

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in any way, including photocopy, photograph, magnetic, or other record, without the prior written permission of N.E.T. Unpublished-rights reserved under the copyright laws of the United States.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).

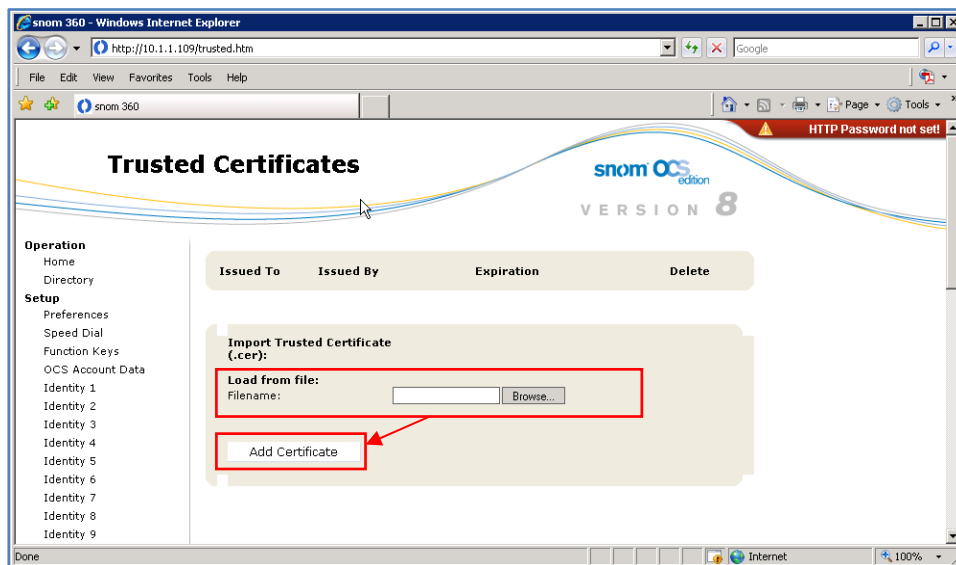
Step 1: Install VX Root Certificate onto the snom Phone

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.

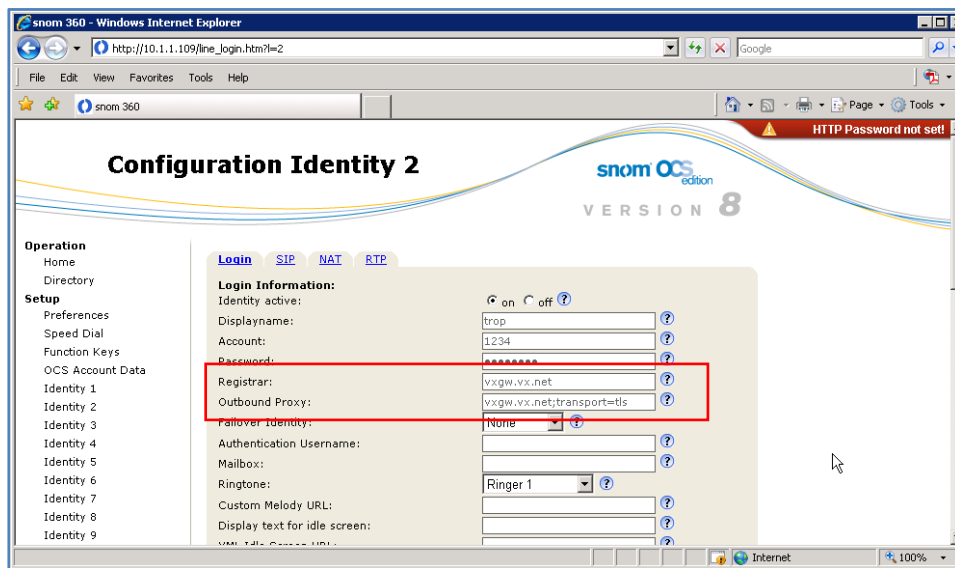
Step 2: Enter the Configuration Identity

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#
```

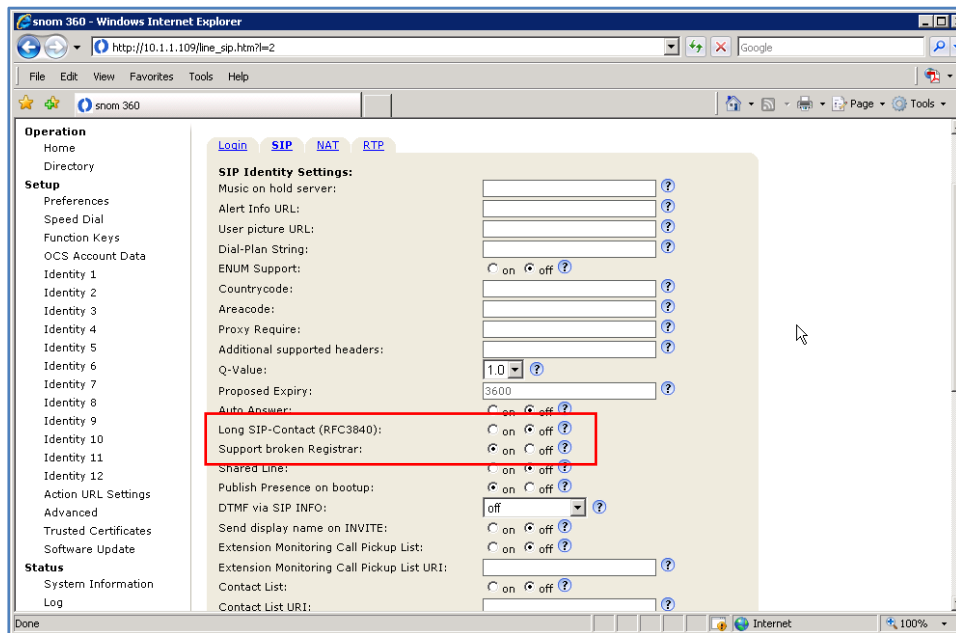
2. On the snom Login Tab, the common name also applies to the **Registrar** and **Outbound Proxy**. The Outbound Proxy includes `;transport=tls`, which enables TLS on the snom phone.

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 screenshot shows the 'General Settings' window with various configuration options. The 'Certificate' section is highlighted with a red rectangle, and the 'Certificate Name' field contains the text 'vxqw.vx.net'.

General Settings

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

SNMP

- Community Name: public
- MIB-II Support: ☐

Certificate

- Certificate Name: vxqw.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

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

- Edit MOTD

Pre-login Banner

- Edit Banner

Radius

- Enable Accounting: ☐

OK Cancel

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**.

Edit TrunkGroup # 1

General SIP H323 S57

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 Transport

Enable TCP: ☐ Enable UDP: ☐

Enable TLS: ☒ Enable Mutual TLS: ☐

Persistent TLS Connection for Registration: ☒

Reuse TLS Connection: ☒

Challenger

Realm:

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: ☐

RTCP

Enable RTCP: ☒

RTCP: ☒

RTCP_XR: ☒

Transmission Interval (secs): 5

OK Cancel

Step 6: Call Route

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

Edit Call Route # 6

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

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
☐ SIP Proxy
☒ SIP Registrar Table
☐ Other
☐ Call Route Table
☐ [Unchanged]

TrunkGroup [N/A]
Node ID [N/A]
SIP Proxy
Peer IP / IF [Unchanged]
Call Route No. None

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.

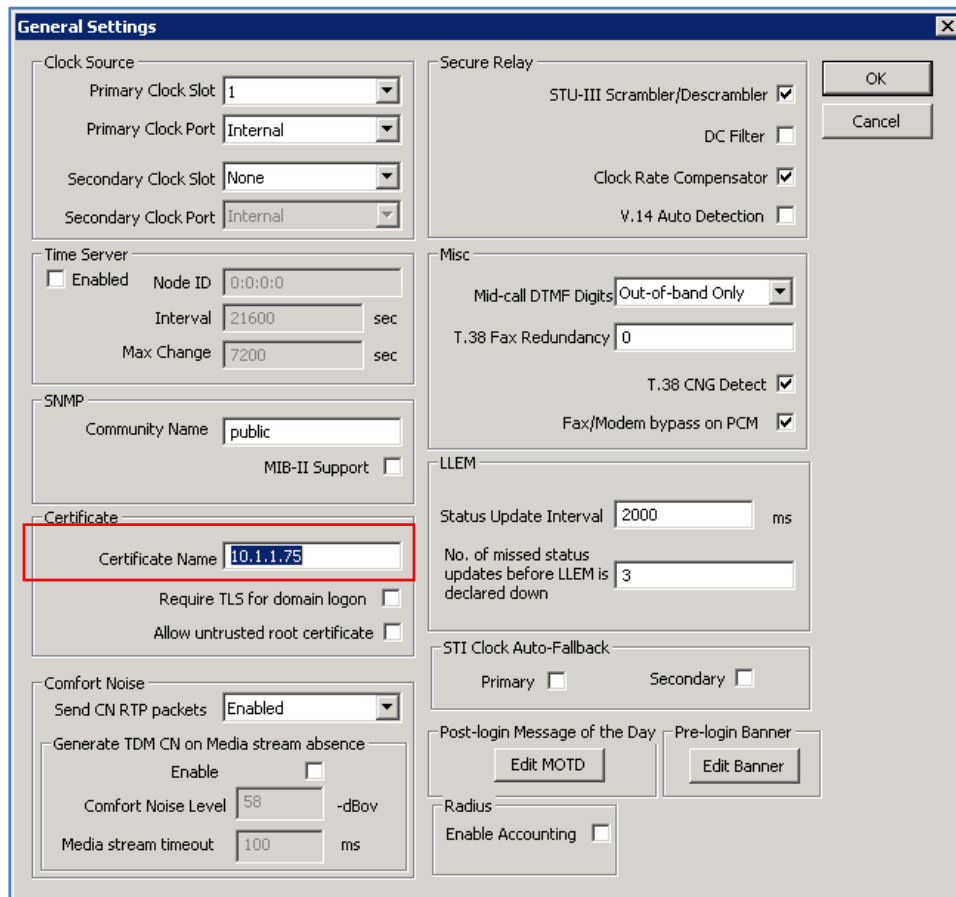
```
UCDemo# gen cert sel
Please input the following information to create a certificate with.
Common Name should be provided at the minimum.

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 screenshot shows the 'General Settings' window with various configuration sections. The 'Certificate' section is highlighted with a red rectangle, and the 'Certificate Name' field contains the text '10.1.1.75'.

General Settings

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

SNMP

- Community Name: public
- MIB-II Support: ☐

Certificate

- Certificate Name: 10.1.1.75
- Require TLS for domain logon: ☐
- Allow untrusted root certificate: ☐

Comfort Noise

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

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

- Edit MOTD

Pre-login Banner

- Edit Banner

Radius

- Enable Accounting: ☐

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' dialog box with the 'SIP' tab selected. The 'SIP Transport' section is highlighted with a red box. The settings in this section are:

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

Other settings visible in the dialog include:

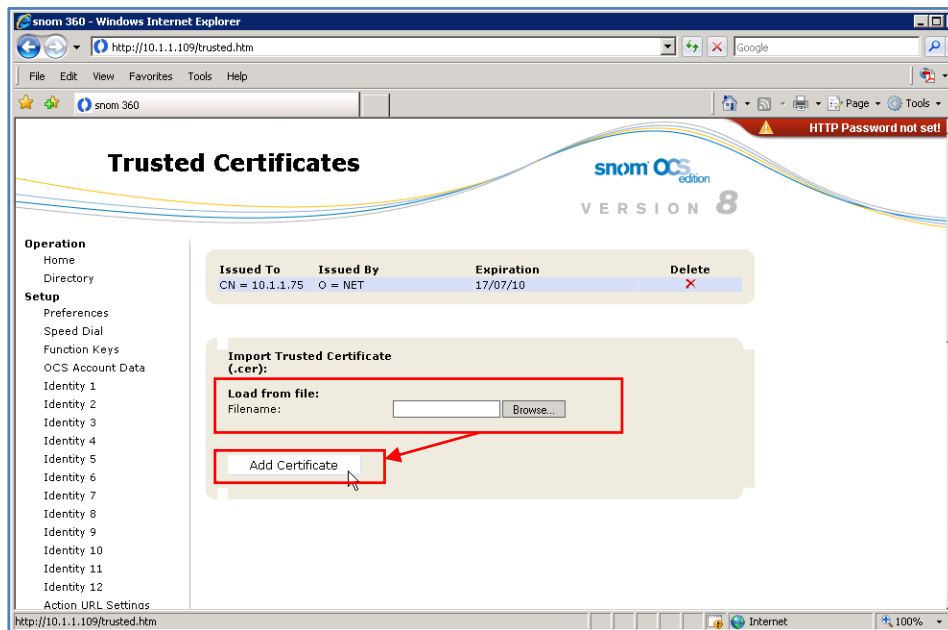
- SIP Common: Session Expires (3), Outbound Proxy, Registrar Address, Subscriber Table (None), Reject non Subscribers (No), Reg-Timeout Retry (0), Music on Hold Filename, Ringback Audio Filename, Reliable Provisional Responses (Supported), Send Symmetric Packetization Time (Yes), Use tel: for Outgoing 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.
- RTCP: Enable RTCP, RTCP, RTCP_XR, Transmission Interval (secs) (5).
- Challenger: Realm.

Step 4: Export the Self-Signed Certificate

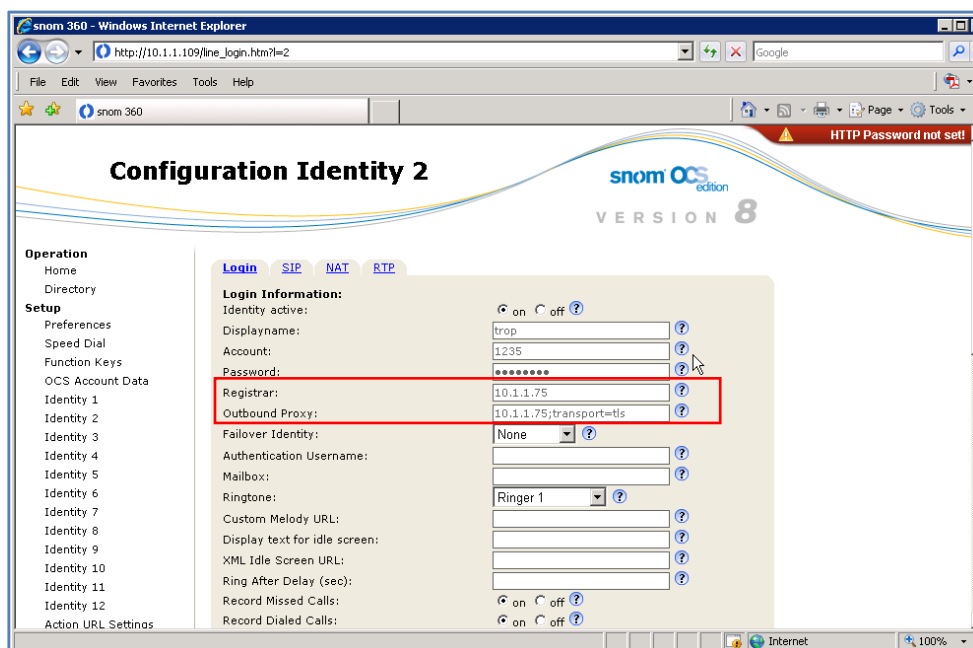
1. Use VXbuilder's Manage File or FTP to move the file to your PC.

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

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.

The screenshot shows the 'OCS Account Data' configuration page in a web browser. The page title is 'snom 360 - Windows Internet Explorer' and the URL is 'http://10.1.1.109/ocs.htm'. The left navigation pane shows 'Setup' > 'OCS Account Data' selected. The main content area has a heading 'OCS Account Data' and a sub-heading 'Please type in your account data here'. Below this, there are three input fields: 'SIP-URI' with the value 'jsmith@vx.net', 'Username (DOMAIN\USERNAME)' with the value 'vx\jsmith', and 'Password' with a masked value '*****'. Each field has a help icon (?). A 'Save' button is located below the password field.

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.

The screenshot shows the 'Configuration Identity 1' page in a web browser. The page title is 'snom 360 - Windows Internet Explorer' and the URL is 'http://10.1.1.109/line_login.htm?l=1'. The left navigation pane shows 'Setup' > 'Identify 1' selected. The main content area has a heading 'Configuration Identity 1' and a sub-heading 'Login'. Below this, there are several input fields: 'Identity active:' with a radio button set to 'on', 'Displayname:' with the value 'James Smith', 'Account:' with the value 'jsmith', 'Password:' with a masked value '*****', 'Registrar:' with the value 'vx.net', 'Outbound Proxy:' with the value 'ocs.vx.net;transport=tcp', 'Failover Identity:' with a dropdown menu set to 'Identity 2', 'Authentication Username:' with the value 'vx\jsmith', 'Mailbox:' with the value 'sip:jsmith@vx.net;opaque=app', 'Ringtone:' with a dropdown menu set to 'Ringer 1', 'Custom Melody URL:', 'Display text for idle screen:' with the value 'James Smith', 'XML Idle Screen URL:', 'Ring After Delay (sec):', 'Record Missed Calls:', 'Record Dialed Calls:', and 'Record Received Calls:'. Each field has a help icon (?). A red box highlights the 'Outbound Proxy' field. At the bottom, there are buttons for 'Save', 'Re-Register', 'Play Ringer', 'Remove Identity', and 'Remove All Identities'.

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.

The screenshot shows the 'Configuration Identity 1' page in a Windows Internet Explorer browser. The address bar shows 'http://10.1.1.109/line_sip.htm?l=1'. The page has a sidebar on the left with a tree view containing 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), and Manual. The main content area has tabs for 'Login', 'SIP', 'NAT', and 'RTP', with 'SIP' selected. Below the tabs is the 'SIP Identity Settings' section. It contains various configuration options with input fields, radio buttons, and dropdown menus. At the bottom of the settings area is a 'Save' button.

Configuration Identity 1

snom OCS edition
VERSION 8

Operation
Home
Directory

Setup
Preferences
Speed Dial
Function Keys
OCS Account Data
Identity 1
Identity 2
Identity 3
Identity 4
Identity 5
Identity 6
Identity 7
Identity 8
Identity 9
Identity 10
Identity 11
Identity 12
Action URL Settings
Advanced
Trusted Certificates
Software Update

Status
System Information
Log
SIP Trace
DNS Cache
Subscriptions
PCAP Trace
Memory
Settings

Manual

SIP Identity Settings:

Music on hold server: ?

Alert Info URL: ?

User picture URL: ?

Dial-Plan String: ?

ENUM Support: ☐ on ☒ off ?

Countrycode: ?

Areacode: ?

Proxy Require: ?

Additional supported headers: ?

Q-Value: ?

Proposed Expiry: ?

Auto Answer: ☐ on ☒ off ?

Long SIP-Contact (RFC3840): ☐ on ☒ off ?

Support broken Registrar: ☒ on ☐ off ?

Shared Line: ☐ on ☒ off ?

Publish Presence on bootup: ☒ on ☐ off ?

DTMF via SIP INFO: ?

Send display name on INVITE: ☐ on ☒ off ?

Extension Monitoring Call Pickup List: ☐ on ☒ off ?

Extension Monitoring Call Pickup List URI: ?

Contact List: ☒ on ☐ off ?

Contact List URI: ?

Server Type Support: ?

Remove all bindings on unregister: ☐ on ☒ off ?

Subscription Expiry (s): ?

Enable hook flash: ☐ on ☒ off ?

Report Machine State: ☒ on ☐ off ?

Report Phone State: ☒ on ☐ off ?

Save

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

snom 360 - Windows Internet Explorer

http://10.1.1.109/line_login.htm?l=2

File Edit View Favorites Tools Help

snom 360

Configuration Identity 2

snom OCS edition
VERSION 8

Operation
Home
Directory

Setup
Preferences
Speed Dial
Function Keys
OCS Account Data
Identity 1
Identity 2
Identity 3
Identity 4
Identity 5
Identity 6
Identity 7
Identity 8
Identity 9
Identity 10
Identity 11
Identity 12
Action URL Settings
Advanced
Trusted Certificates
Software Update

Status
System Information
Log
SIP Trace

Login SIP NAT RTP

Login Information:

Identity active: ☒ on ☐ off ?

Displayname: trop ?

Account: 1235 ?

Password: ***** ?

Registrar: 10.1.1.75 ?

Outbound Proxy: 10.1.1.75 ?

Failover Identity: None ?

Authentication Username: ?

Mailbox: ?

Ringtone: Ringer 1 ?

Custom Melody URL: ?

Display text for idle screen: ?

XML Idle Screen URL: ?

Ring After Delay (sec): ?

Record Missed Calls: ☒ on ☐ off ?

Record Dialed Calls: ☒ on ☐ off ?

Record Received Calls: ☒ on ☐ off ?

Save Re-Register Play Ringer

Remove Identity

Remove All Identities

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.

The screenshot shows the 'Configuration Identity 2' page in a Windows Internet Explorer browser. The address bar shows 'http://10.1.1.109/line_sip.htm?i=2'. The page has a sidebar on the left with a tree view containing 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), and Manual. The main content area has tabs for 'Login', 'SIP', 'NAT', and 'RTP', with 'SIP' selected. Below the tabs is the 'SIP Identity Settings' section. It contains various configuration fields and options for Identity 2, including Music on hold server, Alert Info URL, User picture URL, Dial-Plan String, ENUM Support (radio buttons for on/off), Countrycode, Areacode, Proxy Require, Additional supported headers, Q-Value (dropdown set to 1.0), Proposed Expiry (text field with 3600), Auto Answer (radio buttons for on/off), Long SIP-Contact (RFC3840) (radio buttons for on/off), Support broken Registrar (radio buttons for on/off), Shared Line (radio buttons for on/off), Publish Presence on bootup (radio buttons for on/off), DTMF via SIP INFO (dropdown set to off), Send display name on INVITE (radio buttons for on/off), Extension Monitoring Call Pickup List (radio buttons for on/off), Extension Monitoring Call Pickup List URI (text field), Contact List (radio buttons for on/off), Contact List URI (text field), Server Type Support (dropdown set to Default), Remove all bindings on unregister (radio buttons for on/off), Subscription Expiry (s) (text field with 3600), Enable hook flash (radio buttons for on/off), Report Machine State (radio buttons for on/off), and Report Phone State (radio buttons for on/off). Each field has a help icon (question mark). At the bottom of the settings area is a 'Save' button.

Configuration Identity 2

snom OCS edition
VERSION 8

Operation
Home
Directory

Setup
Preferences
Speed Dial
Function Keys
OCS Account Data
Identity 1
Identity 2
Identity 3
Identity 4
Identity 5
Identity 6
Identity 7
Identity 8
Identity 9
Identity 10
Identity 11
Identity 12
Action URL Settings
Advanced
Trusted Certificates
Software Update

Status
System Information
Log
SIP Trace
DNS Cache
Subscriptions
PCAP Trace
Memory
Settings

Manual

SIP Identity Settings:

Music on hold server: ?

Alert Info URL: ?

User picture URL: ?

Dial-Plan String: ?

ENUM Support: ☐ on ☒ off ?

Countrycode: ?

Areacode: ?

Proxy Require: ?

Additional supported headers: ?

Q-Value: 1.0 ?

Proposed Expiry: 3600 ?

Auto Answer: ☐ on ☒ off ?

Long SIP-Contact (RFC3840): ☐ on ☒ off ?

Support broken Registrar: ☒ on ☐ off ?

Shared Line: ☐ on ☒ off ?

Publish Presence on bootup: ☒ on ☐ off ?

DTMF via SIP INFO: off ?

Send display name on INVITE: ☐ on ☒ off ?

Extension Monitoring Call Pickup List: ☐ on ☒ off ?

Extension Monitoring Call Pickup List URI: ?

Contact List: ☐ on ☒ off ?

Contact List URI: ?

Server Type Support: Default ?

Remove all bindings on unregister: ☐ on ☒ off ?

Subscription Expiry (s): 3600 ?

Enable hook flash: ☐ on ☒ off ?

Report Machine State: ☒ on ☐ off ?

Report Phone State: ☒ on ☐ off ?

Save

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

The screenshot shows the 'Advanced Settings' page of a snom 360 device, accessed via a web browser. The browser's address bar shows 'http://10.1.1.109/advanced_network.htm'. The page has a navigation tree on the left and a main settings area on the right. The navigation tree includes sections for 'Operation' (Home, Directory), 'Setup' (Preferences, Speed Dial, Function Keys, OCS Account Data, Identities 1-12, Action URL Settings, Advanced, Trusted Certificates, Software Update), and 'Status' (System Information, Log, SIP Trace, DNS Settings). The 'Advanced' option under 'Setup' is selected. The main settings area has tabs for 'Network', 'Behavior', 'Audio', 'SIP/RTP', 'QoS/Security', and 'Update'. The 'Network' tab is active, showing settings for DHCP (ON), IP address (10.1.1.109), Netmask (255.255.255.0), Host Name, IP Gateway (10.1.1.50), DNS (Domain: vx.net, Servers: 10.1.1.4), Time (NTP Time Server: 10.1.1.4, NTP Refresh Time: 3600, Timezone: -8 United States - Pacific Time), and HTTP (HTTP Proxy, HTTP port: 80, HTTPS port: 443, Webserver connection type: http or https, Auto Logout). Each input field has a help icon (?) to its right.

snom 360 - Windows Internet Explorer
http://10.1.1.109/advanced_network.htm

File Edit View Favorites Tools Help

snom 360

Advanced Settings

snom OCS edition
VERSION 8

Operation
Home
Directory

Setup
Preferences
Speed Dial
Function Keys
OCS Account Data
Identity 1
Identity 2
Identity 3
Identity 4
Identity 5
Identity 6
Identity 7
Identity 8
Identity 9
Identity 10
Identity 11
Identity 12
Action URL Settings
Advanced
Trusted Certificates
Software Update

Status
System Information
Log
SIP Trace
DNS Settings

Network Behavior Audio SIP/RTP QoS/Security Update

Network:
DHCP: ☐ on ☒ off ?
IP address: ?
Netmask: ?
Host Name: ?
IP Gateway: ?

DNS:
Domain: ?
DNS Server 1: ?
DNS Server 2: ?

Time:
NTP Time Server: ?
NTP Refresh Time (sec): ?
Timezone: ?

HTTP:
HTTP Proxy: ?
HTTP port: ?
HTTPS port: ?
Webserver connection type: ?
Auto Logout (min): ?

8. View System Information to confirm your settings.

The screenshot shows a web browser window titled "snom 360 - Windows Internet Explorer" with the address bar displaying "http://10.1.1.109/info.htm". The page is titled "System Information" and features the "snom OCS edition VERSION 8" logo. On the left, a navigation menu lists sections: Operation (Home, Directory), Setup (Preferences, Speed Dial, Function Keys, OCS Account Data, Identities 1-12, Action URL Settings, Advanced, Trusted Certificates, Software Update), and Status (System Information, Log, SIP Trace, DNS Settings). The main content area displays the following information:

System Information:	
Phone Type:	snom360-SIP
MAC-Address:	000413294EDB
IP-Address:	10.1.1.109
Firmware-Version:	snom360-SIP snapshot_branch_8_2_2009_06_08_22_00_03_snom 18991
Firmware-URL:	http://provisioning.snom.com/tmp/snom360-OCS-snapshot_branch_8_2_2009_06_08_22_00_03_snom-SIP-f.bin
Production Information:	Mac:000413294EDB;Version:Standard;Hardware:snom360 (H:R2A,PO:2007-10091);Date:17/12/07;Copyright(C) snom technology AG
Uptime:	0 days, 1 hours, 26 minutes
Memfree:	1148 K
Bootloader-Version:	1.1.3-s

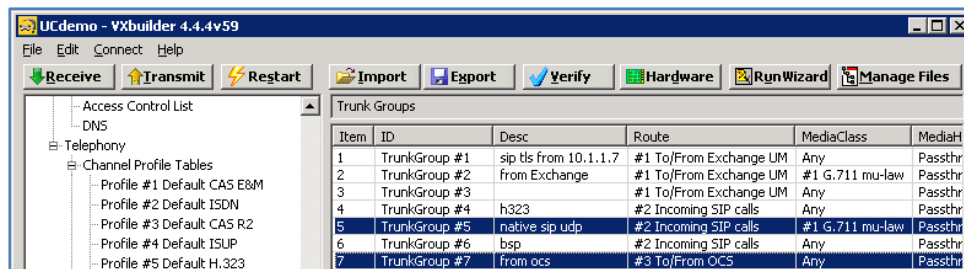
SIP Identity Status:	
Identity 1 Status:	jsmith@vx.net: OK
Identity 2 Status:	1235@10.1.1.75: Success
Identity 3 Status:	
Identity 4 Status:	
Identity 5 Status:	
Identity 6 Status:	
Identity 7 Status:	
Identity 8 Status:	
Identity 9 Status:	
Identity 10 Status:	
Identity 11 Status:	
Identity 12 Status:	

Ethernet Status:	
Net Port:	Connection Type: 10 Mbit Half Duplex Status: connected
PC Port:	Connection Type: Status: not connected

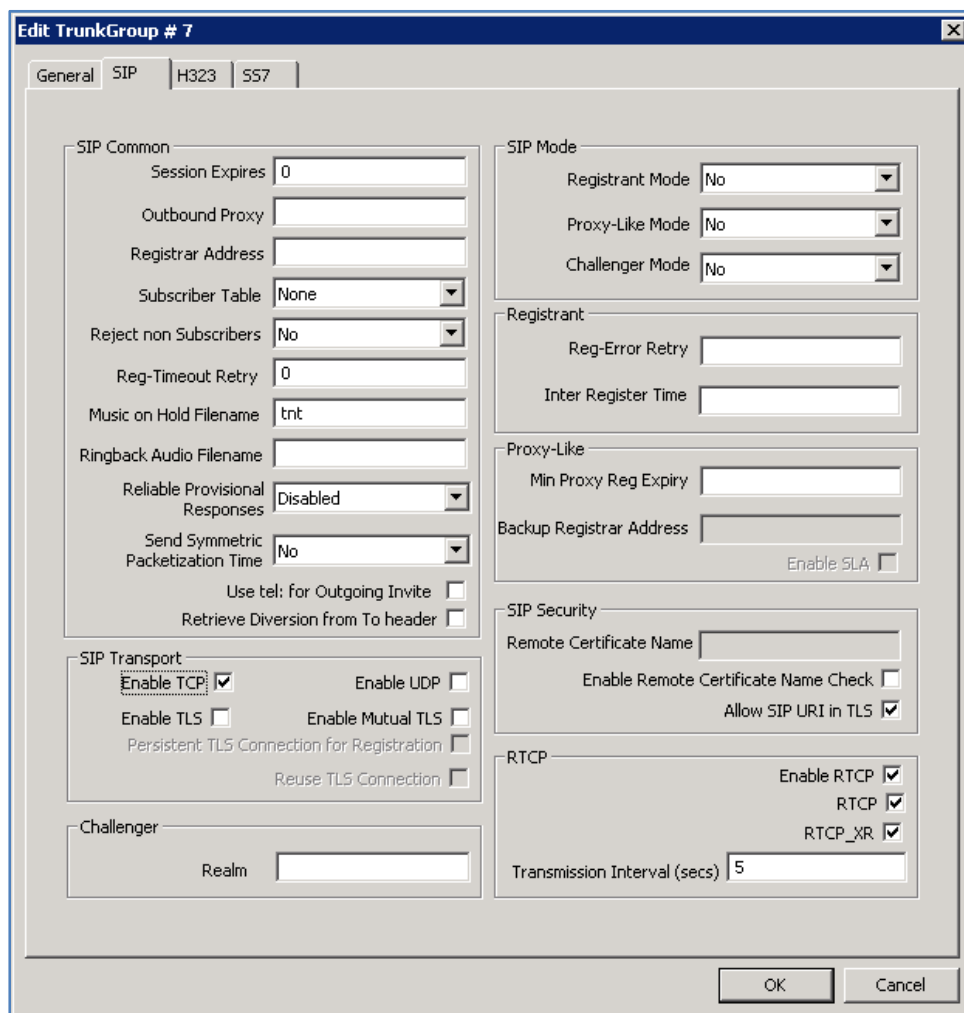
9. Your snom phone is now ready to use.



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.

Edit Call Route # 2

General Parameters

Enabled ☒ Using Regular Expression ☐ Desc: all SIP calls to mediation Priority: 0

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 ☒ SIP Proxy ☐ SIP Registrar Table ☐ Other ☐ Call Route Table ☐ [Unchanged]

TrunkGroup: #7 from ocs Node ID: [N/A]

SIP Proxy: mediation.vx.net:5060 Peer IP / IF: [Unchanged]

Call Route No.: None

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.

Edit TrunkGroup # 5

General SIP H323 SS7

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: ☐

Retrieve Diversion from To header: ☐

SIP Transport

Enable TCP: ☐ Enable UDP: ☒

Enable TLS: ☐ Enable Mutual TLS: ☐

Persistent TLS Connection for Registration: ☐

Reuse TLS Connection: ☐

Challenger

Realm:

SIP Mode

Registrant Mode: No

Proxy-Like Mode: No

Challenger Mode: No

Registrant

Reg-Error Retry: 100

Inter Register Time: 100

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: ☐

RTCP

Enable RTCP: ☐

RTCP: ☐

RTCP_XR: ☐

Transmission Interval (secs): 5

OK Cancel

14. Call Route to SIP Registrar.

Edit Call Route # 5

General Parameters

Enabled ☒ Using Regular Expression ☐ Desc UC IDD to Native SIP Priority 0

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 ☐ SIP Proxy ☒ SIP Registrar Table ☐ Other ☐ Call Route Table ☐ [Unchanged]

TrunkGroup [N/A] Node ID [N/A] SIP Proxy Peer IP / IP [Unchanged] Call Route No. None

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 (hex)	In Trunkgroup#	Calling Number	Called Number	Out Node ID or Trunkgroup#	Inbound Transport	Outbound Transport
x001d	Tkgrp: 5	14083489775	+1114	Tkgrp: 7	UDP	TCP

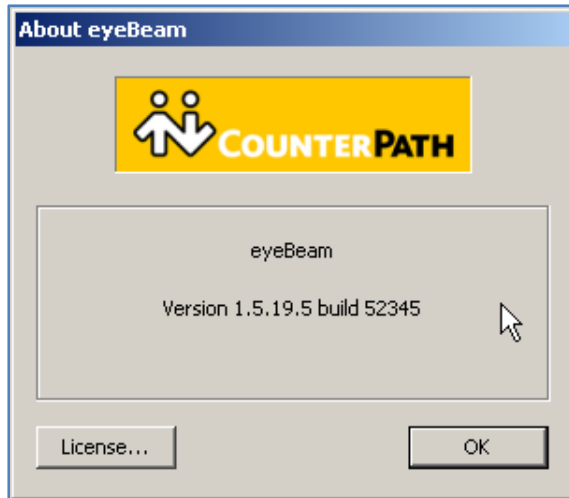
10.1.1.75 - PuTTY						
UCdemo#						
UCdemo# sho call detail						
CSN (hex)	In Trunkgroup#	Calling Number	Called Number	Out Node ID or Trunkgroup#	Inbound Transport	Outbound Transport
x001f	Tkgrp: 7	+1114	14083489775@...51784	Tkgrp: 5	TCP	UDP

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

10.1.1.75 - PuTTY						
UCdemo# sho call detail						
CSN (hex)	In Trunkgroup#	Calling Number	Called Number	Out Node ID or Trunkgroup#	Inbound Transport	Outbound Transport
x0030	Tkgrp: 5	1235	14083489775@...51784	Tkgrp: 5	UDP	UDP

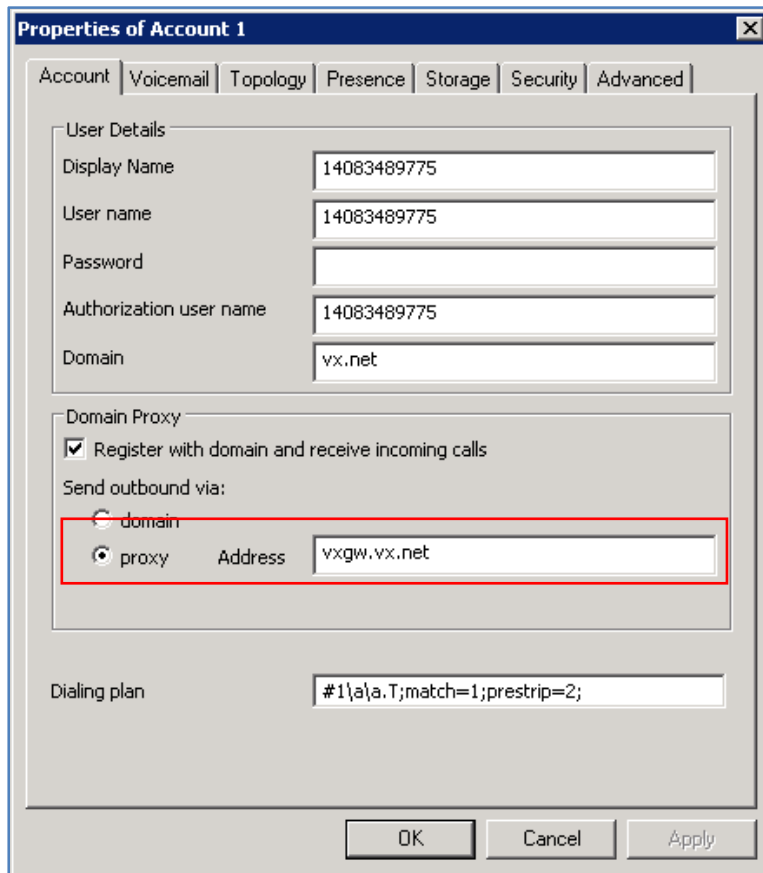
Configuring TLS on eyeBeam

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.



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.



Properties of Account 1

Account | Voicemail | Topology | Presence | Storage | Security | Advanced

User Details

Display Name: 14083489775

User name: 14083489775

Password:

Authorization user name: 14083489775

Domain: vx.net

Domain Proxy

☒ Register with domain and receive incoming calls

Send outbound via:

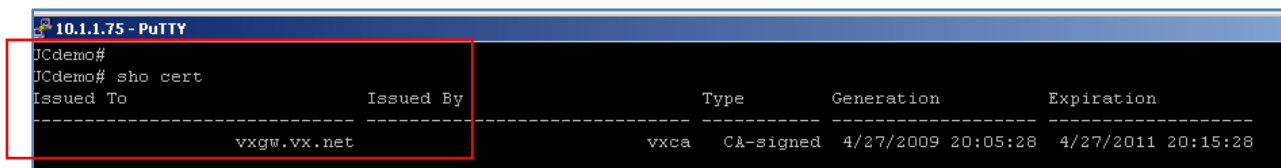
☐ domain

☒ proxy Address: vxgw.vx.net

Dialing plan: #1\a\a.T;match=1;prestrip=2;

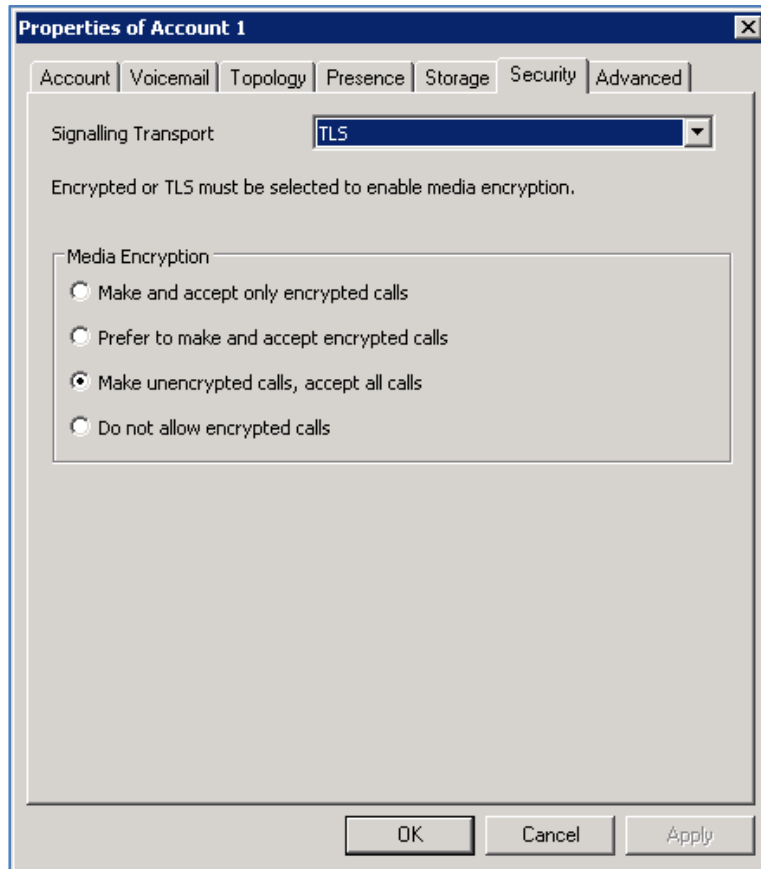
OK Cancel Apply

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

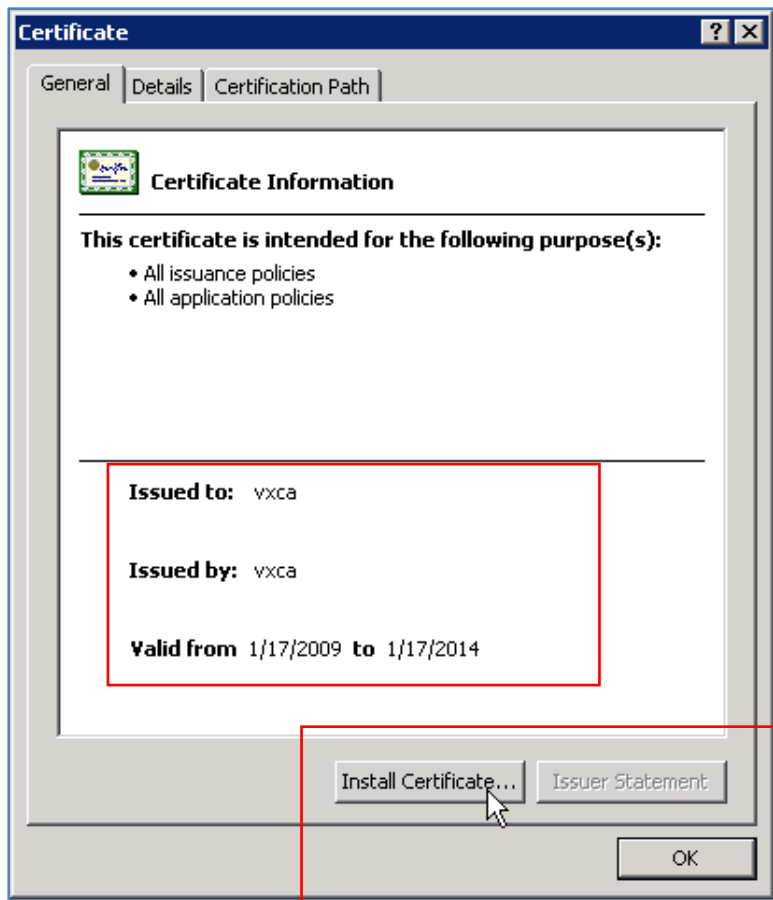


Step 3: Importing the Root Certificate to the eyeBeam PC

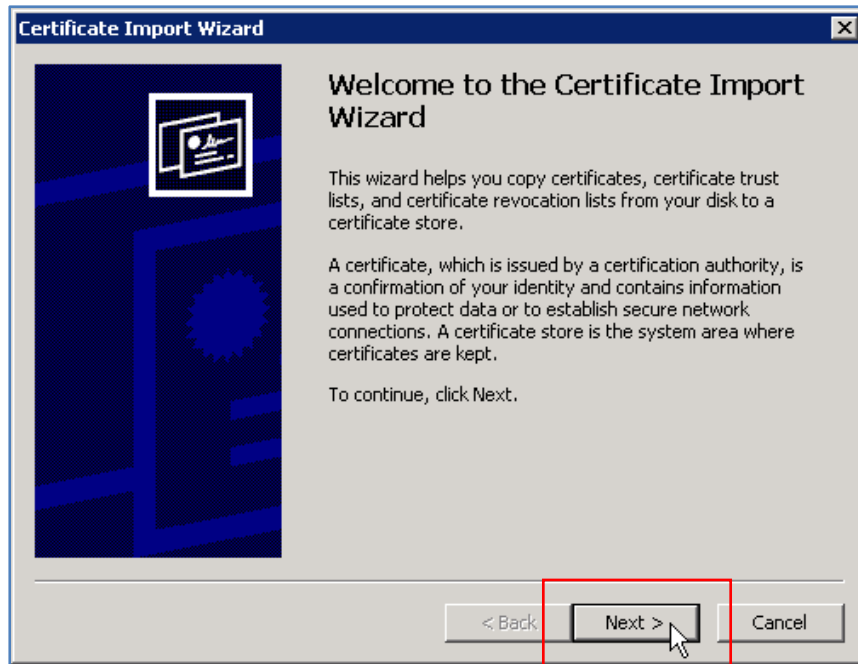
1. Transfer to the PC the **root certificate** of the Certificate Authority that signed the **vxgw.vx.net** certificate.



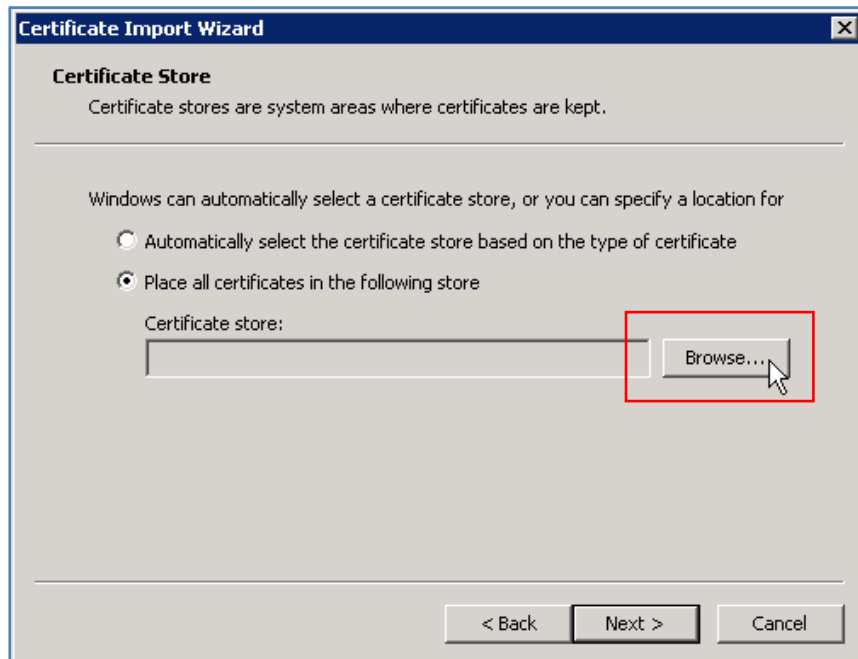
2. On the Certificate view, General Tab, Double click **Install Certificate** to install the certificate using the following instructions.
 - a. **vxca** is the root certificate from the Certificate Authority used to sign the **vxgw.vx.net** certificate.



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



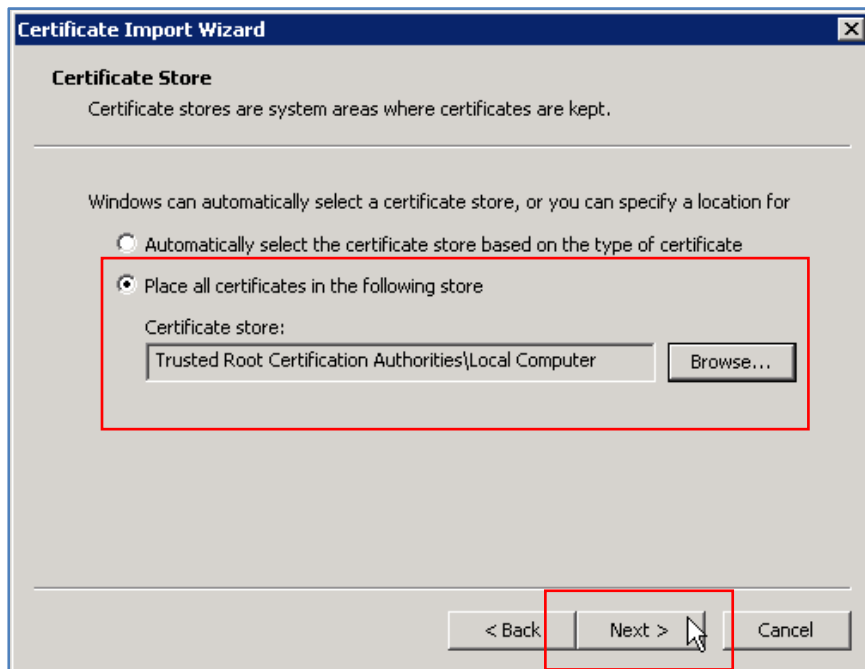
4. **Browse** the Certificate Store to select certificate storage location. Click **Next** to continue.



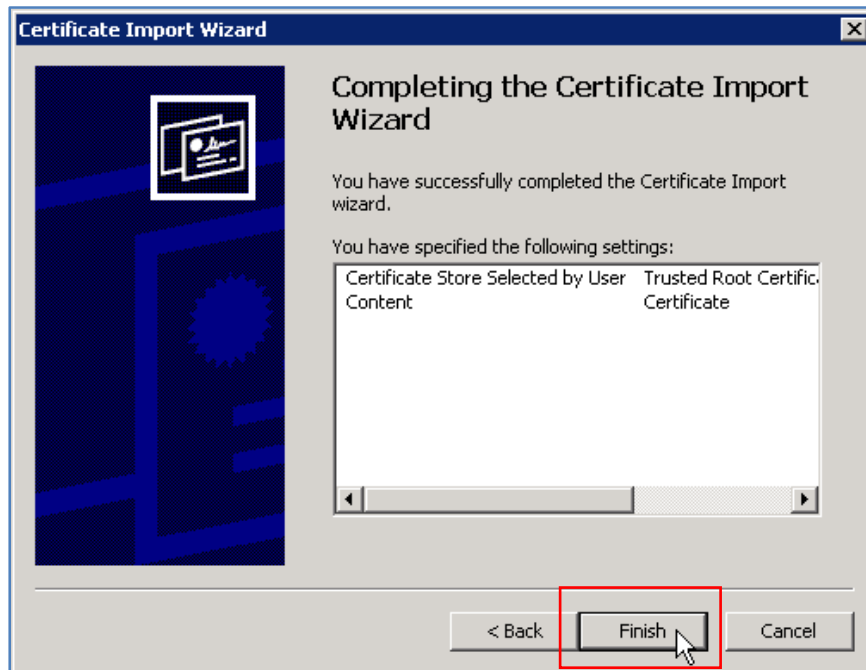
5. Select the **Certificate Store** and click **OK**.



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**.



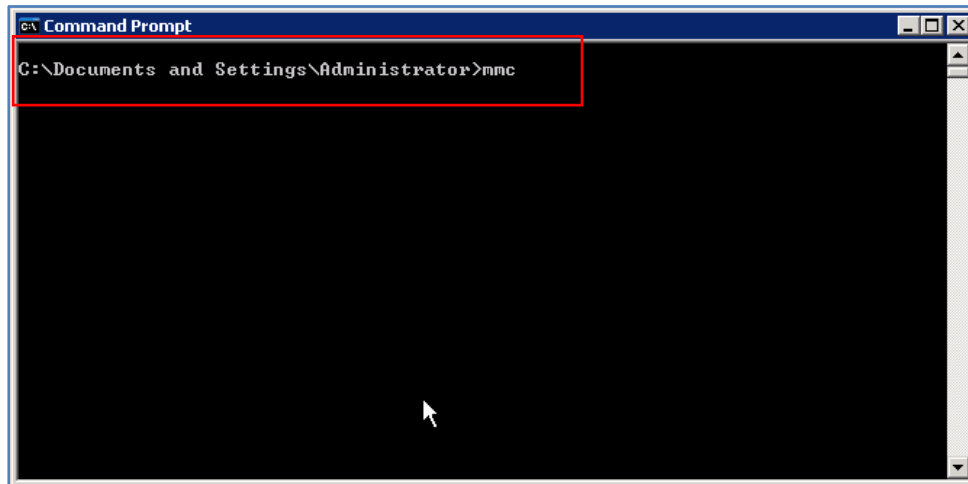
9. You must now **REBOOT your PC** to complete the process. This is a required step to complete the process.

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

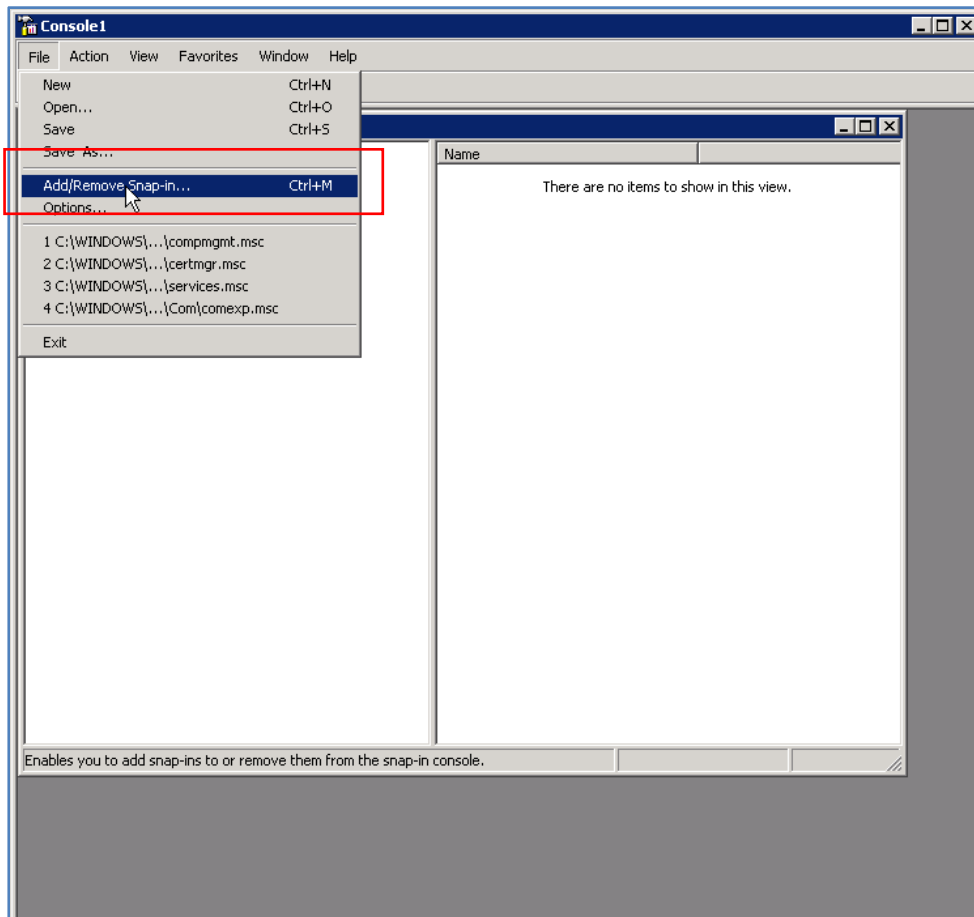
Step 4: Verify Certificate Installation

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

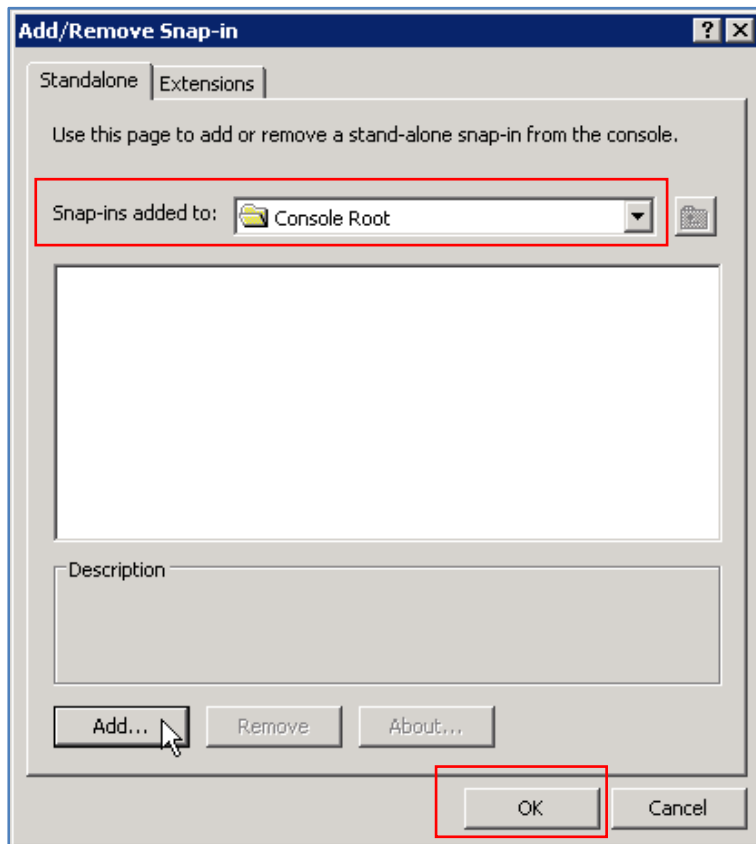
1. At the command prompt, enter **mmc**



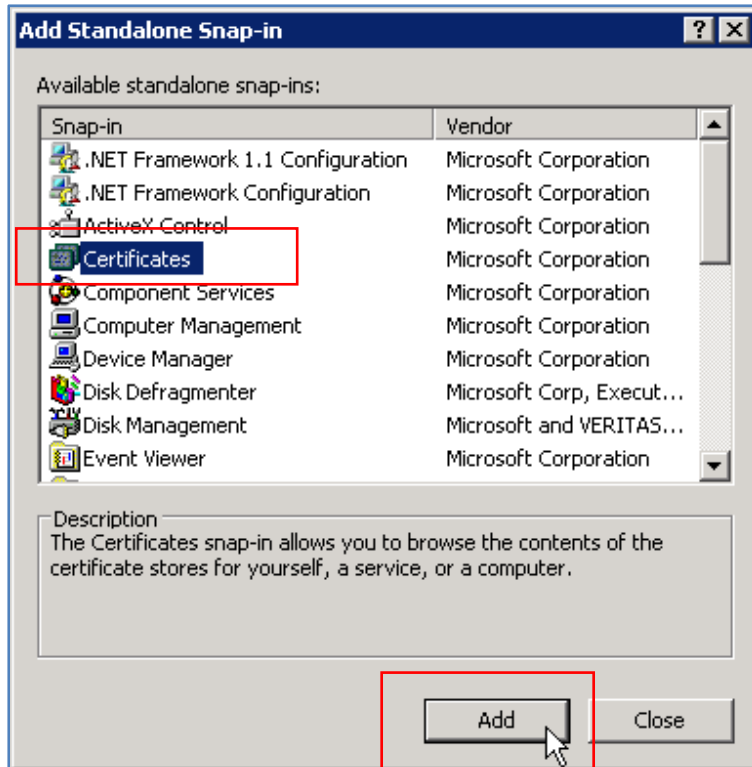
2. At the Console 1 view, select **Add/Remove Snap-In...**



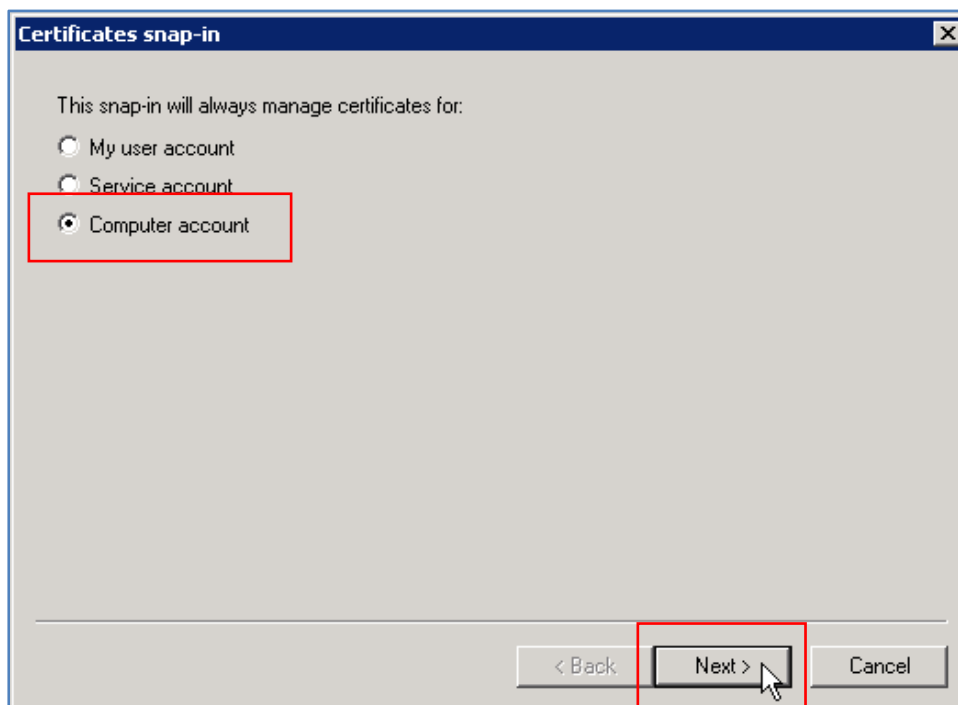
3. From the Standalone Tab, select the **Console Root** folder from the **Snap-ins added to** field. Click **Add** and then **OK**. The Add Standalone Snap-in view displays.



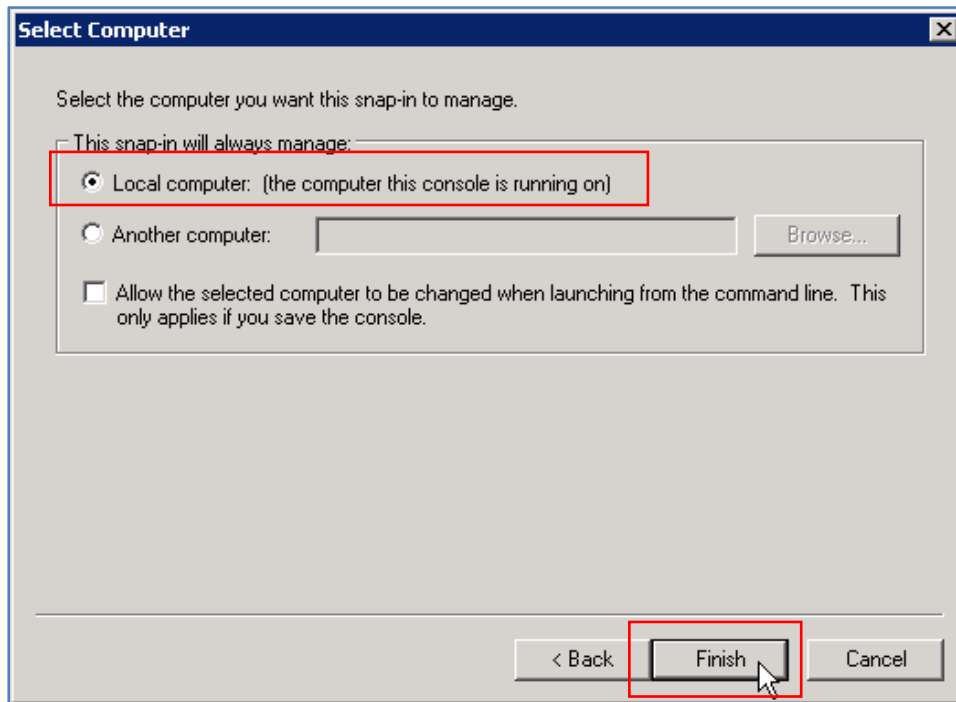
4. Select the **Certificates**, and click **Add**. The Certificates snap-in view displays.



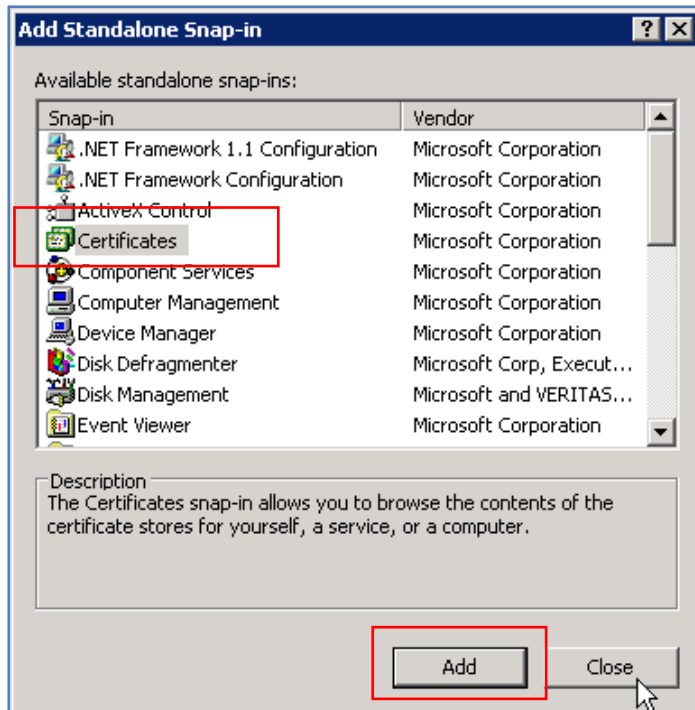
5. Select the radio button for **Computer account** and click **Next**.



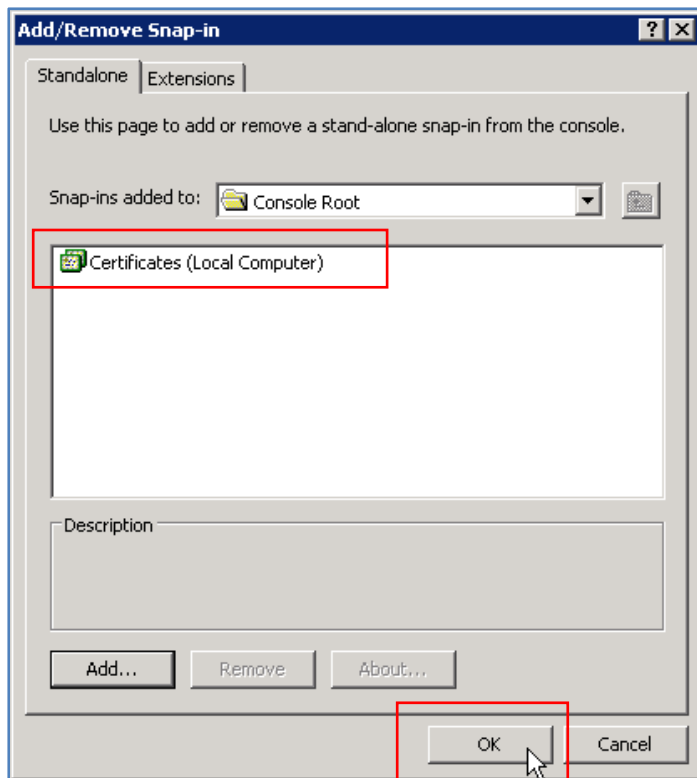
6. Select the radio button for **Local computer** and click **Finish**.



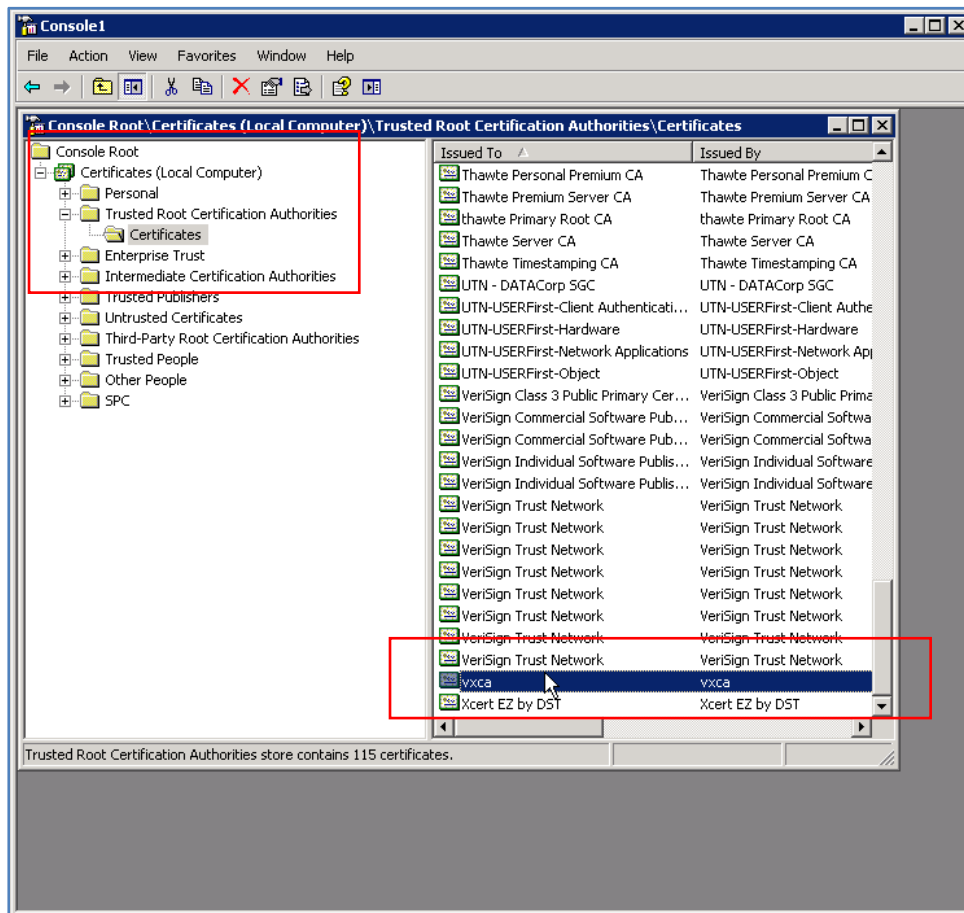
7. From the **Add Standalone Snap-in** view, select **Certificates** and click **Add**.



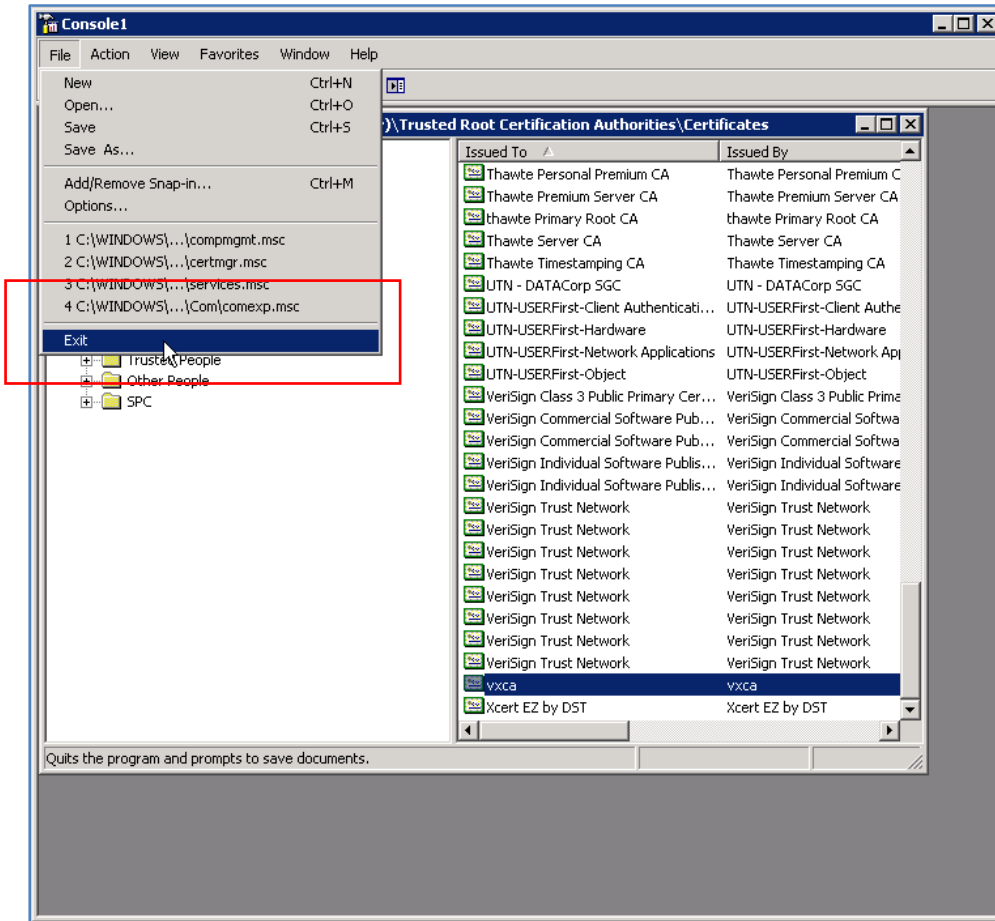
8. From the Standalone Tab, the **Certificates (Local Computer)** Snap-ins display as added. Click **OK**.



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.

Edit TrunkGroup # 1

General SIP H323 SS7

SIP Common

Session Expires

Outbound Proxy

Registrar Address

Subscriber Table

Reject non Subscribers

Reg-Timeout Retry

Music on Hold Filename

Ringback Audio Filename

Reliable Provisional Responses

Send Symmetric Packetization Time

Use tel: for Outgoing Invite ☐

Retrieve Diversion from To header ☐

SIP Mode

Registrant Mode

Proxy-Like Mode

Challenger Mode

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 ☒

SIP Transport

Enable TCP ☐

Enable UDP ☐

Enable TLS ☒

Enable Mutual TLS ☐

Persistent TLS Connection for Registration ☒

Reuse TLS Connection ☒

Challenger

Realm

RTCP

Enable RTCP ☒

RTCP ☒

RTCP_XR ☒

Transmission Interval (secs)

OK Cancel

Step 6: VX General Menu

The vxgw.vx.net installed certificate.

The image shows a 'General Settings' dialog box with various configuration options organized into sections. The 'Certificate' section is highlighted, showing the 'vxgw.vx.net' certificate name. Other sections include 'Clock Source', 'Secure Relay', 'Time Server', 'SNMP', 'Misc', 'LLEM', 'Comfort Noise', 'STI Clock Auto-Fallback', and 'Radius'. Checkboxes and dropdown menus are used for many settings, and some have associated buttons like 'Edit MOTD' and 'Edit Banner'.

Section	Parameter	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
	Max Change	7200 sec
SNMP	Community Name	public
	MIB-II Support	<input type="checkbox"/>
Certificate	Certificate Name	vxgw.vx.net
	Require TLS for domain login	<input type="checkbox"/>
	Allow untrusted root certificate	<input type="checkbox"/>
Comfort Noise	Send CN RTP packets	Enabled
	Generate TDM CN on Media stream absence	<input type="checkbox"/>
	Comfort Noise Level	58 -dBov
Media stream timeout	Media stream timeout	100 ms
	Misc	Mid-call DTMF Digits
T.38 Fax Redundancy	T.38 Fax Redundancy	0
	T.38 CNG Detect	<input checked="" type="checkbox"/>
Fax/Modem bypass on PCM	Fax/Modem bypass on PCM	<input checked="" type="checkbox"/>
	LLEM	Status Update Interval
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"/>

Step 7: eyeBeam TLS to snom Calls

10.1.1.75 - PuTTY

```
UCdemo#
UCdemo# sho call detail
```

CSN (hex)	In Trunkgroup#	Calling Number	Called Number	Out Node ID or Trunkgroup#	Inbound Transport	Outbound Transport
x0001	Tkgrp: 1	14083489775	1235@10.1.1.109	Tkgrp: 5	TLS	UDP

10.1.1.75 - PuTTY

```
UCdemo# sho call detail
```

CSN (hex)	In Trunkgroup#	Calling Number	Called Number	Out Node ID or Trunkgroup#	Inbound Transport	Outbound Transport
x0002	Tkgrp: 1	14083489775	1235@10.1.1.109:2062	Tkgrp: 1	TLS	TLS

Step 8: snom TLS Configuration

snom 360 - Windows Internet Explorer

http://10.1.1.109/line_login.htm?l=2

File Edit View Favorites Tools Help

snom 360

HTTP Password not set!

Configuration Identity 2

snom OCS edition
VERSION 8

Operation

- Home
- Directory

Setup

- Preferences
- Speed Dial
- Function Keys
- OCS Account Data
- Identity 1
- Identity 2
- Identity 3
- Identity 4
- Identity 5
- Identity 6
- Identity 7
- Identity 8
- Identity 9
- Identity 10
- Identity 11
- Identity 12
- Action URL Settings
- Advanced
- Trusted Certificates
- Software Update

Status

- System Information

Login **SIP** **NAT** **RTP**

Login Information:

Identity active: ☒ on ☐ off ?

Displayname: trop ?

Account: 1235 ?

Password: ***** ?

Registrar: vxgw.vx.net ?

Outbound Proxy: vxgw.vx.net;transport=tls ?

Fallover Identity: None ?

Authentication Username: ?

Mailbox: ?

Ringtone: Ringer 1 ?

Custom Melody URL: ?

Display text for idle screen: ?

XML Idle Screen URL: ?

Ring After Delay (sec): ?

Record Missed Calls: ☒ on ☐ off ?

Record Dialed Calls: ☒ on ☐ off ?

Record Received Calls: ☒ on ☐ off ?

Save Re-Register Play Ringer

Remove Identity