

Configuration Note

snom 360 Phone with VX for Branch Survivability

Release 1.0



Copyright © 2009 Network Equipment Technologies, Inc. All rights reserved.

NETWORK EQUIPMENT TECHNOLOGIES, INC. (hereinafter referred to as "N.E.T."), PROVIDES THIS DOCUMENT AS IS, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

No part of this publication may be stored in a retrieval system, transmitted or reproduced in any way, including photocopy, photograph, magnetic, or other record, without the prior written permission of N.E.T. Unpublished-rights reserved under the copyright laws of the United States.

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	4
Content	4
Intended Audience.....	4
Configuring snom 360 and VX with TLS	5
Step 1: Install VX Root Certificate onto the snom Phone	5
Step 2: Enter the Configuration Identity.....	6
Step 3: SIP Settings.....	7
Step 4: VX Settings	8
Step 5: Trunk Group Settings	9
Step 6: Call Route	10
Step 7: snom SIP Registration	10
Generating a Self-Signed Certificate	11
Step 1: Generate the Certificate	11
Step 2: VX Settings	12
Step 3: Trunk Group Settings	13
Step 4: Export the Self-Signed Certificate	13
Configuring OCS Mediation snom with VX Registrar Fallback	15
Step 1: Setting Up the snom Phone	15
Examples	26
VX Registrar.....	26
Calls between snom Phone <> eyeBeam	26
Configuring TLS on eyeBeam	27
Step 1: eyeBeam SIP Account Configuration	28
Step 2: eyeBeam Security Settings.....	29
Step 3: Importing the Root Certificate to the eyeBeam PC.....	30
Step 4: Verify Certificate Installation	34
Step 5: VX Configuration	41
Step 6: VX General Menu.....	42
Step 7: eyeBeam TLS to snom Calls	43
Step 8: snom TLS Configuration	43

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).

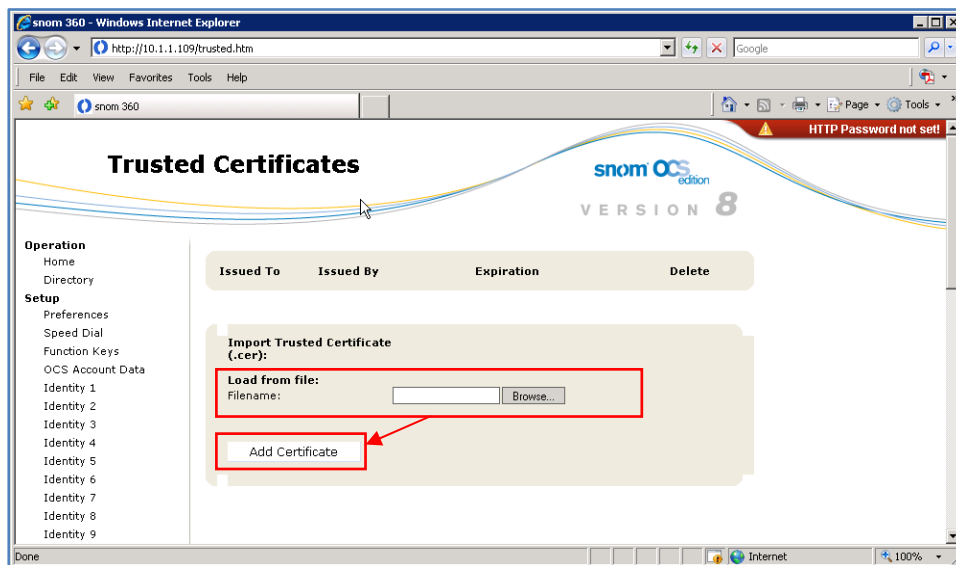
Step 1: Install VX Root Certificate onto the snom Phone

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.

N.E.T.

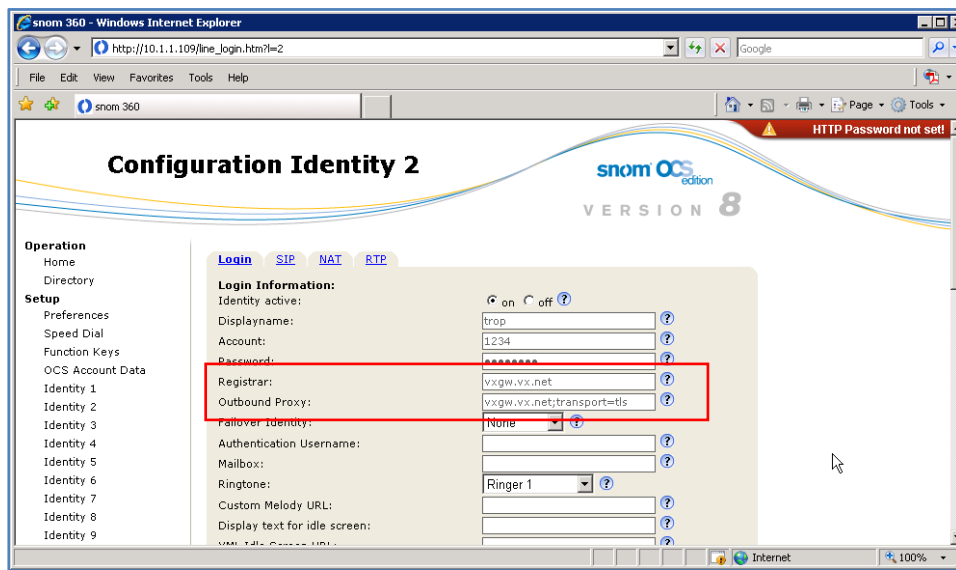
Step 2: Enter the Configuration Identity

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#
```

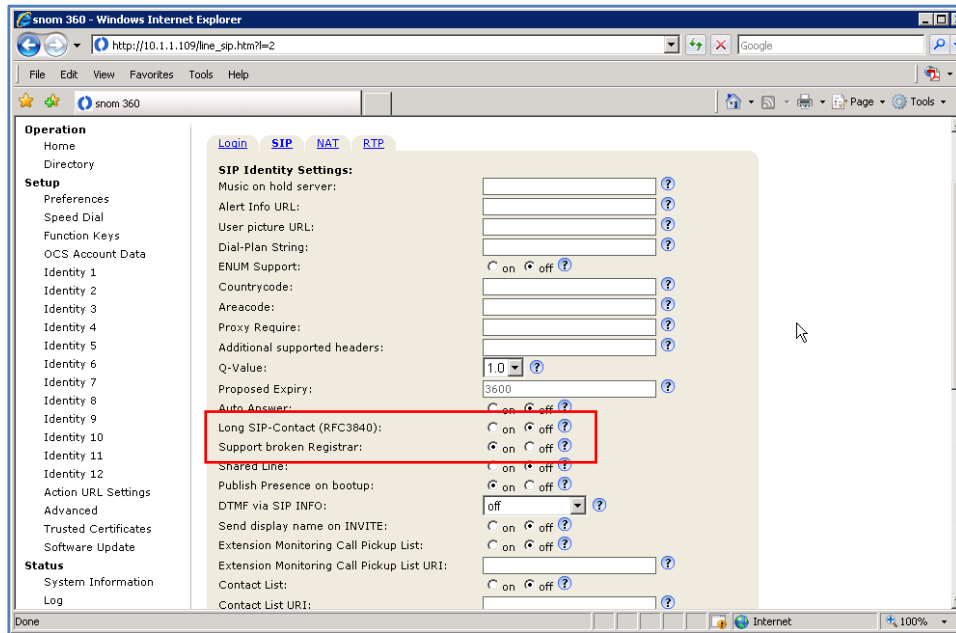
2. On the snom Login Tab, the common name also applies to the **Registrar** and **Outbound Proxy**. The Outbound Proxy includes `;transport=tls`, which enables TLS on the snom phone.

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 Registrar** to **OFF**.



Step 4: VX Settings

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

The image shows a 'General Settings' dialog box with various configuration options. The 'Certificate' section is highlighted with a red border, and the 'Certificate Name' field contains the text 'vxqw.vx.net'. Other sections include 'Clock Source', 'Secure Relay', 'Time Server', 'SNMP', 'Misc', 'LLEM', 'Comfort Noise', 'STI Clock Auto-Fallback', 'Post-login Message of the Day', 'Pre-login Banner', and 'Radius'.

Section	Field/Option	Value
Clock Source	Primary Clock Slot	1
	Primary Clock Port	Internal
	Secondary Clock Slot	None
	Secondary Clock Port	Internal
Secure Relay	STU-III Scrambler/Descrambler	<input checked="" type="checkbox"/>
	DC Filter	<input type="checkbox"/>
	Clock Rate Compensator	<input checked="" type="checkbox"/>
	V.14 Auto Detection	<input type="checkbox"/>
Time Server	Enabled	<input type="checkbox"/>
	Node ID	0:0:0:0
	Interval	21600 sec
SNMP	Community Name	public
	MIB-II Support	<input type="checkbox"/>
Certificate	Certificate Name	vxqw.vx.net
	Require TLS for domain logon	<input type="checkbox"/>
Misc	Mid-call DTMF Digits	Out-of-band Only
	T.38 Fax Redundancy	0
	T.38 CNG Detect	<input checked="" type="checkbox"/>
LLEM	Status Update Interval	2000 ms
	No. of missed status updates before LLEM is declared down	3
STI Clock Auto-Fallback	Primary	<input type="checkbox"/>
	Secondary	<input type="checkbox"/>
Post-login Message of the Day	Edit MOTD	[Button]
	Pre-login Banner	Edit Banner [Button]
Radius	Enable Accounting	<input type="checkbox"/>
	Comfort Noise	Send CN RTP packets: Enabled
Comfort Noise	Generate TDM CN on Media stream absence	Enable <input type="checkbox"/>
	Comfort Noise Level	58 -dBov
	Media stream timeout	100 ms

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.**

The screenshot shows the 'Edit TrunkGroup # 1' configuration window with the 'SIP' tab selected. The 'SIP Transport' section is highlighted with a red box, indicating the following settings:

- Enable TCP:
- Enable UDP:
- Enable TLS:
- Enable Mutual TLS:
- Persistent TLS Connection for Registration:
- Reuse TLS Connection:

Other visible settings include:

- SIP Common:** Session Expires (1), Outbound Proxy, Registrar Address, Subscriber Table (None), Reject non Subscribers (No), Reg-Timeout Retry (0), Music on Hold Filename, Ringback Audio Filename, Reliable Provisional Responses (Supported), Send Symmetric Packetization Time (Yes), Use tel: for Outgoing Invite, Retrieve Diversion from To header.
- SIP Mode:** Registrant Mode (No), Proxy-Like Mode (No), Challenger Mode (No).
- Registrant:** Reg-Error Retry, Inter Register Time.
- Proxy-Like:** Min Proxy Reg Expiry, Backup Registrar Address, Enable SLA.
- SIP Security:** Remote Certificate Name, Enable Remote Certificate Name Check, Allow SIP URI in TLS.
- Challenger:** Realm.
- RTCP:** Enable RTCP, RTCP, RTCP_XR, Transmission Interval (secs) (5).

N.E.T.

Step 6: Call Route

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

The screenshot shows the 'Edit Call Route # 6' configuration window. The 'Destination' section is highlighted with a red box, showing the following options:

- BSP
- SIP Proxy
- SIP Registrar Table
- Other
- Call Route Table
- [Unchanged]

Other sections in the window include:

- General Parameters:** Enabled , Using Regular Expression , Desc: UC IDD to Native SIP, Priority: 0.
- Input to Match:** Match Rule: \{+(-)}+, Match Using AD Field: None, Match Exact Length: , Expression Helper, Numbering Type: Any, Numbering Plan: Any, Advanced SIP Matching: , CarrierSelectInfo: Any, Carrier Code: [Empty].
- Translate to Output:** Translation Rule: 1, Translate Using AD Field: None, Numbering Type: Unknown, Numbering Plan: Unknown, CarrierSelectInfo: Untranslated, Carrier Code: [Empty], Circuit Code: Untranslated.
- On Match Parameters:** Signaling Diffserv: Best Effort, Media Diffserv: Best Effort, CallingTransTable: None, Media Class: Any, Transfer Cap: Untranslated, Msg Xlat Table: [None], Jitter Min Delay: 50 ms, Jitter Optimization: 7.
- BSP Link Requirements:** Min Quality: 0 %, Ping Limit: 0 ms.

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@his.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**.

The image shows a 'General Settings' dialog box with the following sections and values:

- Clock Source:** Primary Clock Slot: 1, Primary Clock Port: Internal, Secondary Clock Slot: None, Secondary Clock Port: Internal.
- Secure Relay:** STU-III Scrambler/Descrambler: , DC Filter: , Clock Rate Compensator: , V.14 Auto Detection: .
- Time Server:** Enabled, Node ID: 0:0:0:0, Interval: 21600 sec, Max Change: 7200 sec.
- Misc:** Mid-call DTMF Digits: Out-of-band Only, T.38 Fax Redundancy: 0, T.38 CNG Detect: , Fax/Modem bypass on PCM: .
- SNMP:** Community Name: public, MIB-II Support: .
- Certificate:** Certificate Name: 10.1.1.75 (highlighted), Require TLS for domain logon: , Allow untrusted root certificate: .
- Comfort Noise:** Send CN RTP packets: Enabled, Generate TDM CN on Media stream absence: Enable , Comfort Noise Level: 58 -dBov, Media stream timeout: 100 ms.
- LLEM:** Status Update Interval: 2000 ms, No. of missed status updates before LLEM is declared down: 3.
- STI Clock Auto-Fallback:** Primary: , Secondary: .
- Post-login Message of the Day:** Edit MOTD button.
- Pre-login Banner:** Edit Banner button.
- Radius:** Enable Accounting: .

Buttons: OK, Cancel.

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**.

The screenshot shows the 'Edit TrunkGroup # 1' configuration window with the SIP Tab selected. The 'SIP Transport' section is highlighted with a red box. The following table summarizes the configuration options shown in the image:

Section	Option	Value / State
SIP Common	Session Expires	3
	Outbound Proxy	
	Registrar Address	
	Subscriber Table	None
	Reject non Subscribers	No
	Reg-Timeout Retry	0
	Music on Hold Filename	
	Ringback Audio Filename	
	Reliable Provisional Responses	Supported
	Send Symmetric Packetization Time	Yes
SIP Mode	Registrant Mode	No
	Proxy-Like Mode	No
	Challenger Mode	No
Registrant	Reg-Error Retry	
	Inter Register Time	
Proxy-Like	Min Proxy Reg Expiry	
	Backup Registrar Address	
	Enable SLA	<input type="checkbox"/>
SIP Security	Remote Certificate Name	
	Enable Remote Certificate Name Check	<input type="checkbox"/>
	Allow SIP URI in TLS	<input type="checkbox"/>
RTCP	Enable RTCP	<input checked="" type="checkbox"/>
	RTCP	<input checked="" type="checkbox"/>
	RTCP_XR	<input checked="" type="checkbox"/>
	Transmission Interval (secs)	5
SIP Transport (highlighted)	Enable TCP	<input type="checkbox"/>
	Enable UDP	<input type="checkbox"/>
SIP Transport (highlighted)	Enable TLS	<input checked="" type="checkbox"/>
	Enable Mutual TLS	<input type="checkbox"/>
SIP Transport (highlighted)	Persistent TLS Connection for Registration	<input checked="" type="checkbox"/>
	Reuse TLS Connection	<input checked="" type="checkbox"/>
Challenger	Realm	

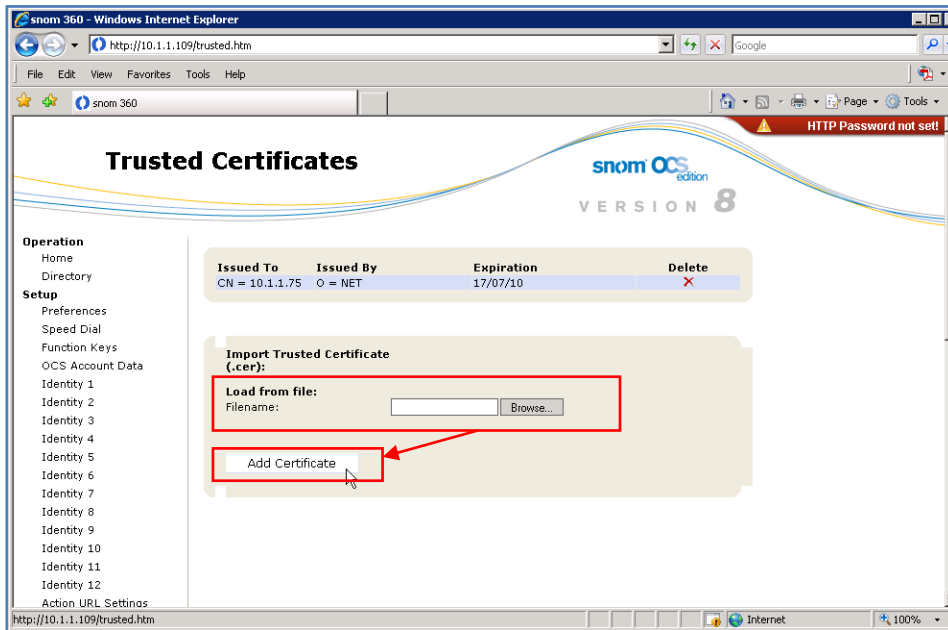
Step 4: Export the Self-Signed Certificate

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

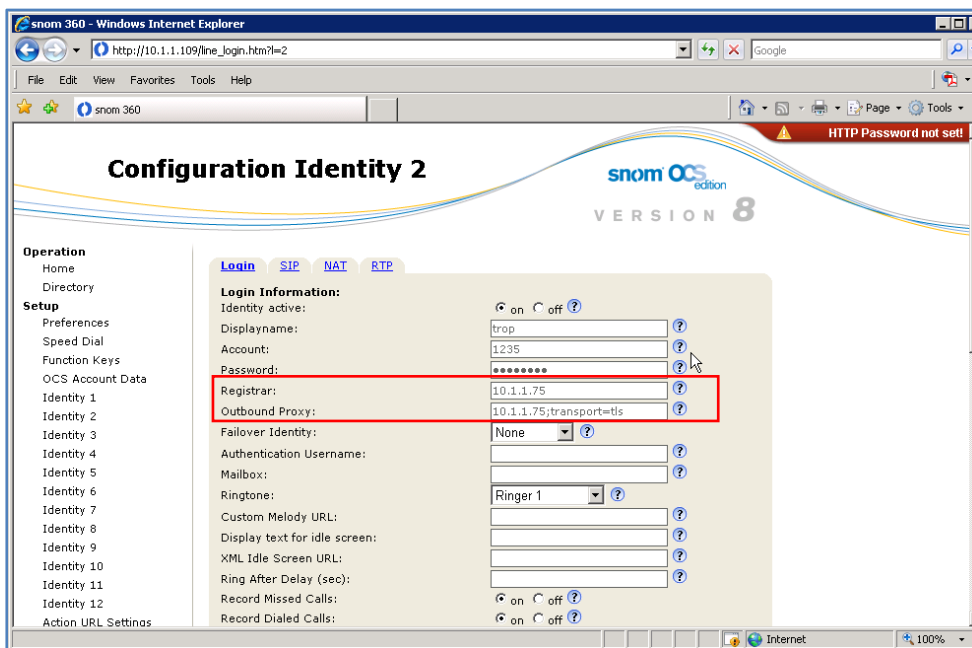
```
UCdemo# export cert 10.1.1.75 10cert.cer
Exporting a certificate was successful.
UCdemo#
```

N.E.T.

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.

The screenshot shows the snom 360 web interface. The browser window title is "snom 360 - Windows Internet Explorer" and the address bar shows "http://10.1.1.109/". The page has a red warning banner at the top right that says "HTTP Password not set!". The main heading is "Welcome to Your Phone!" with the snom OCS edition logo and "VERSION 8".

On the left is a sidebar menu with the following sections:

- Operation:** Home, Directory
- Setup:** Preferences, Speed Dial, Function Keys, OCS Account Data, Identity 1-12, Action URL Settings, Advanced, Trusted Certificates, Software Update
- Status:** System Information, Log, SIP Trace, DNS Cache, Subscriptions, PCAP Trace, Memory, Settings
- Manual**

The main content area features a "snom OCS edition / create your own style" header and a "snom OCS edition / GUI customization" section with a "snom1" icon. Below this is a "Dial a Number:" form with a text input field and "Dial" and "Hangup" buttons. Underneath is an "Outgoing Identity:" dropdown menu currently showing "jsmith@vx.net" and a "Set" button.

There are three tables of call logs:

- Dialed Numbers:**

Date	Time	Duration	Costs	Local Identity	Number
7/21/2009	4:32PM	0:04		1235@10.1.1.75	14083489775
7/21/2009	3:35PM	0:05		jsmith@vx.net	14083489775
- Missed Calls:**

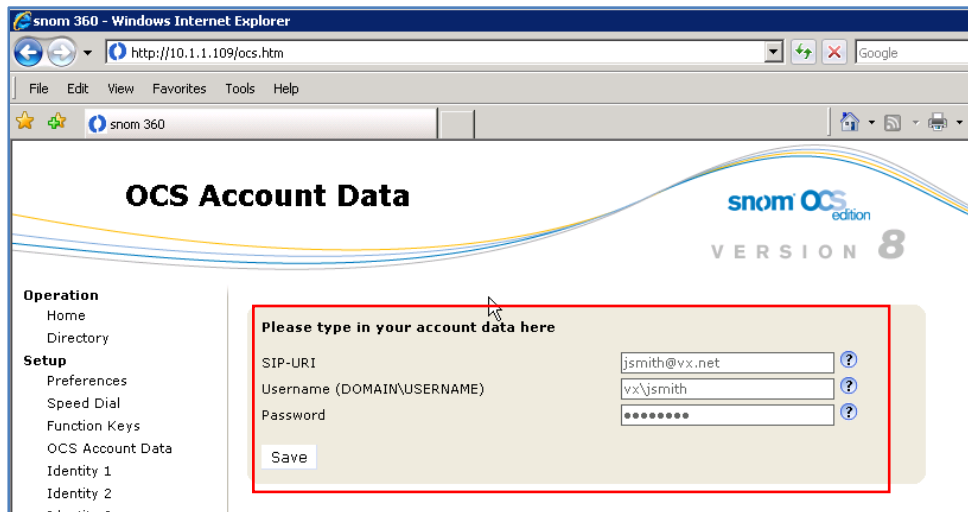
Date	Time	Missed	Local Identity	Number
7/21/2009	3:33PM	1	jsmith@vx.net	<sip:14083489775;phone-context=enterprise@vx.net,user=phone>
- Received Calls:**

Date	Time	Duration	Costs	Local Identity	Number
7/21/2009	4:32PM	0:03		1235@10.1.1.75	<sip:14083489775@10.1.1.75>
7/21/2009	3:36PM	0:00		jsmith@vx.net	<sip:14083489775;phone-context=enterprise@vx.net,user=phone>

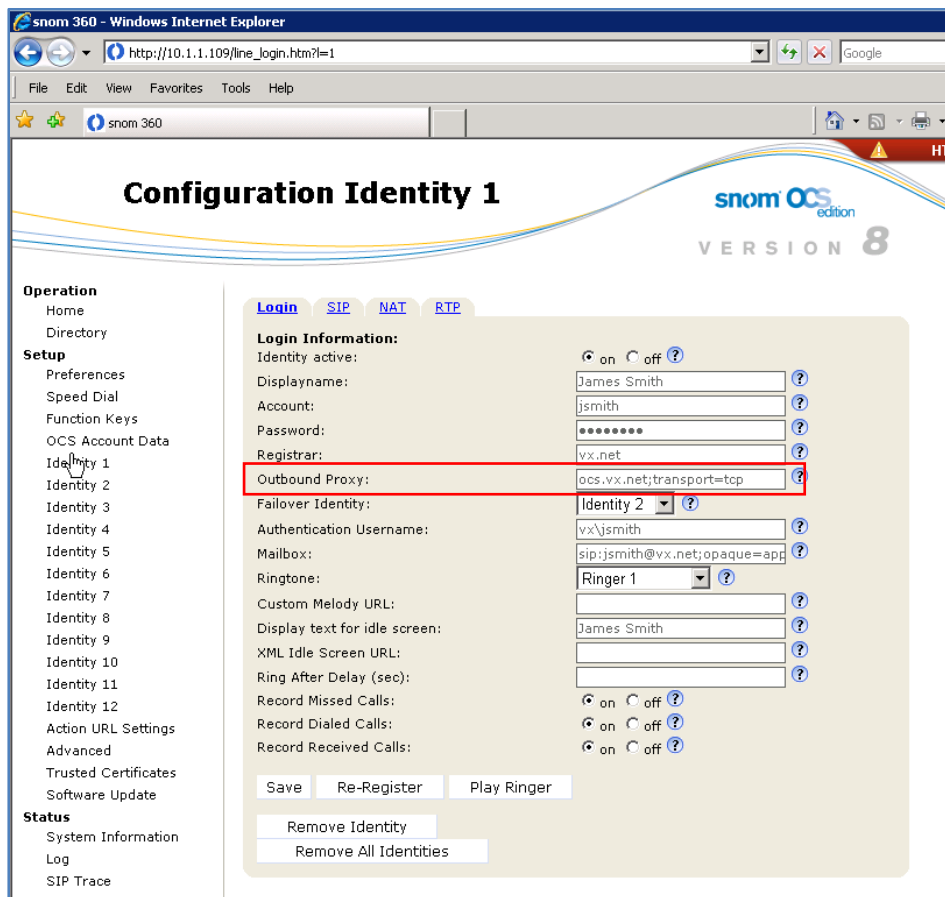
The footer of the page includes the snom logo and "© 2000-2009 snom AG".

N.E.T.

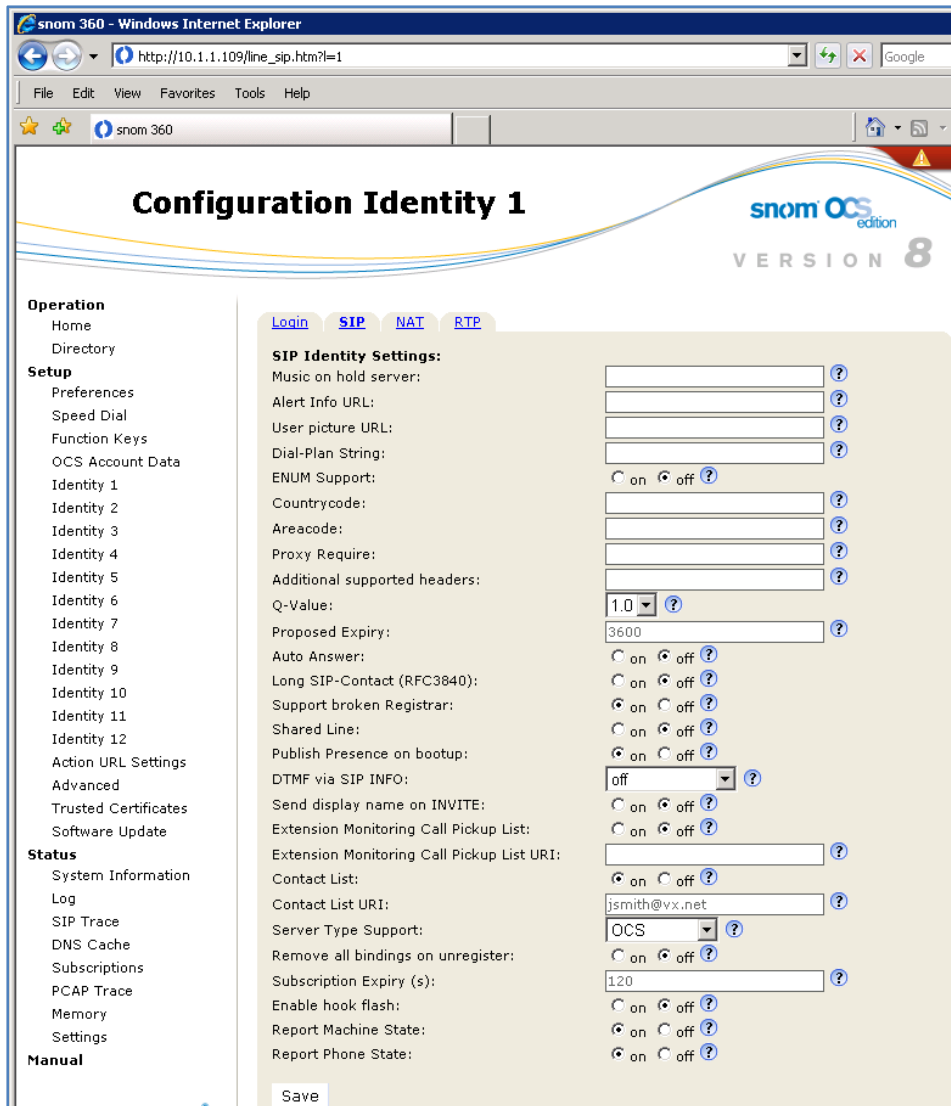
2. To configure the phone for OCS, from the navigation tree located in the left pane select **Setup>OCS Account Data**. The OCS Account Data view displays showing the OCS Identity with the SIP Registrar backup identity. Click **Save** to continue.



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.

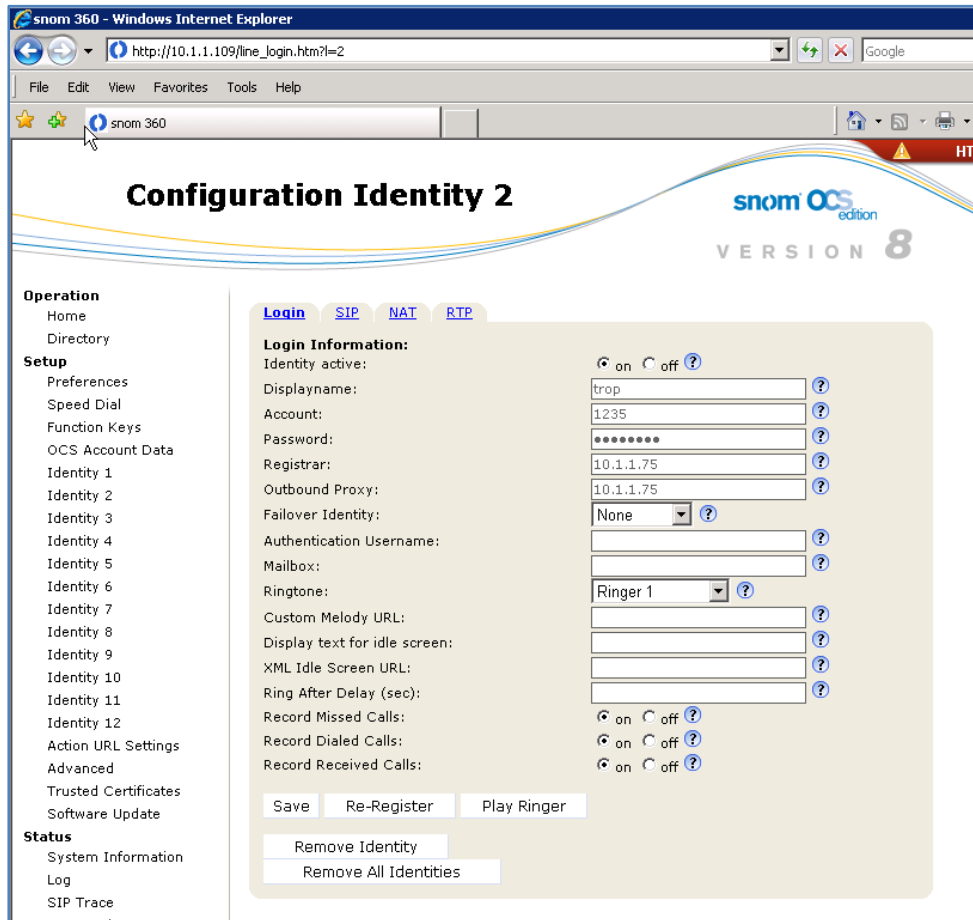


- In the right pane, select the **SIP tab** to display the SIP configuration settings for Identity 1. This configures the phone to login as a communicator to OCS.

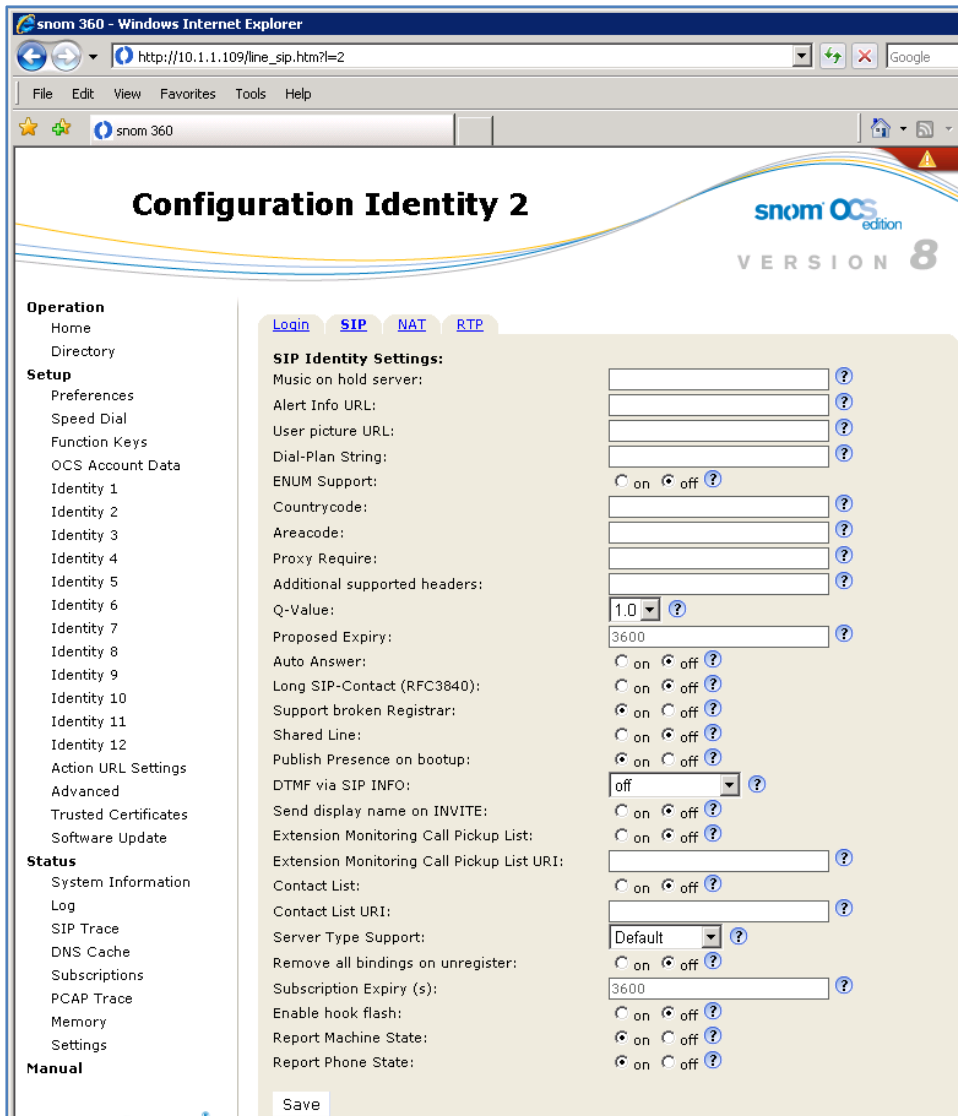


N.E.T.

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

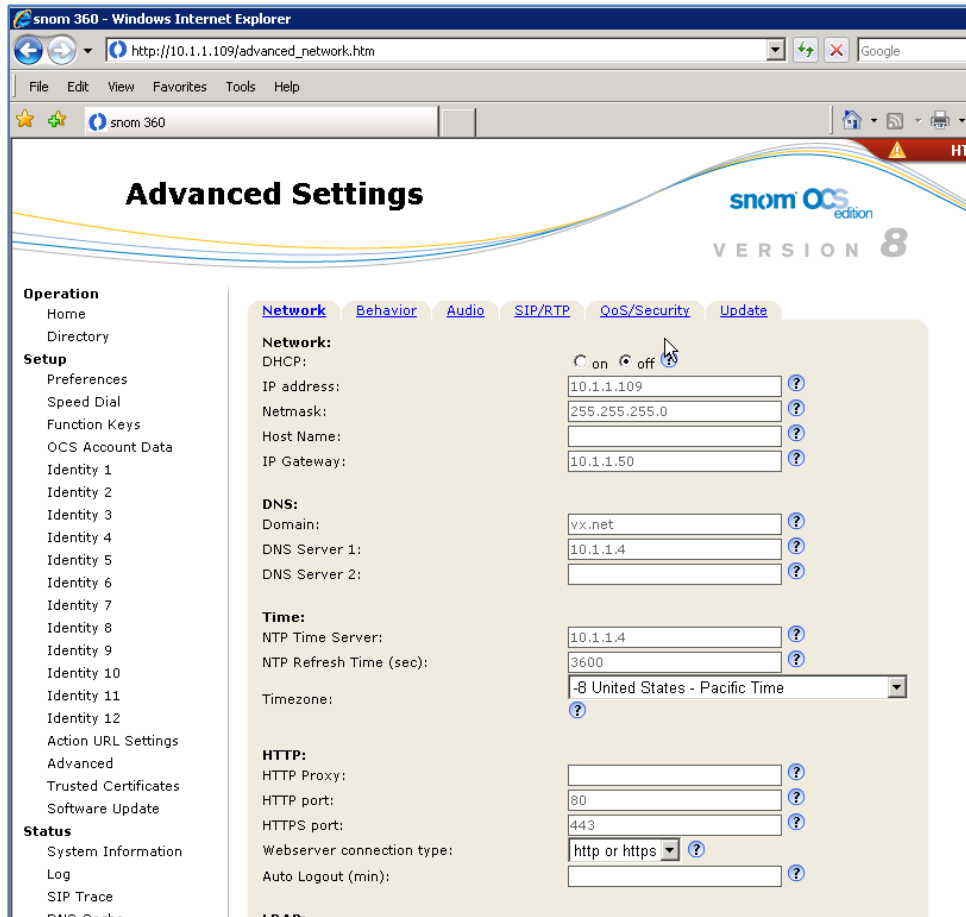


- In the right pane, select the **SIP tab** to display the SIP configuration settings for Identity 2. This configures backup for the phone to login as a communicator to OCS.

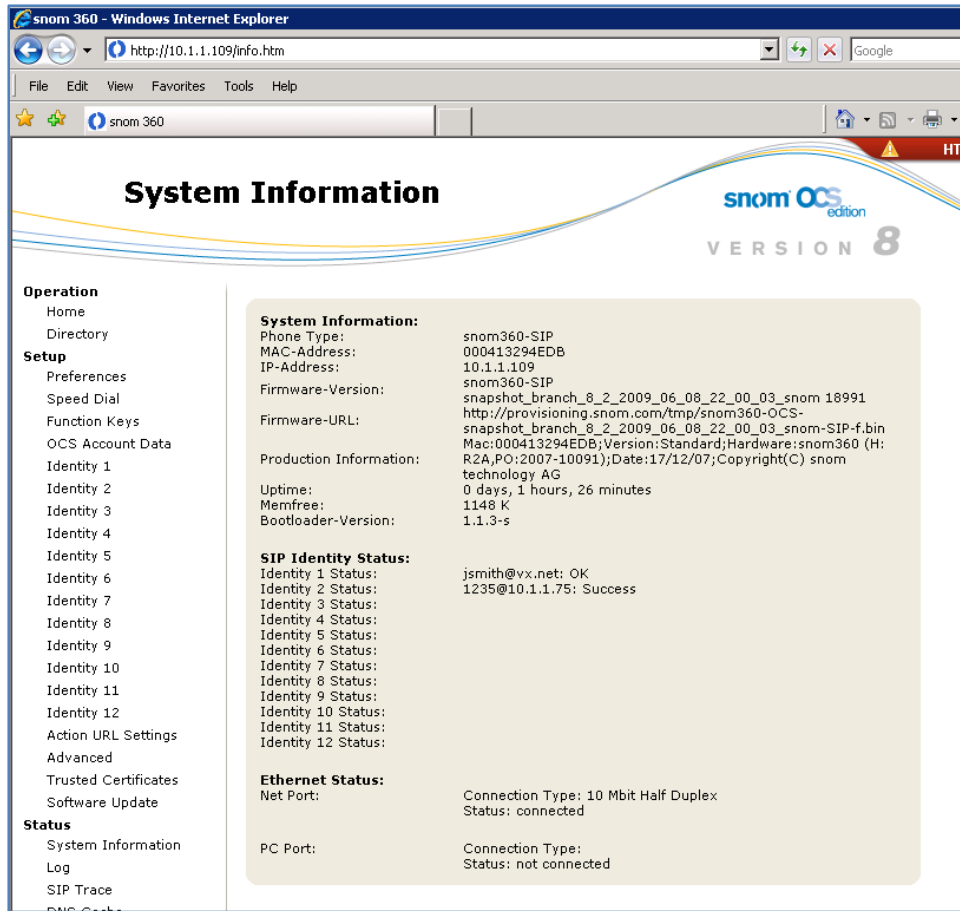


N.E.T.

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



8. View System Information to confirm your settings.

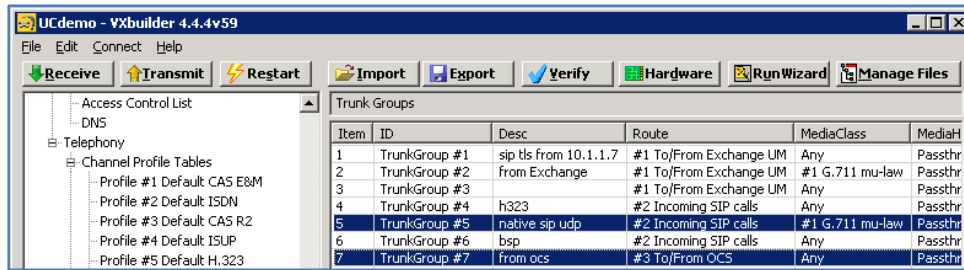


9. Your snom phone is now ready to use.

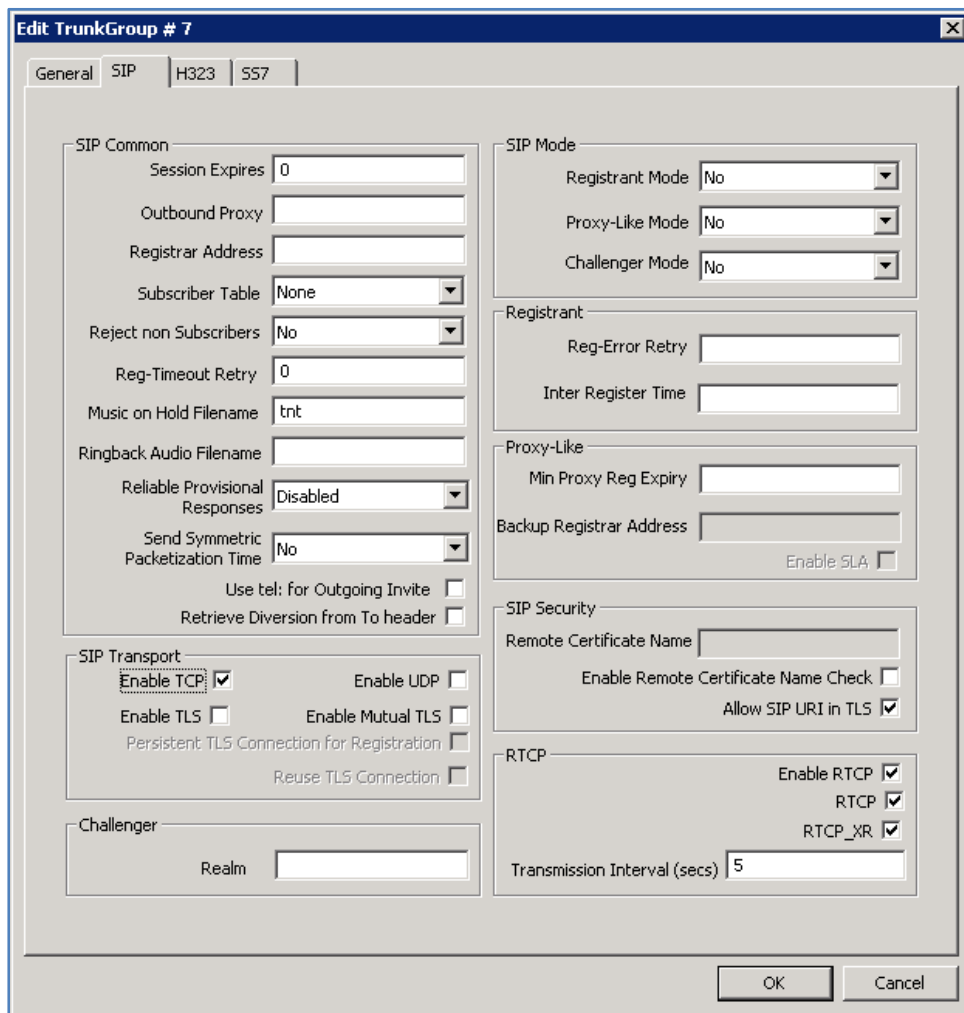


N.E.T.

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.

Edit Call Route # 2

General Parameters
 Enabled Using Regular Expression Desc: all SIP calls to mediation Priority: 0
 OK Cancel

Input to Match
 Match Rule: #1{+} Match Using AD Field: None
 Match Exact Length Expression Helper Numbering Type: Any Numbering Plan: Any
 Advanced SIP Matching CarrierSelectInfo: Any Carrier Code:

Translate to Output
 Translation Rule: \1 Translate Using AD Field: None
 Numbering Type: Unknown Numbering Plan: Unknown
 CarrierSelectInfo: Untranslated Carrier Code: Circuit Code: Untranslated

On Match Parameters
 Signaling Diffserv: Best Effort Media Diffserv: Best Effort CallingTransTable: None
 Media Class: Any Transfer Cap: Untranslated Msg Xlat Table: [None]
 Jitter Min Delay: 50 ms Jitter Optimization: 7

Destination
 BSP TrunkGroup: #7 from ocs
 SIP Proxy Node ID: [N/A]
 SIP Registrar Table SIP Proxy: mediation.vx.net:5060
 Other Peer IP / IF: [Unchanged]
 Call Route Table Call Route No.: None
 [Unchanged]

BSP Link Requirements
 Min Quality: 0 %
 Ping Limit: 0 ms

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.

The screenshot shows the 'Edit TrunkGroup # 5' configuration window with the 'SIP' tab selected. The window is divided into several sections:

- SIP Common:** Session Expires (0), Outbound Proxy, Registrar Address, Subscriber Table (None), Reject non Subscribers (No), Reg-Timeout Retry (100), Music on Hold Filename (tnt), Ringback Audio Filename, Reliable Provisional Responses (Disabled), Send Symmetric Packetization Time (No), Use tel: for Outgoing Invite, and Retrieve Diversion from To header.
- SIP Mode:** Registrant Mode (No), Proxy-Like Mode (No), and Challenger Mode (No).
- Registrant:** Reg-Error Retry (100) and Inter Register Time (100).
- Proxy-Like:** Min Proxy Reg Expiry, Backup Registrar Address, and Enable SLA (checkbox).
- SIP Security:** Remote Certificate Name, Enable Remote Certificate Name Check, and Allow SIP URI in TLS (checkbox).
- RTCP:** Enable RTCP (checkbox), RTCP (checkbox), and RTCP_XR (checkbox).
- Challenger:** Realm.
- SIP Transport:** Enable TCP (checkbox), Enable UDP (checked), Enable TLS (checkbox), Enable Mutual TLS (checkbox), Persistent TLS Connection for Registration (checkbox), and Reuse TLS Connection (checkbox).

At the bottom right, there are 'OK' and 'Cancel' buttons.

14. Call Route to SIP Registrar.

Edit Call Route # 5

General Parameters
 Enabled Using Regular Expression Desc UC IDD to Native SIP Priority 0
 OK Cancel

Input to Match
 Match Rule #2{+{+} Match Using AD Field None
 Match Exact Length Expression Helper Numbering Type Any Numbering Plan Any
 Advanced SIP Matching CarrierSelectInfo Any Carrier Code

Translate to Output
 Translation Rule \1 Translate Using AD Field None
 Numbering Type Unknown Numbering Plan Unknown
 CarrierSelectInfo Untranslated Carrier Code Circuit Code Untranslated

On Match Parameters
 Signaling Diffserv Best Effort Media Diffserv Best Effort CallingTransTable None
 Media Class Any Transfer Cap Untranslated Msg Xlat Table [None]
 Jitter Min Delay 50 ms Jitter Optimization 7

Destination
 BSP TrunkGroup [N/A]
 SIP Proxy Node ID [N/A]
 SIP Registrar Table SIP Proxy
 Other Peer IP / IP [Unchanged]
 Call Route Table Call Route No. None
 [Unchanged]

BSP Link Requirements
 Min Quality 0 %
 Ping Limit 0 ms

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

```

10.1.1.75 - PuTTY
-----
Item TG# Address of Record Contact Address NAT Address Expires TransportType
-----
1 5 1235 1235@10.1.1.109 0.0.0.0 56s UDP
2 5 14083489775 14083489775@10.1.1.103:51784 0.0.0.0 39s UDP
    
```

Calls between snom Phone <> eyeBeam

```

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
-----
x001d Tkgrp: 5 14083489775 +1114 Tkgrp: 7 UDP TCP
    
```

```

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
-----
x001f Tkgrp: 7 +1114 14083489775@...51784 Tkgrp: 5 TCP UDP
    
```

```

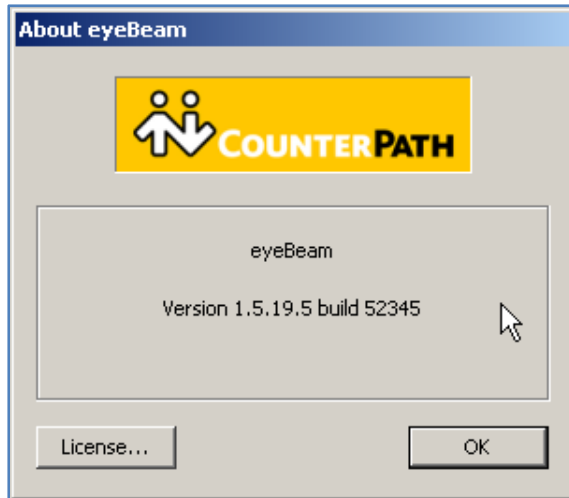
10.1.1.75 - PuTTY
UCdemo# sho call detail
CSN In Trunkgroup# Calling Number Called Number Out Node ID Inbound Outbound
(hex) or Trunkgroup# Transport Transport
-----
x0020 Tkgrp: 5 14083489775 1235@10.1.1.109 Tkgrp: 5 UDP UDP
    
```

```

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
-----
x0030 Tkgrp: 5 1235 14083489775@...51784 Tkgrp: 5 UDP UDP
    
```

Configuring TLS on eyeBeam

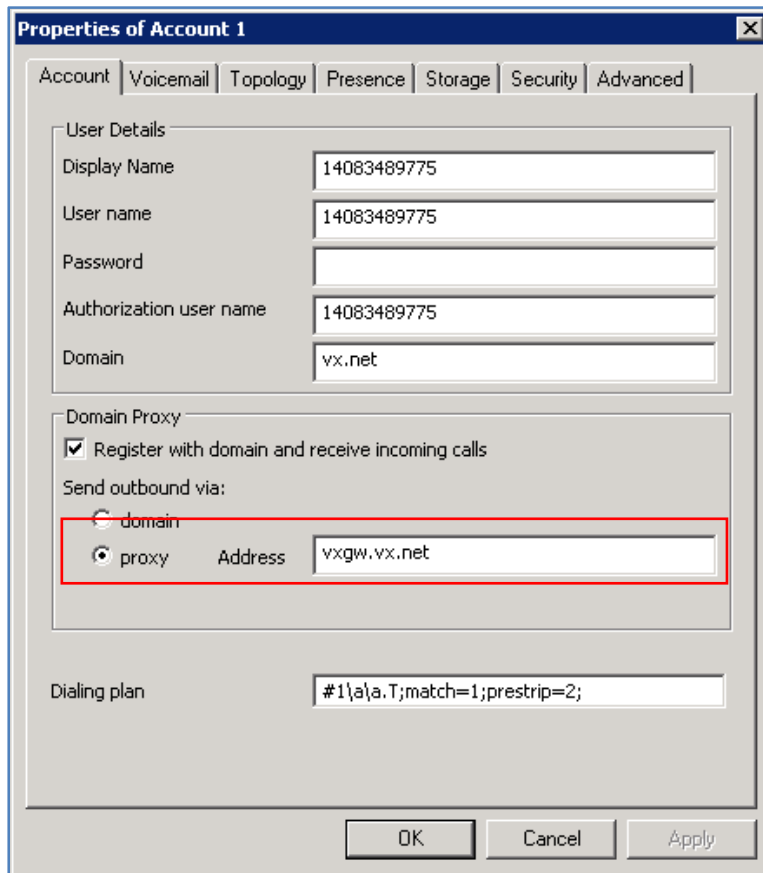
eyeBeam with TLS is similar to other TLS clients. The most important task is to import to the PC the **root certificate** from the Certificate Authority that signed the VX certificate.



N.E.T.

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.

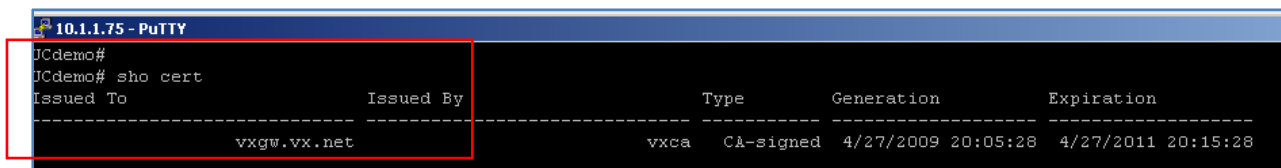


The screenshot shows the 'Properties of Account 1' dialog box with the following fields and settings:

- User Details:**
 - Display Name: 14083489775
 - User name: 14083489775
 - Password: (empty)
 - Authorization user name: 14083489775
 - Domain: vx.net
- Domain Proxy:**
 - Register with domain and receive incoming calls
 - Send outbound via:
 - domain
 - proxy Address: vxgw.vx.net
- Dialing plan:** #1\a\a.T;match=1;prestrip=2;

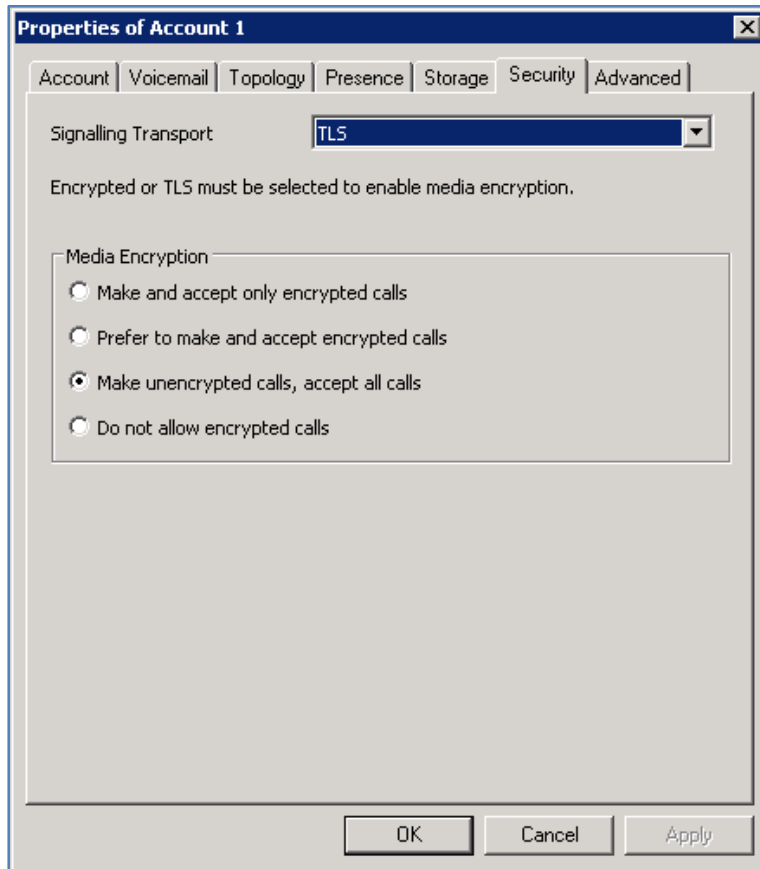
Buttons: OK, Cancel, Apply

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



```
10.1.1.75 - PuTTY
JCdemo#
JCdemo# 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
```

Step 2: eyeBeam Security Settings



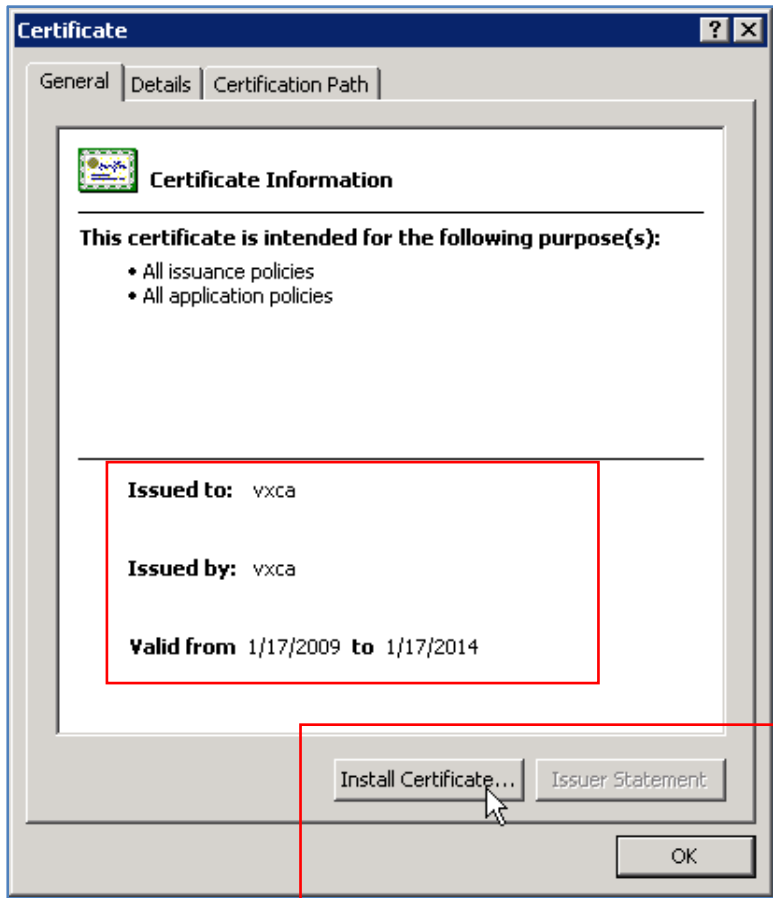
N.E.T.

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.



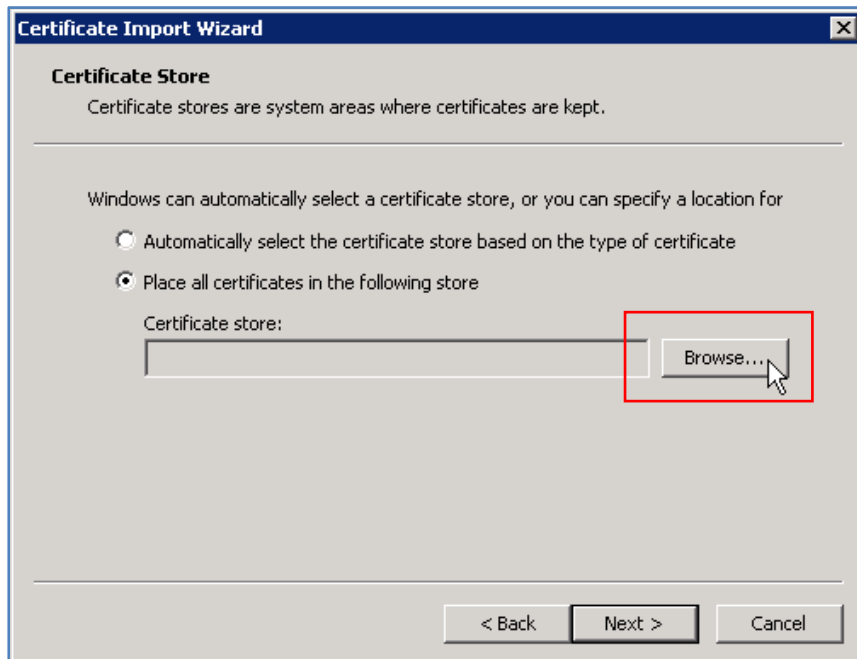
2. On the Certificate view, General Tab, Double click **Install Certificate** to install the certificate using the following instructions.
 - a. **vxca** is the root certificate from the Certificate Authority used to sign the **vxgw.vx.net** certificate.



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

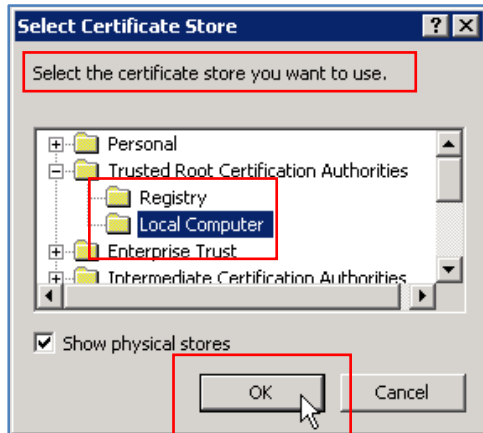


4. **Browse** the Certificate Store to select certificate storage location. Click **Next** to continue.

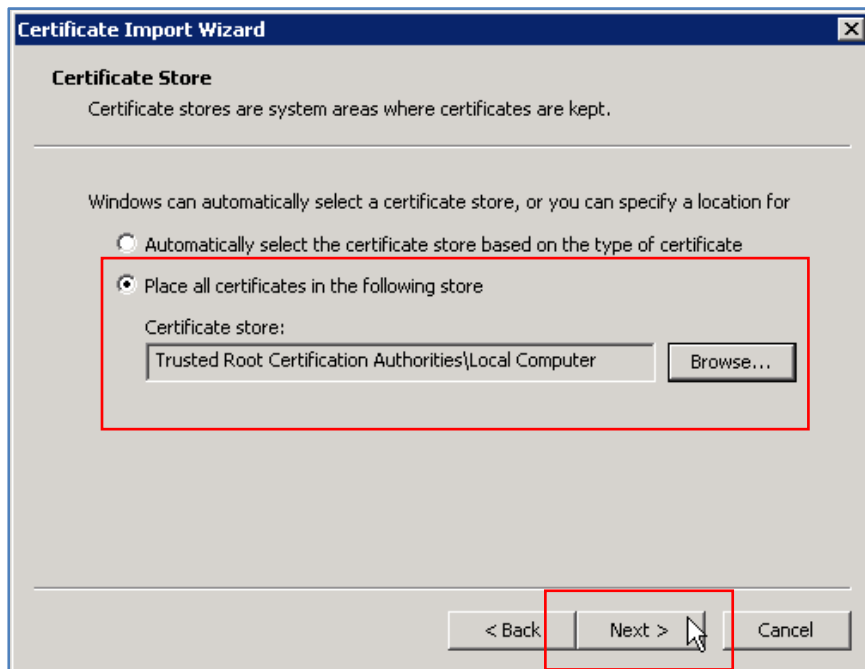


N.E.T.

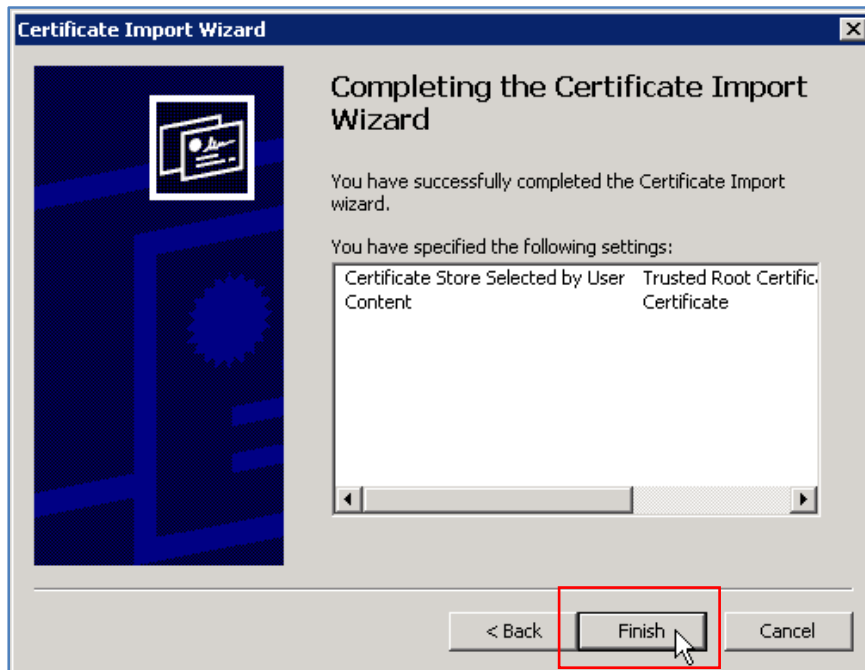
5. Select the **Certificate Store** and click **OK**.



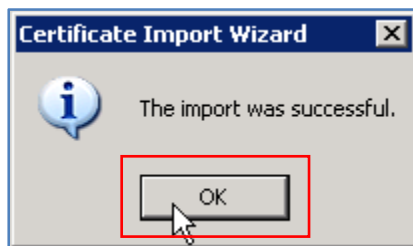
6. Confirm the Certificate Store you have selected, which displays in the **Certificate Store** entry, and click **Next** to continue.



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.

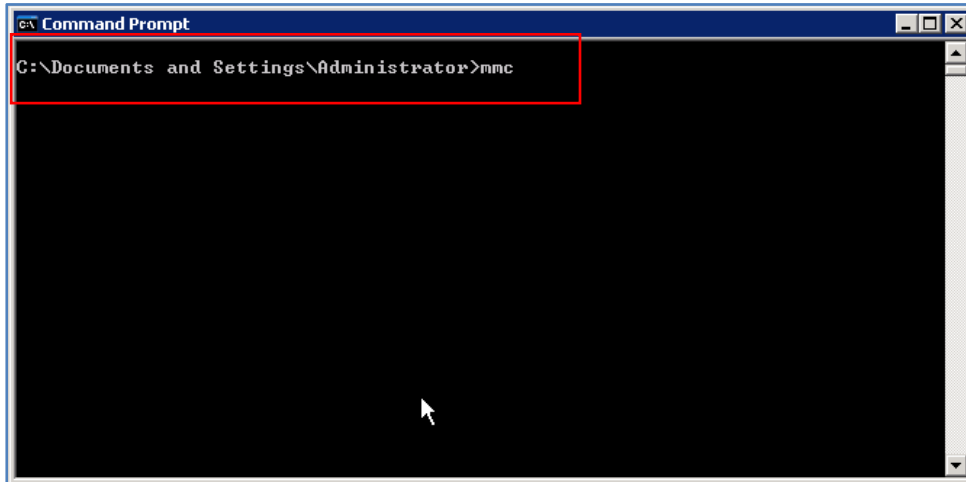
Note: Failure to reboot your PC will invalidate the Certificate Import Wizard steps.

N.E.T.

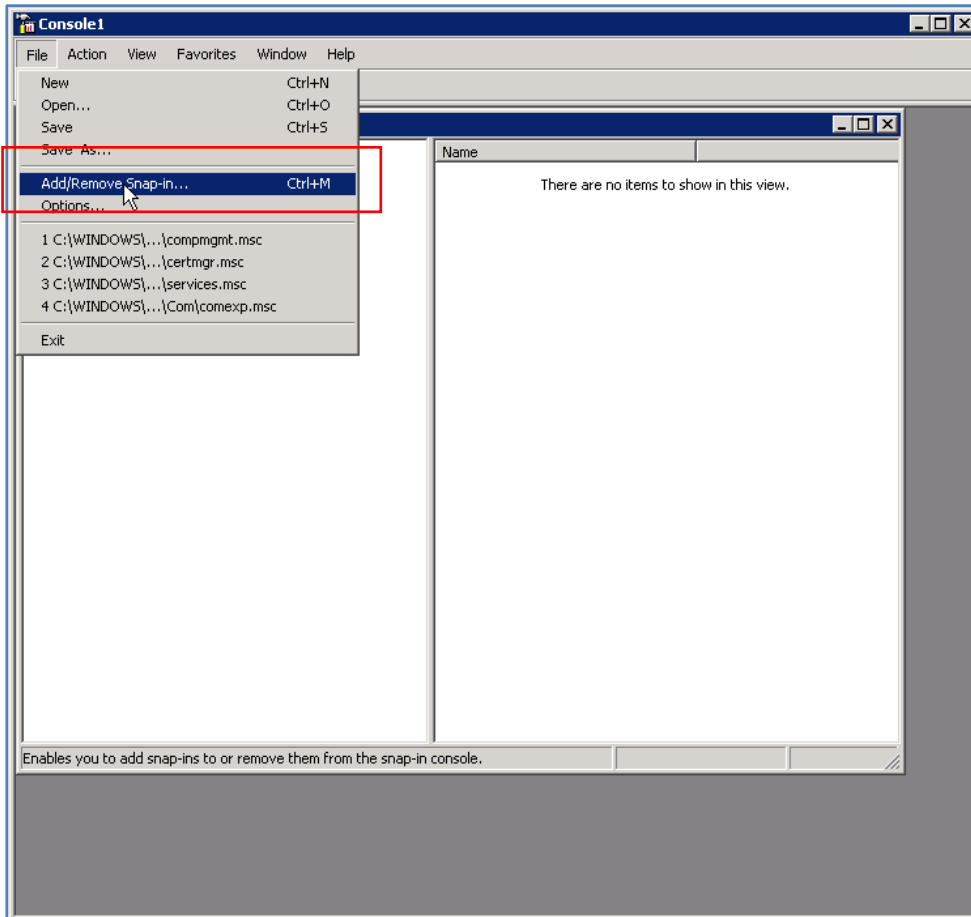
Step 4: Verify Certificate Installation

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

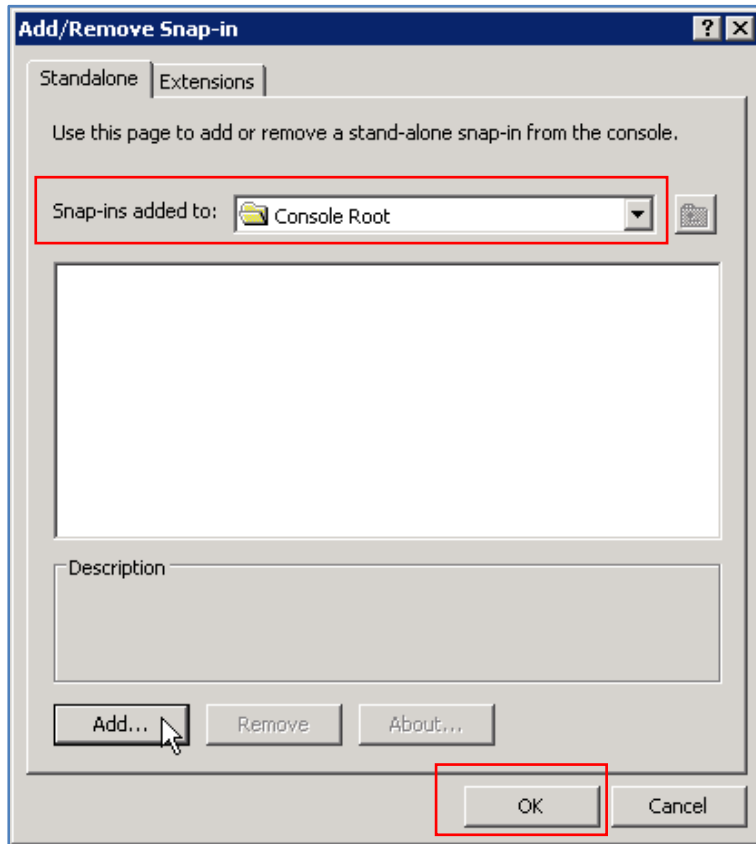
1. At the command prompt, enter **mmc**



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

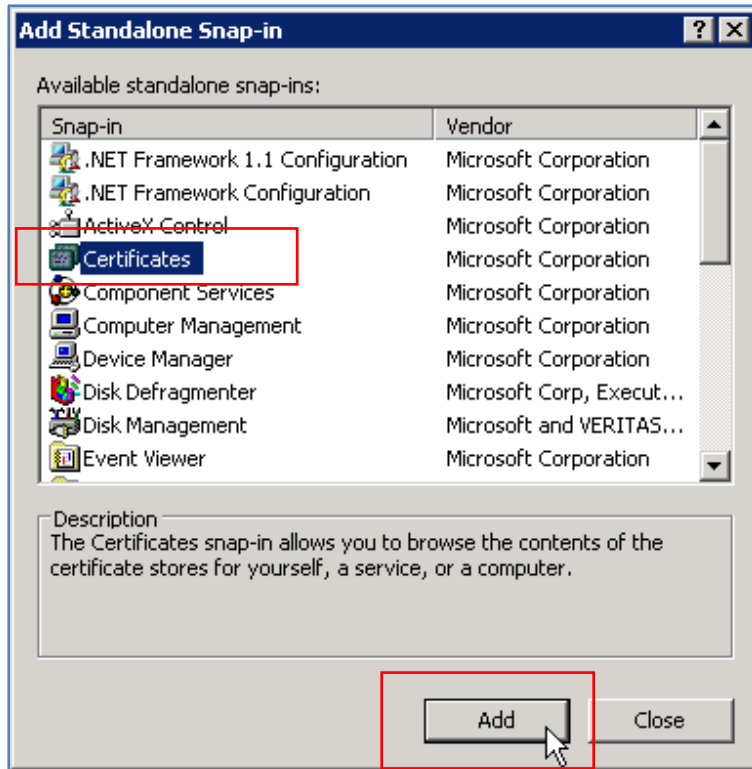


3. From the Standalone Tab, select the **Console Root** folder from the **Snap-ins added to** field. Click **Add** and then **OK**. The Add Standalone Snap-in view displays.

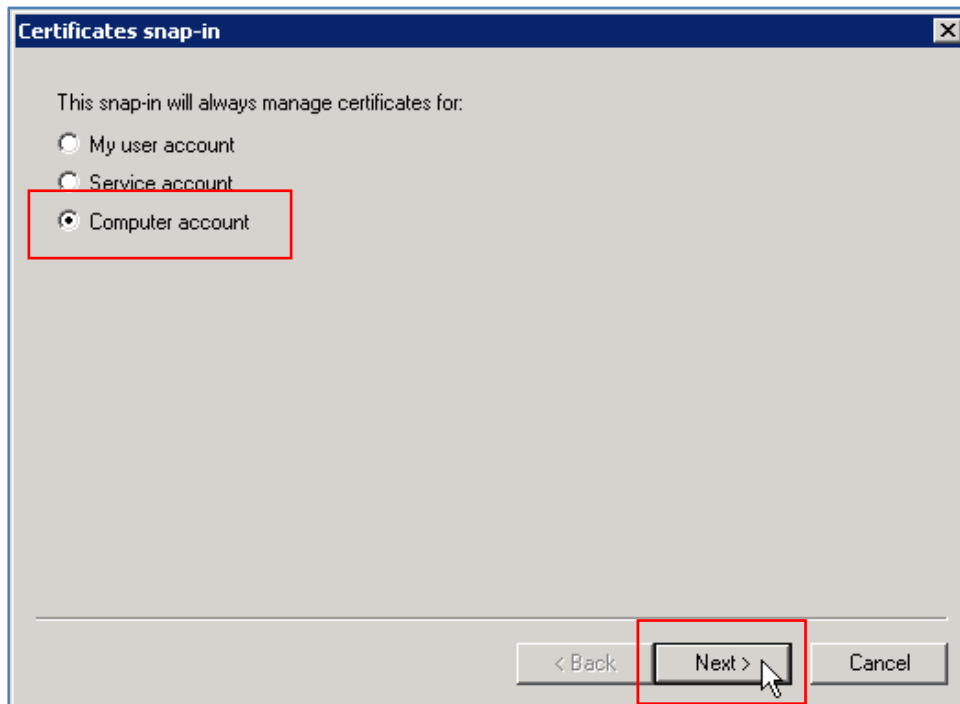


N.E.T.

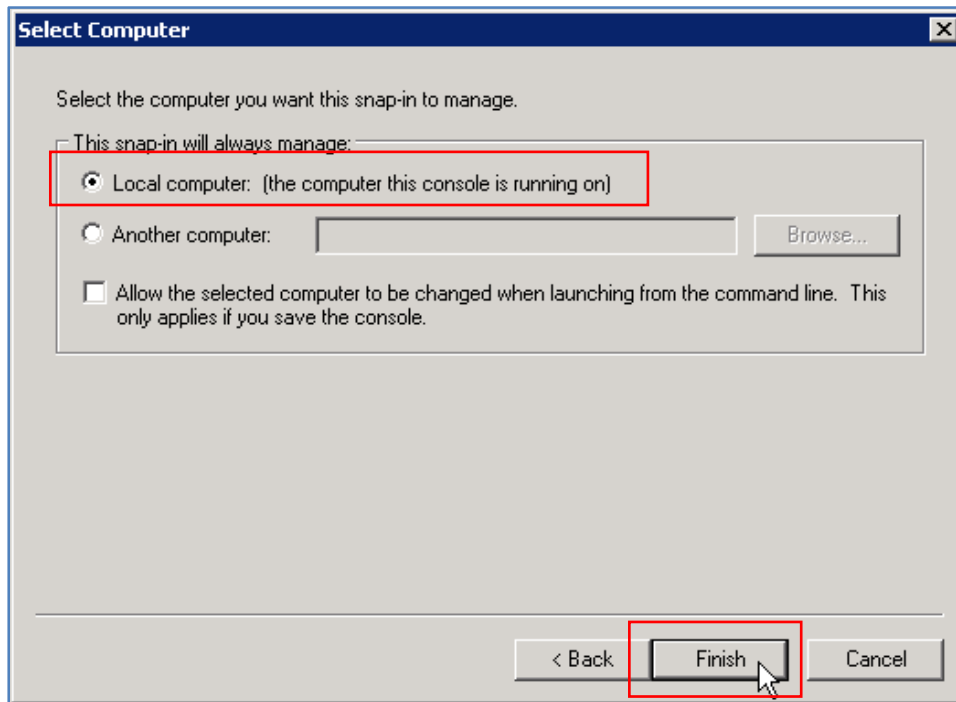
4. Select the **Certificates**, and click **Add**. The Certificates snap-in view displays.



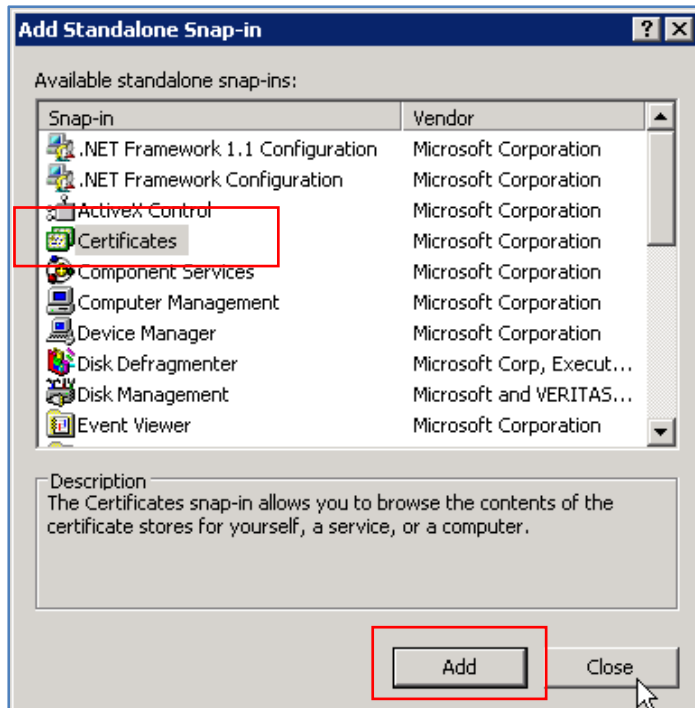
5. Select the radio button for **Computer account** and click **Next**.



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

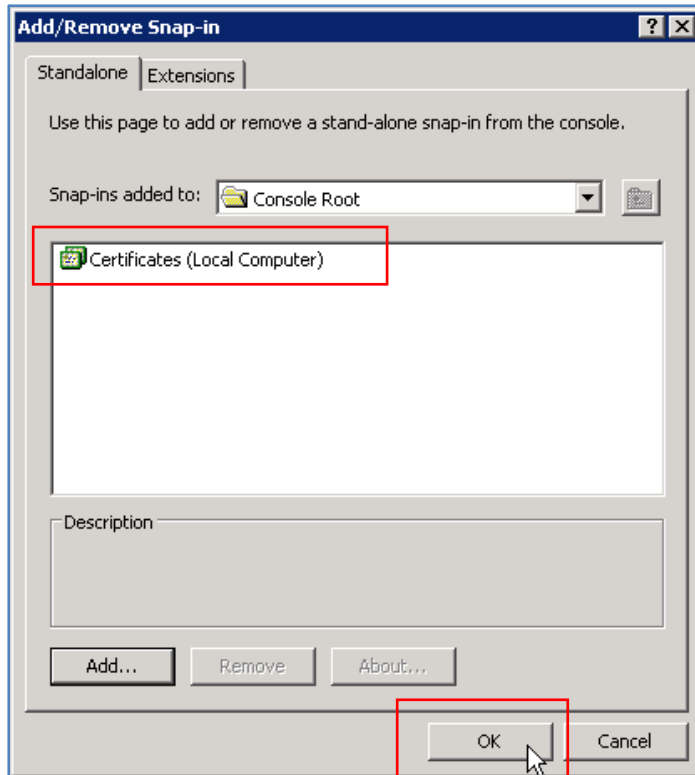


7. From the **Add Standalone Snap-in** view, select **Certificates** and click **Add**.

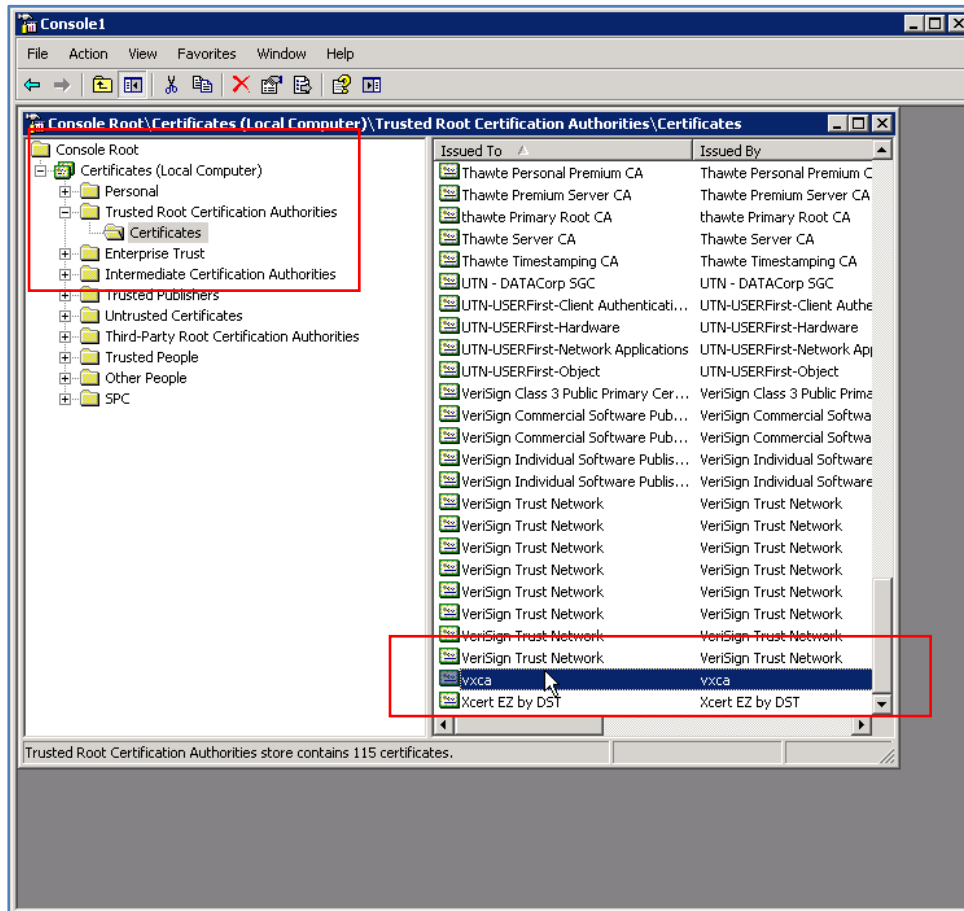


N.E.T.

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



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



Step 5: VX Configuration

A TLS-configured Trunk Group.

The screenshot shows the 'Edit TrunkGroup # 1' configuration window with the 'SIP' tab selected. The window is divided into several sections for configuring SIP parameters:

- SIP Common:**
 - Session Expires: 1
 - Outbound Proxy: (empty)
 - Registrar Address: (empty)
 - Subscriber Table: None
 - Reject non Subscribers: No
 - Reg-Timeout Retry: 0
 - Music on Hold Filename: (empty)
 - Ringback Audio Filename: (empty)
 - Reliable Provisional Responses: Supported
 - Send Symmetric Packetization Time: Yes
 - Use tel: for Outgoing Invite:
 - Retrieve Diversion from To header:
- SIP Mode:**
 - Registrant Mode: No
 - Proxy-Like Mode: No
 - Challenger Mode: No
- Registrant:**
 - Reg-Error Retry: (empty)
 - Inter Register Time: (empty)
- Proxy-Like:**
 - Min Proxy Reg Expiry: (empty)
 - Backup Registrar Address: (empty)
 - Enable SLA:
- SIP Security:**
 - Remote Certificate Name: (empty)
 - Enable Remote Certificate Name Check:
 - Allow SIP URI in TLS:
- SIP Transport:**
 - Enable TCP:
 - Enable UDP:
 - Enable TLS:
 - Enable Mutual TLS:
 - Persistent TLS Connection for Registration:
 - Reuse TLS Connection:
- Challenger:**
 - Realm: (empty)
- RTCP:**
 - Enable RTCP:
 - RTCP:
 - RTCP_XR:
 - Transmission Interval (secs): 5

Buttons for 'OK' and 'Cancel' are located at the bottom right of the window.

N.E.T.

Step 6: VX General Menu

The vxgw.vx.net installed certificate.

General Settings

Clock Source
Primary Clock Slot: 1
Primary Clock Port: Internal
Secondary Clock Slot: None
Secondary Clock Port: Internal

Time Server
 Enabled
Node ID: 0:0:0:0
Interval: 21600 sec
Max Change: 7200 sec

SNMP
Community Name: public
MIB-II Support:

Certificate
Certificate Name: vxgw.vx.net
Require TLS for domain logon:
Allow untrusted root certificate:

Comfort Noise
Send CN RTP packets: Enabled
Generate TDM CN on Media stream absence: Enable
Comfort Noise Level: 58 -dBov
Media stream timeout: 100 ms

Secure Relay
STU-III Scrambler/Descrambler:
DC Filter:
Clock Rate Compensator:
V.14 Auto Detection:

Misc
Mid-call DTMF Digits: Out-of-band Only
T.38 Fax Redundancy: 0
T.38 CNG Detect:
Fax/Modem bypass on PCM:

LLEM
Status Update Interval: 2000 ms
No. of missed status updates before LLEM is declared down: 3

STI Clock Auto-Fallback
Primary: Secondary:

Post-login Message of the Day **Pre-login Banner**
Edit MOTD Edit Banner

Radius
Enable Accounting:

OK Cancel

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

