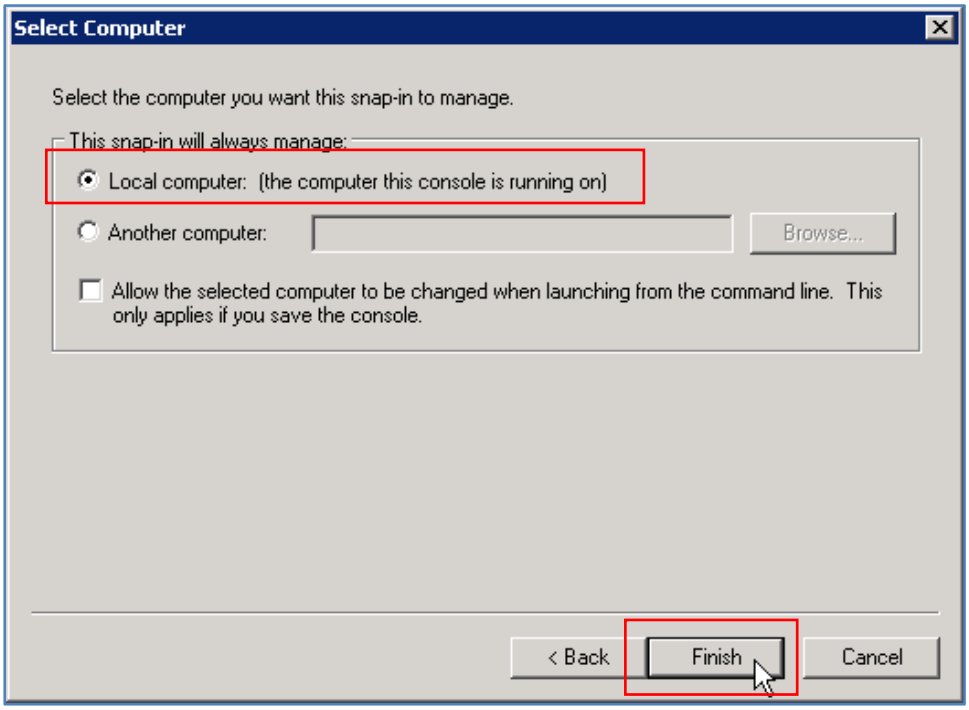
4. Select the **Certificates**, and click **Add**. The Certificates snap-in view displays.



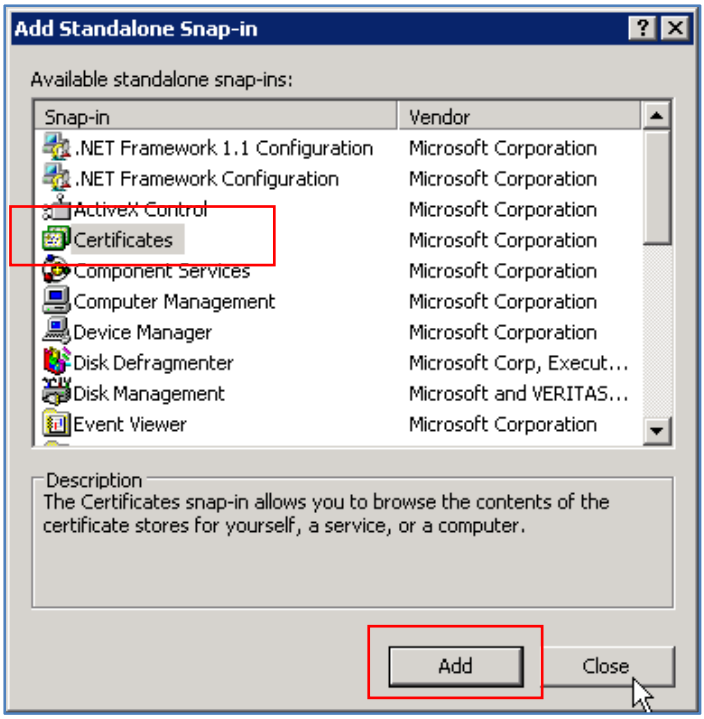
5. Select the radio button for **Computer account** and click **Next**.



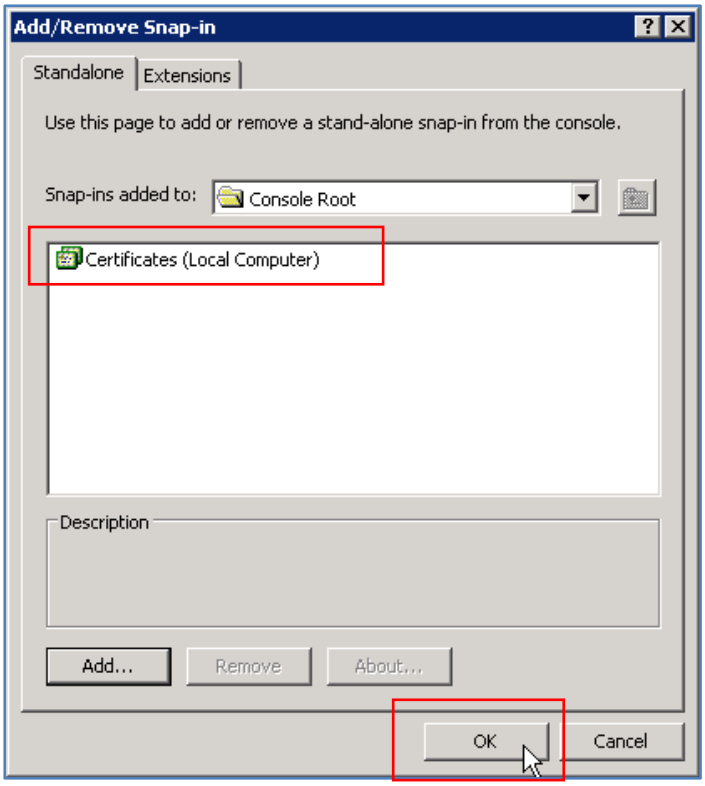
6. Select the radio button for **Local computer** and click **Finish**.



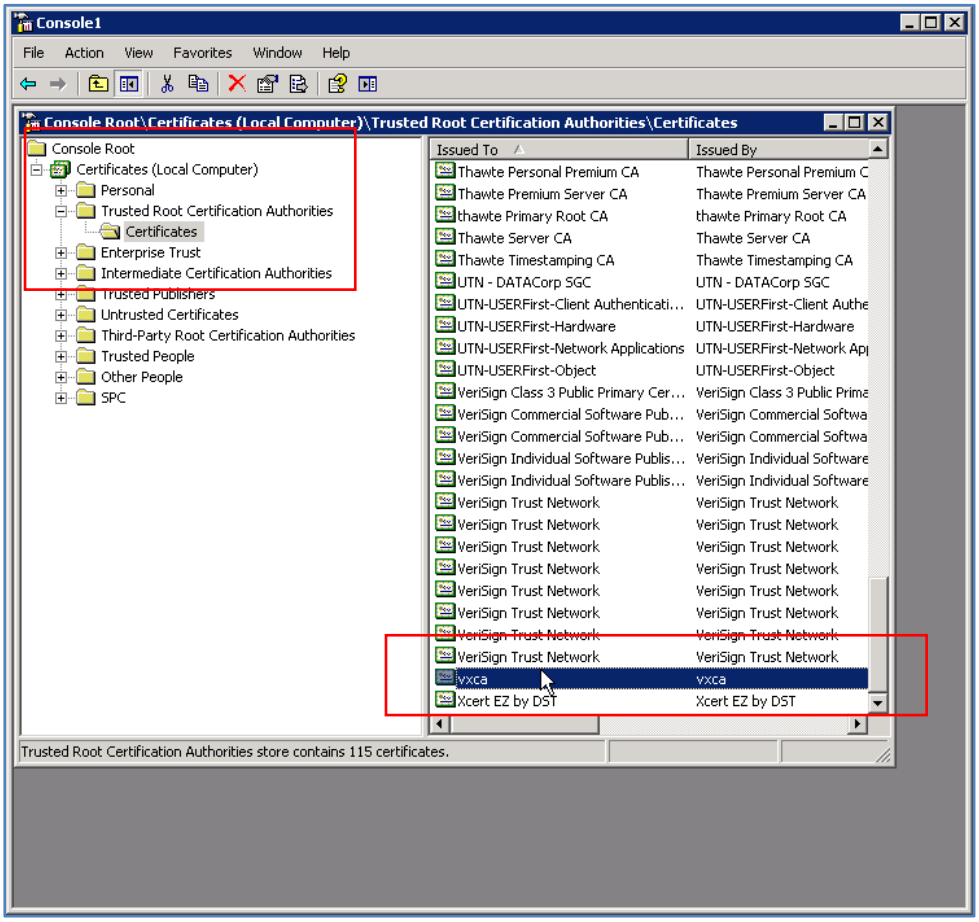
7. From the **Add Standalone Snap-in** view, select **Certificates** and click **Add**.



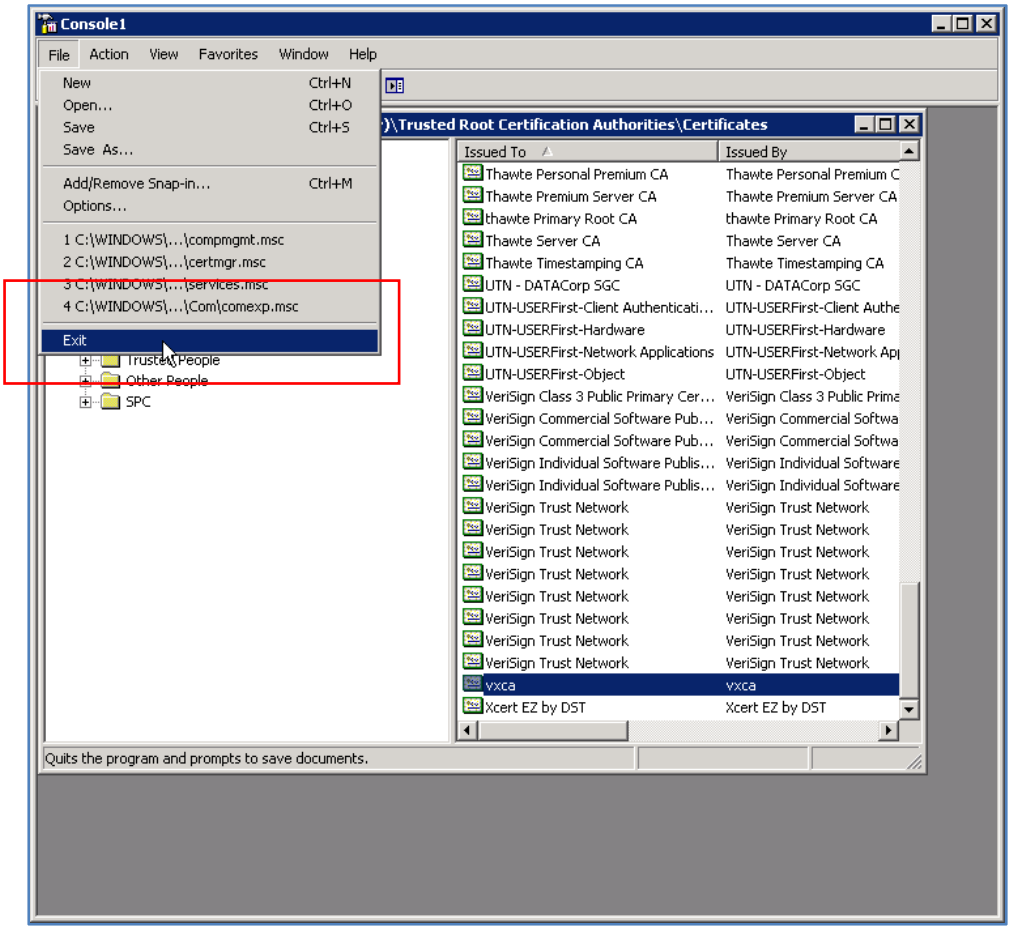
8. From the Standalone Tab, the **Certificates (Local Computer)** Snap-ins display as added. Click **OK**.



9. You can also verify the vxca certificate has been added by viewing the **Console Root>Trusted Root Certifications Authorities>Certificates** folder contents.

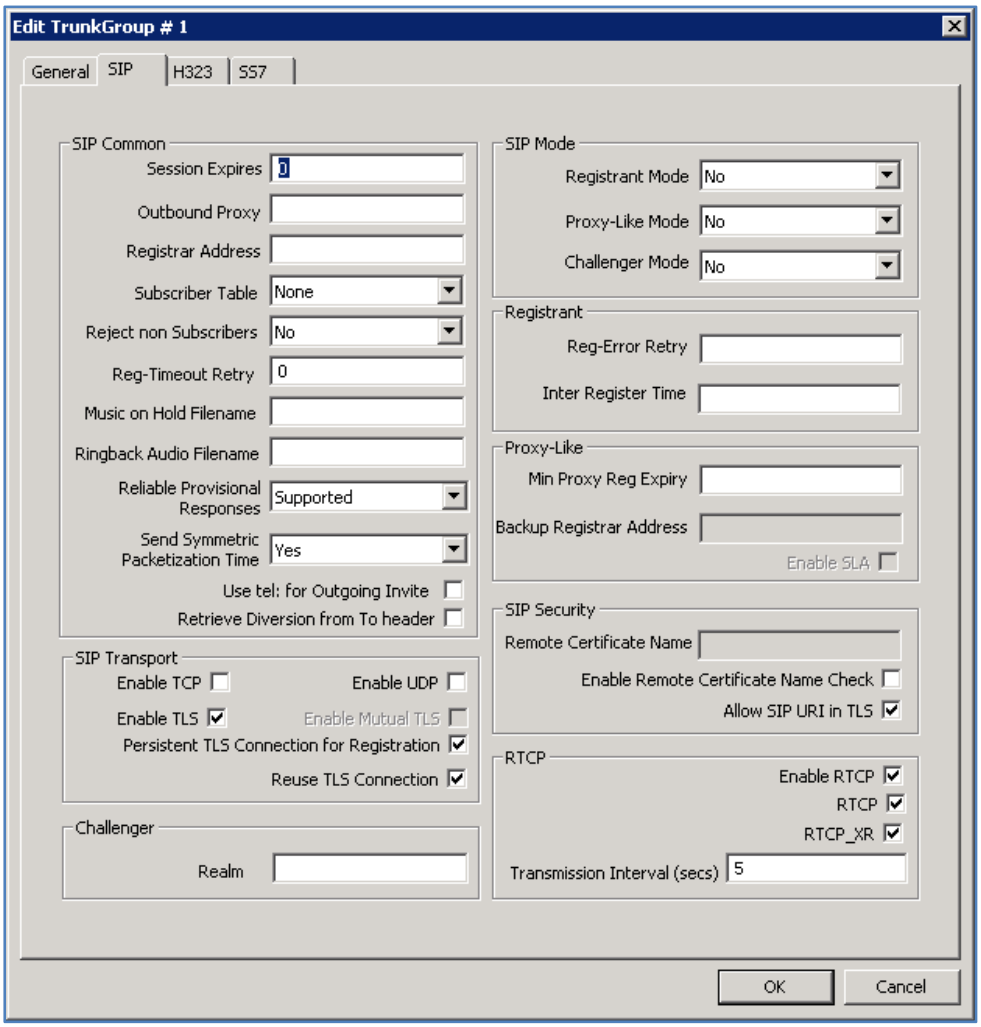


10. **Exit** the console.



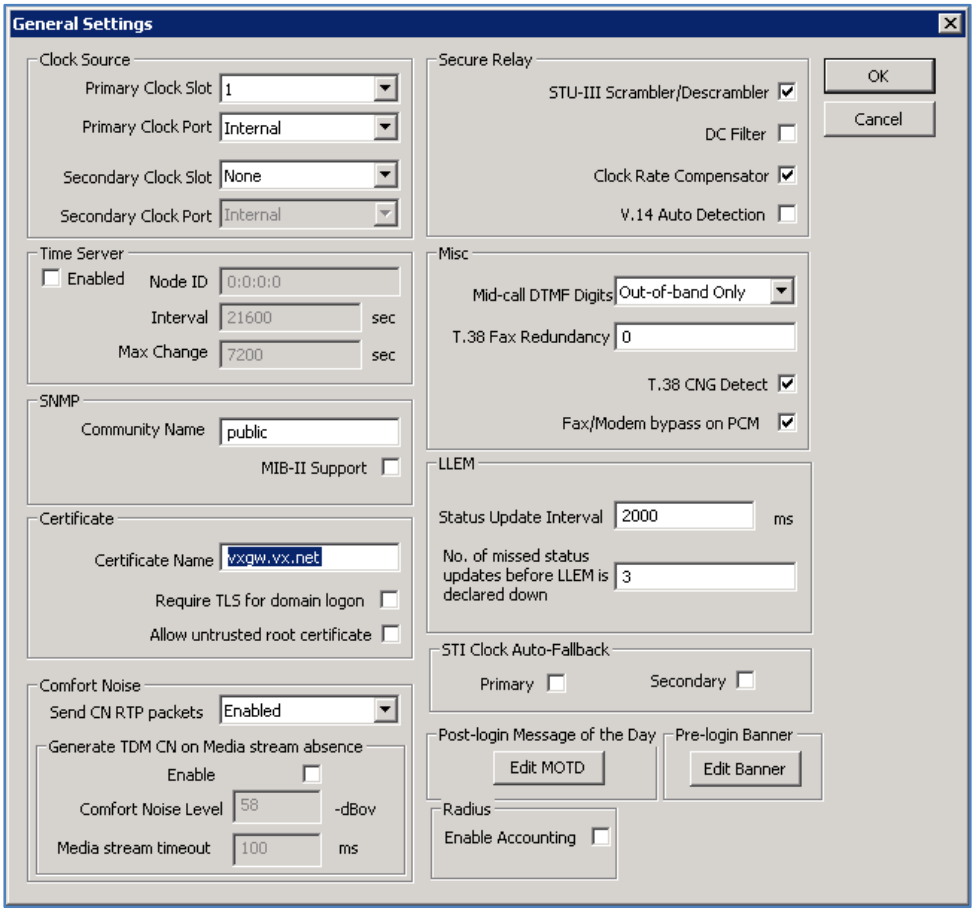
Step 5: VX Configuration

A TLS-configured Trunk Group.



Step 6: VX General Menu

The `vxgw.vx.net` installed certificate.



Step 7: eyeBeam TLS to snom Calls

```
10.1.1.75 - PuTTY
UCdemo#
UCdemo# sho call detail
CSN    In Trunkgroup#  Calling Number       Called Number        Out Node ID     Inbound    Outbound
(hex)                                                           or Trunkgroup#  Transport  Transport
----- --------------- -------------------- -------------------- --------------- ---------  ---------
x0001 Tkgrp: 1        14083489775          1235@10.1.1.109      Tkgrp: 5        TLS        UDP
```

```
10.1.1.75 - PuTTY
UCdemo# sho call detail
CSN    In Trunkgroup#  Calling Number       Called Number        Out Node ID     Inbound    Outbound
(hex)                                                           or Trunkgroup#  Transport  Transport
----- --------------- -------------------- -------------------- --------------- ---------  ---------
x0002 Tkgrp: 1        14083489775          1235@10.1.1.109:2062 Tkgrp: 1        TLS        TLS
```

Step 8: snom TLS Configuration