



Alcatel-Lucent VPN Firewall Brick®

Configuring VPN Client for the VPN Firewall Brick With
Certificate-Based Authentication

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2009 Alcatel-Lucent. All Rights Reserved.

Notice

Every effort was made to ensure that this information product was complete and accurate at the time of printing. However, information is subject to change.

Conformance statements

Federal Communications Commission (FCC) Notification and Repair Information This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If the equipment is not installed and used in accordance with the guidelines in this document, the equipment may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the expense of the user.

Alteration or modifications carried out without appropriate authorization may invalidate the user's right to operate the equipment.

Security statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of remote access features. In such an event, applicable tariffs require the customer to pay all network charges for traffic. Lucent Technologies cannot be responsible for such charges and will not make any allowance or give any credit for charges that result from unauthorized access.

Trademarks

VPN Firewall Brick is a registered trademark of Alcatel-Lucent.

Limited warranty

For terms and conditions of sale, contact your Alcatel-Lucent Account Team.

Technical Support

Alcatel-Lucent Customer Technical Support provides a technical assistance telephone number that is monitored 24 hours. For technical support (continental U.S.) call 1-866-582-3688 and select appropriate prompt. For international support, please call +1 630-224-4672.

Contents

1	Overview	5
2	Alcatel-Lucent VPN Firewall BRICK configuration	6
	Importing a Root/Intermediate CA Certificate.....	6
	Task.....	6
	Importing the CRL.....	9
	Task.....	9
	Automatic CRL Update Setting.....	11
	Task.....	11
	Creating an Identity Certificate for VPN Gateway.....	12
	Task.....	12
	Local Presence/Internal Address Pool Configuration.....	16
	Task.....	16
	Configuring a VPN Certificate User Authentication Service.....	18
	Task.....	18
	Configuring the VPN Policy.....	20
	Task.....	20
	Configuring the Client Tunnel Policy.....	24
	Task.....	24
	Allocating Licenses to the Client Tunnel Endpoint.....	29
	Task.....	29
	Configuring Users on the SMS.....	31
	Task.....	31
3	Nokia mVPN Client configuration	32
	Policy creation with Policy Tool using exported CA certificate.....	32

1 Overview

Purpose

This document explains the configuration of Alcatel-Lucent Security Management server for use with IKEv2 VPN Client. The document includes instructions for certificate-based authentication.

2 Alcatel-Lucent VPN Firewall BRICK configuration

Importing a Root/Intermediate CA Certificate

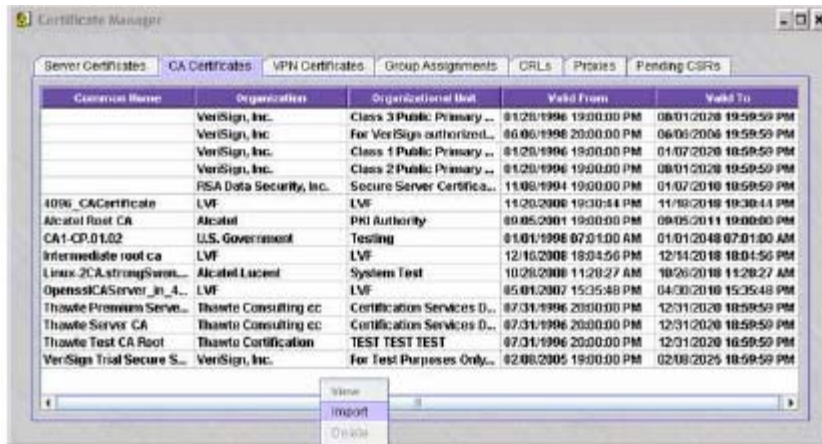
Task

Complete the following steps:

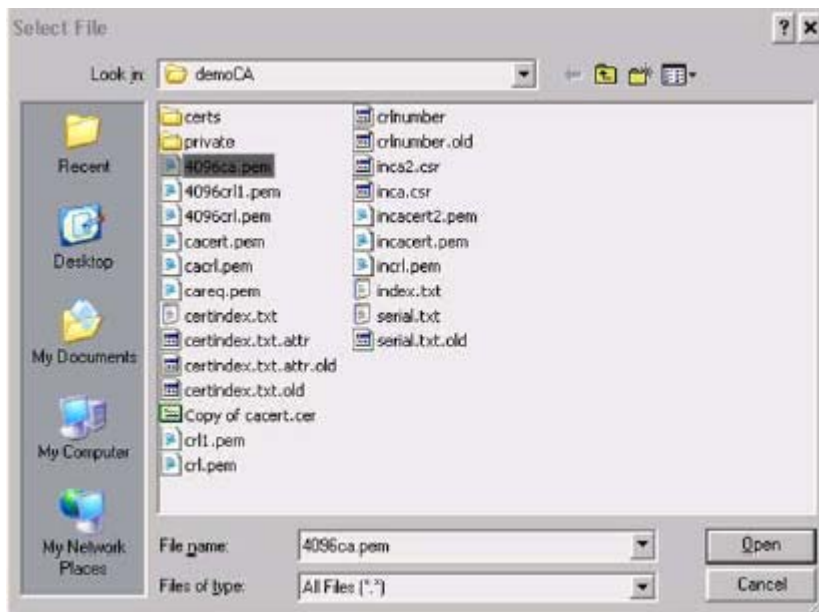
- 1 Open the Certificate Manager from SMS Navigator->Utilities->Certificate Manager.



- 2 Click on the "CA Certificates" tab then right-click and select **Import** to import CA certificate in PEM, Binary certificate, PKCS 7 PEM or PKCS 7 Binary.

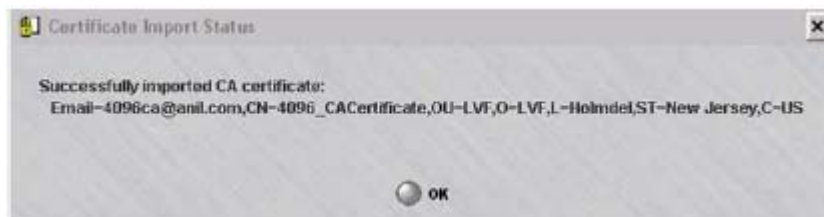


- Click on “Browse” to browse the file structure and select the CA certificate you want to import.





-
- 4 Click **OK** to import the CA certificate.



-
- 5 Click on **OK** to dismiss the message

You have successfully imported CA certificate:

If you are using chained CAs then you need to import the complete CA chain up to the root CA.

END OF STEPS

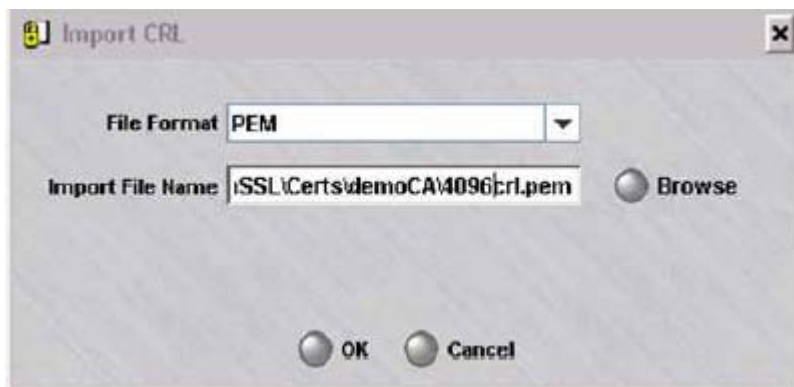
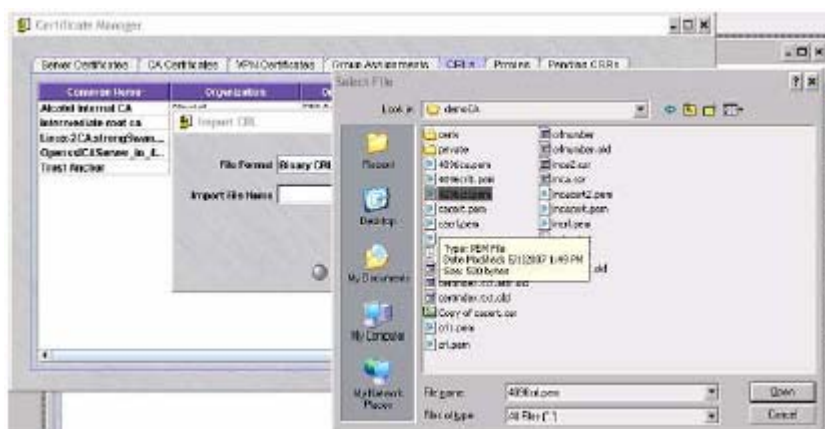
Importing the CRL

Task

Complete the following steps:

- 1 Click on the CRL tab, then right-click and select **Import**.

Click on **Browse** to select the CRL file to import. If you are using CA chain, then you need to import CRL chain up to the root.



- 2 Click **OK** to import the CRL.
- 3 Click on **OK** to dismiss the message You have successfully imported CRL:

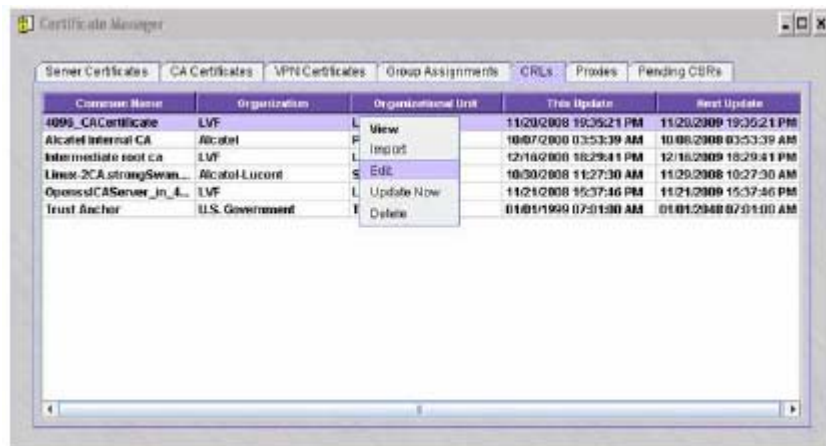


Automatic CRL Update Setting

Task

Complete the following steps:

- 1 Right-click and select **Edit** to edit the properties for the CRL you want to retrieve.



- 2 In the "Update URL" field, type the URL where the CRL will be downloaded from, and click **OK**.

The CRL will be downloaded to the SMS every 24 hours. The SMS will download the updated CRL to the Brick as required.

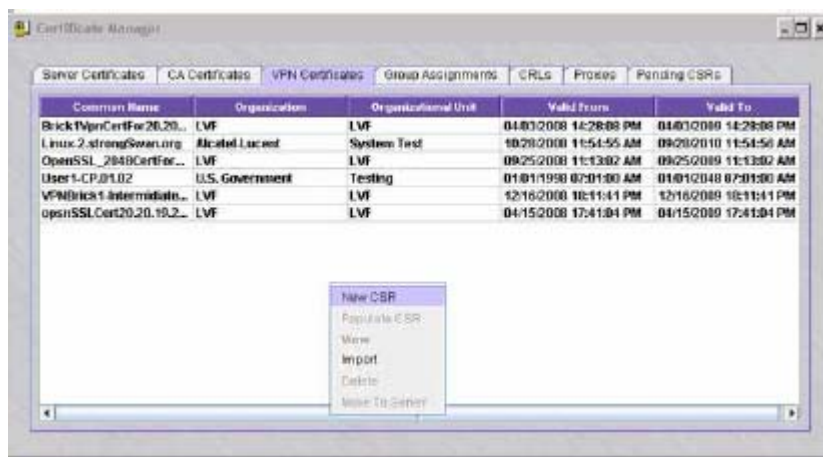


Creating an Identity Certificate for VPN Gateway

Task

Complete the following steps:

- 1 You can use the Certificate Manager to create the Identify certificate for the Gateway. Click on the VPN Certificate tab then right-click and select **New CSR**.



- 2 The Brick's ID type may be set to IP, FQDN or email address, therefore, you need to configure the certificate's SubjectAlternateName as IP, FQDN, or email.

Request Options

Key Length 1024

Key Algorithm RSA

Subject Name

Common Name Linux-2.strongSwan.org

Organization Alcatel-Lucent

Organizational Unit System Test

Locality

State/Province Name

Country US - UNITED STATES

Subject Alternate Name

Email

Domain Name Linux-2.strongSwan.org

IP Address

OK Cancel

3 Click **OK**.

The Certificate Manager will generate the Certificate Request.



4 Save the CSR and get the Identity certificate from the CA server.

The Identity certificate may be obtained in one of the following formats:

- Binary Certificate
- PEM
- PKCS 7 PEM
- PKCS 7 Binary



5 Click on **OK** to dismiss the message Created CSR file:.

6 Use the generated CSR to obtain a certificate from the CA.

Once you have obtained the certificate, click on the Certificate Manager, click on the

“VPN Certificates” tab, then right-click and select **Import**.



- 7 Select the Identity certificate by clicking **Browse** to select the certificate from your file system.



- 8 Click **OK** to import the certificate.

Now you have successfully imported the certificate.

- 9 Assign the certificate to the Group where your VPN Tunnel Endpoint is configured.



- 10 Click **OK** to add the certificate to the group.

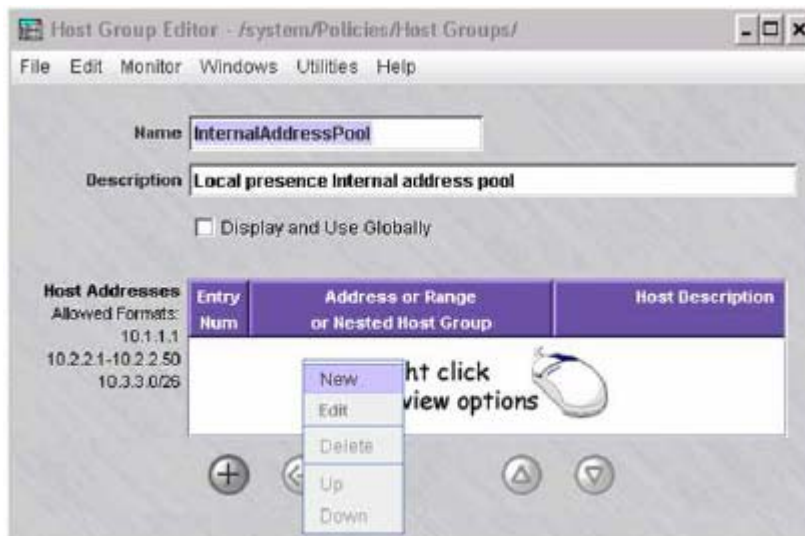
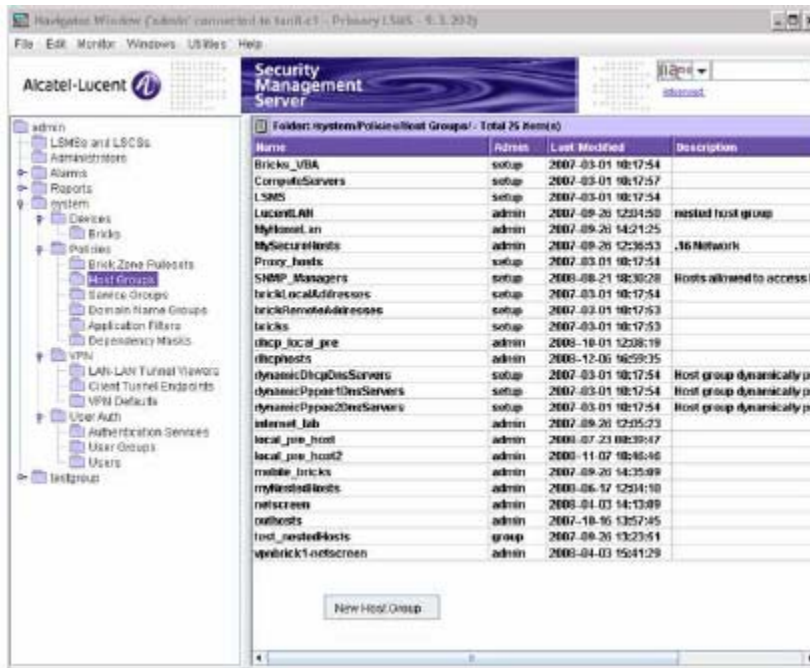
END OF STEPS

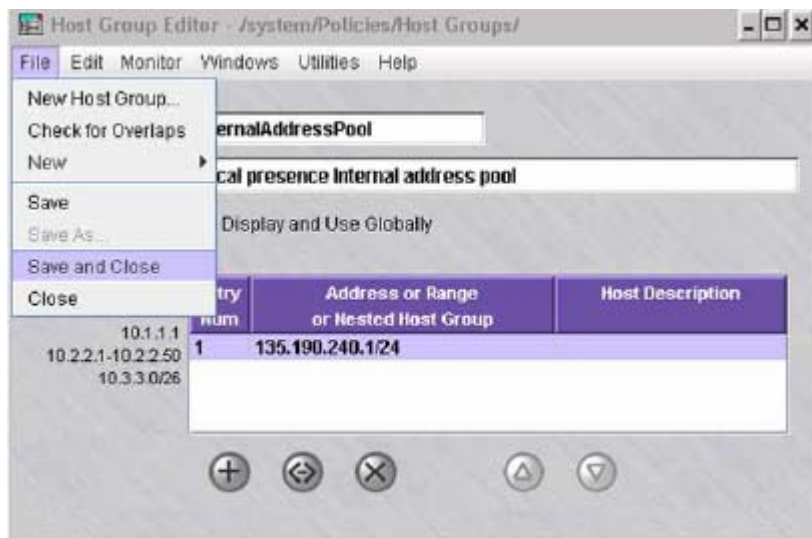
Local Presence/Internal Address Pool Configuration

Task

Complete the following steps:

- 1 Create a Hostgroup called InternalAddressPool by opening SMS Navigator->Policies->Host Groups, then right-click and select New Host Group.





2 Click **File->Save and Close** to save the Host Group.

END OF STEPS

Configuring a VPN Certificate User Authentication Service

Task

Complete the following steps:

- 1 Open SMS Navigator->User Auth->Authentication Service, then right-click and select **New Auth Service**.



- 2 Create an Authentication Service with an Auth Method of **VPN Certificate**, and select the **Required Attributes** of the client that you want the Brick/SMS to verify.

When this is completed, select **File->Save and Close**.



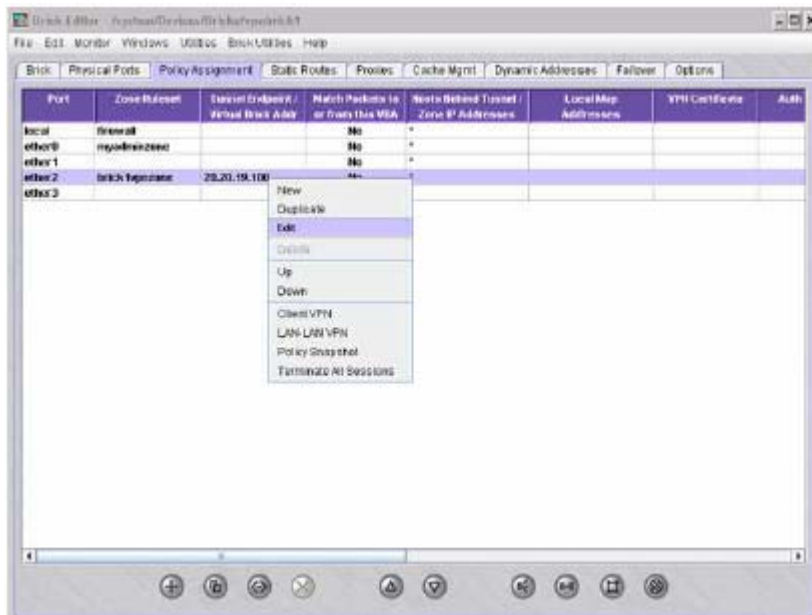
END OF STEPS

Configuring the VPN Policy

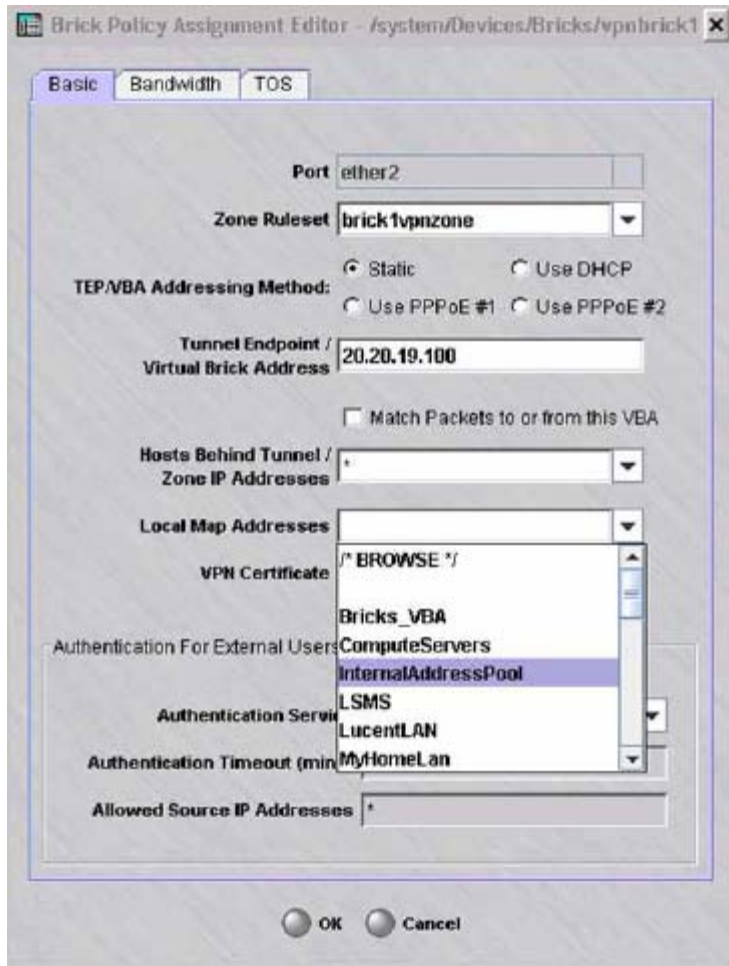
Task

Complete the following steps:

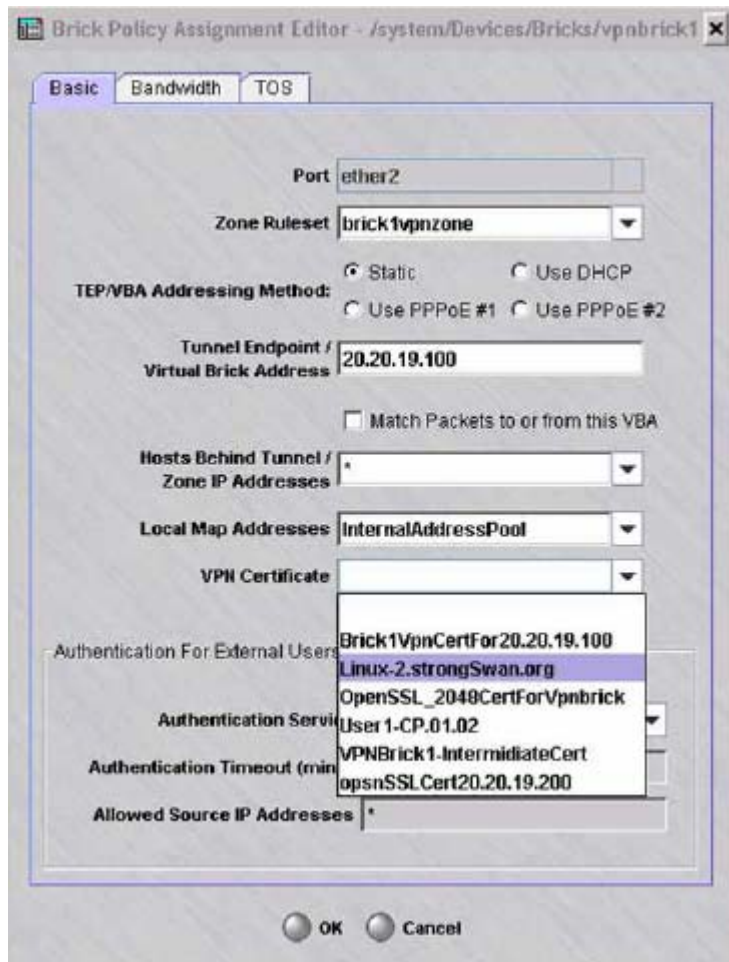
- 1 Edit the Brick with the configured VPN Tunnel Endpoint. click on the Policy Assignment tab, and select **Edit**.



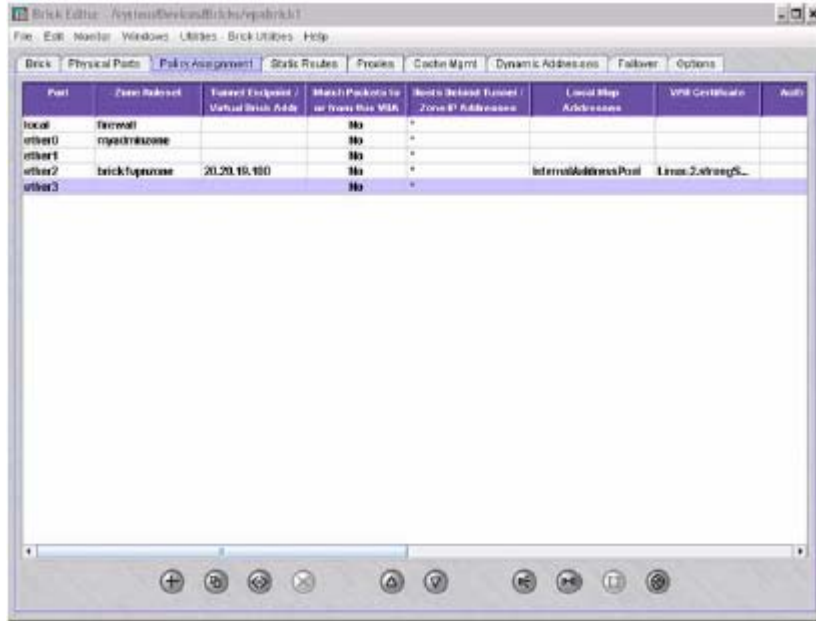
- 2 Assign the Local Presence/Internal Address created above to the VPN policy.



3 Assign the Identity certificate using the Certificate Manager.



- 4 Click **OK** to close the Policy Assignment Editor.
- 5 Click on **File->Save and Apply** to load and apply the new configuration to the Brick.



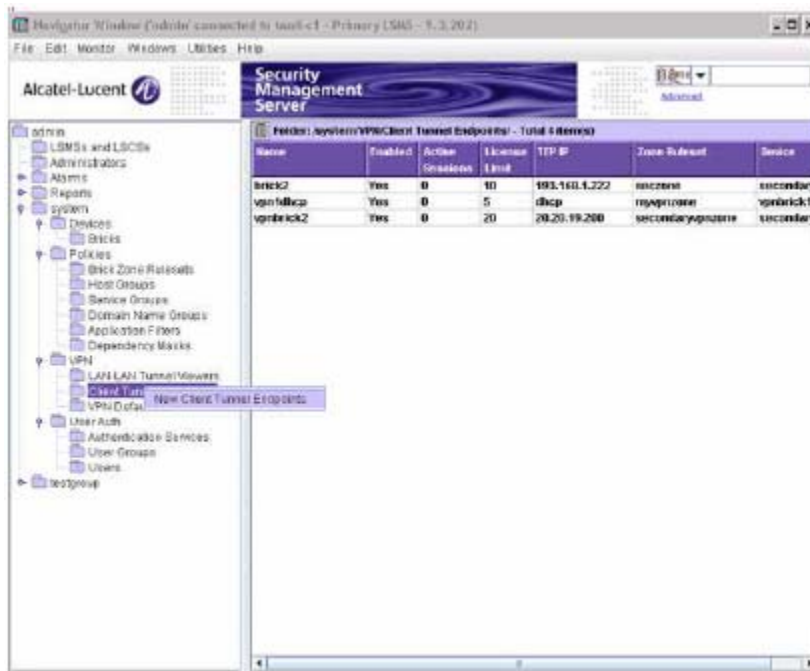
END OF STEPS

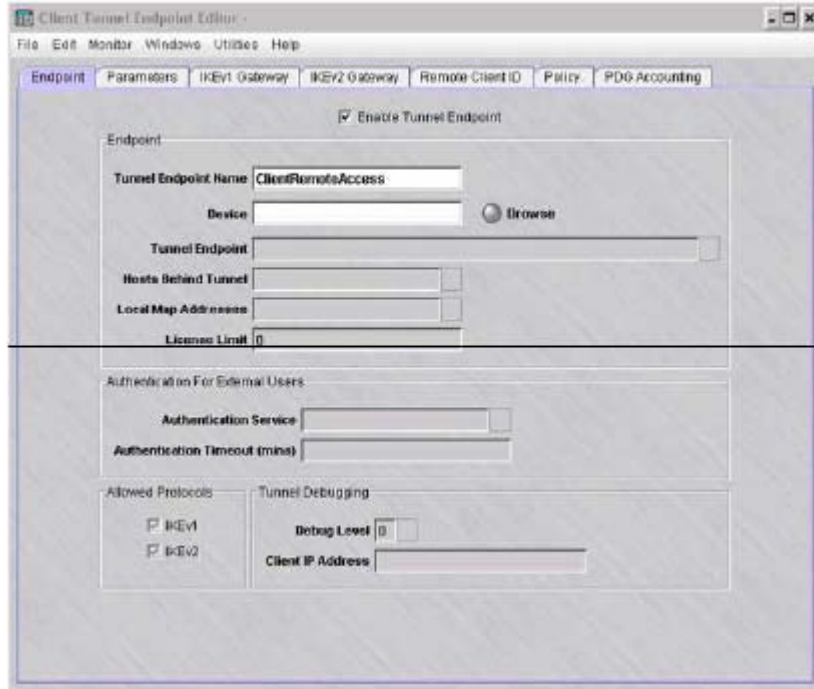
Configuring the Client Tunnel Policy

Task

Complete the following steps;

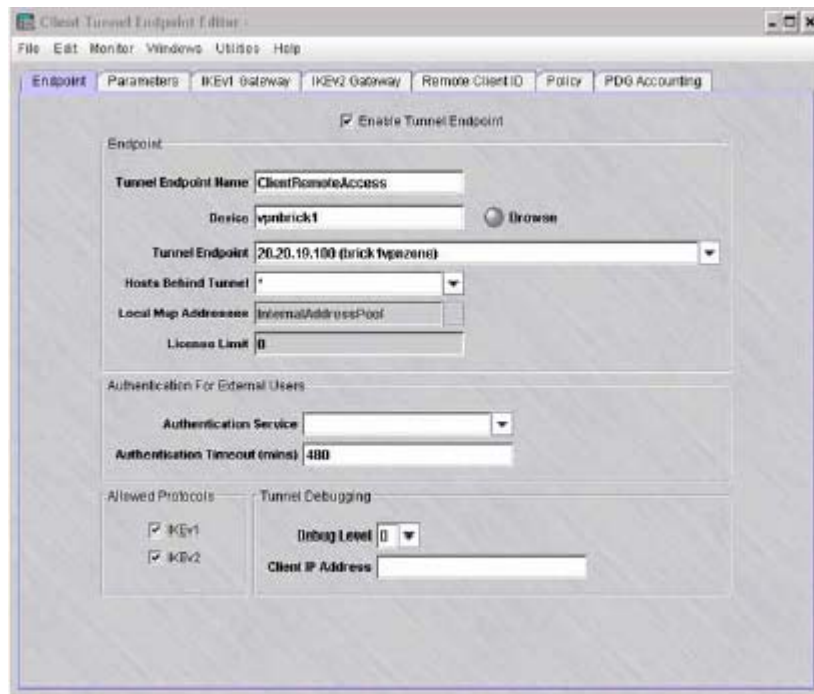
- 1 Choose **SMS Navigator->VPN->Client Tunnel Endpoint**, then right-click and select **New Client Tunnel Endpoints**.





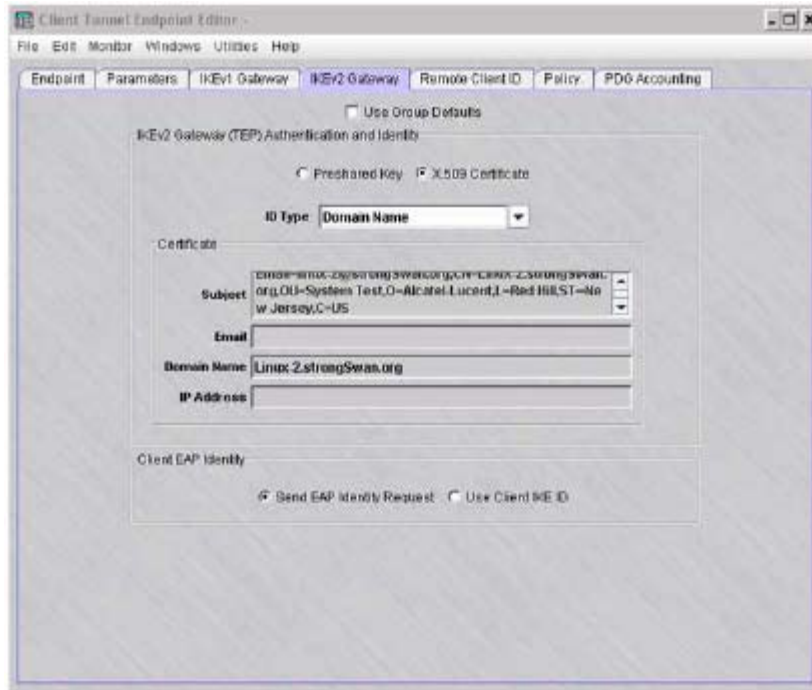
2 Enter a name for the client tunnel endpoint.

Click on **Browse** to select the Brick where you want to create the client tunnel.



3 Select the IKEv2 Gateway tab. De-select the **Use Group Defaults** checkbox. Choose the **X.509 Certificate** radio button.

Click the down arrow next to the **ID Type** field to display a drop-down list, and select the ID type for the Brick to send to the client.

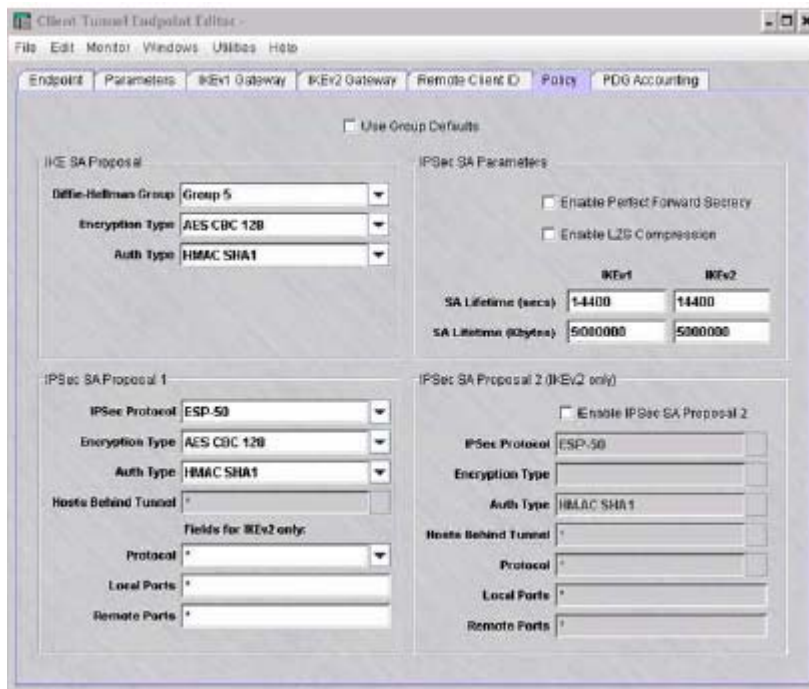


- 4 Click on the Remote ID tab and select **Allow IKEv2 clients to authenticate with x.509 certificates**.

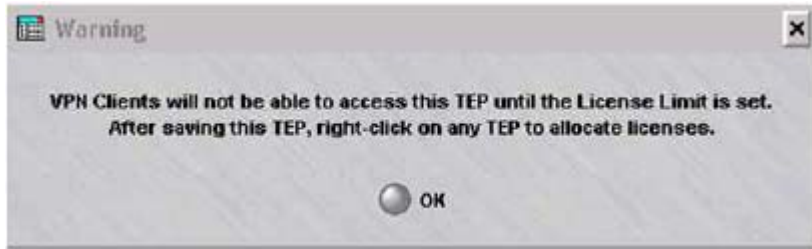
Select the Certificate attribute to use as User ID by choosing **Email Address** or **Domain Name**. This value will be used as the user ID and password for the subject name of the client certificate. The SMS authenticates the Required Attributes with the contents of the client certificate.



5 Configure the required IKE and IPsec policy by clicking on the Policy tab.



6 Click on **File->Save and Apply** to apply and load the updated VPN policy to the Brick.



7 Click on **OK** to dismiss the warning message.

END OF STEPS

Allocating Licenses to the Client Tunnel Endpoint

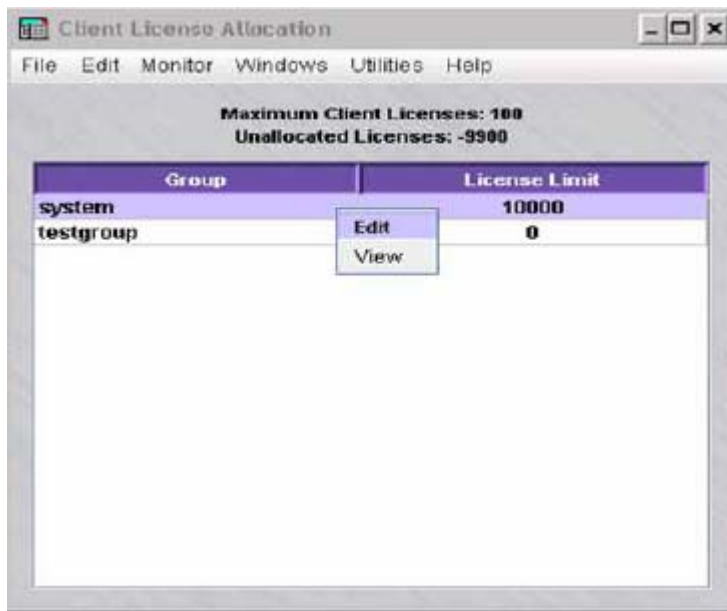
Task

Complete the following steps:

- 1 Go to **SMS Navigator->VPN->Client Tunnel Endpoints**, then right-click and select **Allocate Licenses**.

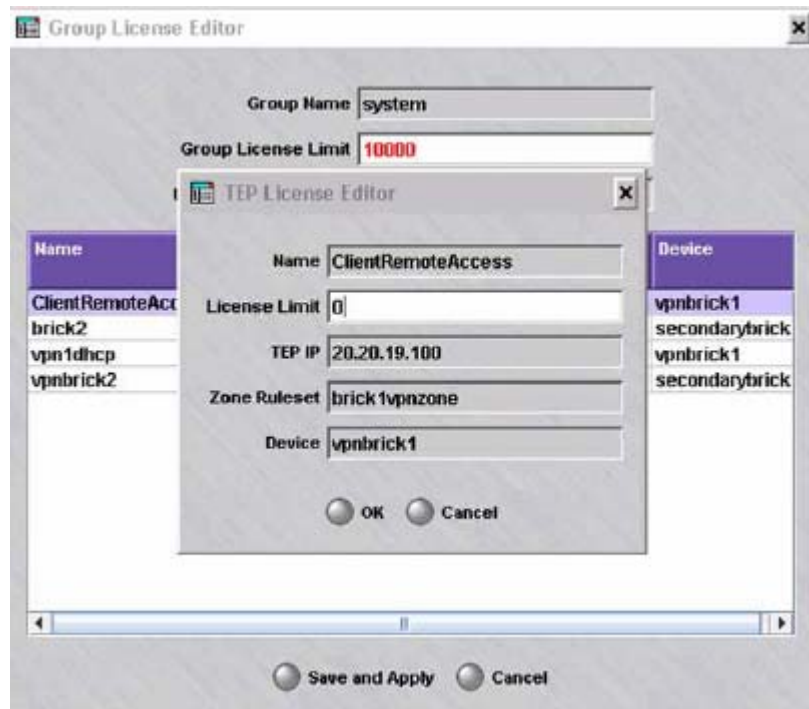


- 2 Right-click on a group and select **Edit** or double-click on the group to enter the license limit for the group.



-
- 3 On the TEP License Editor, allocate the required number of licenses for the client tunnel endpoint.

Click OK and then click **Save and Apply** on the Group License Editor.



END OF STEPS

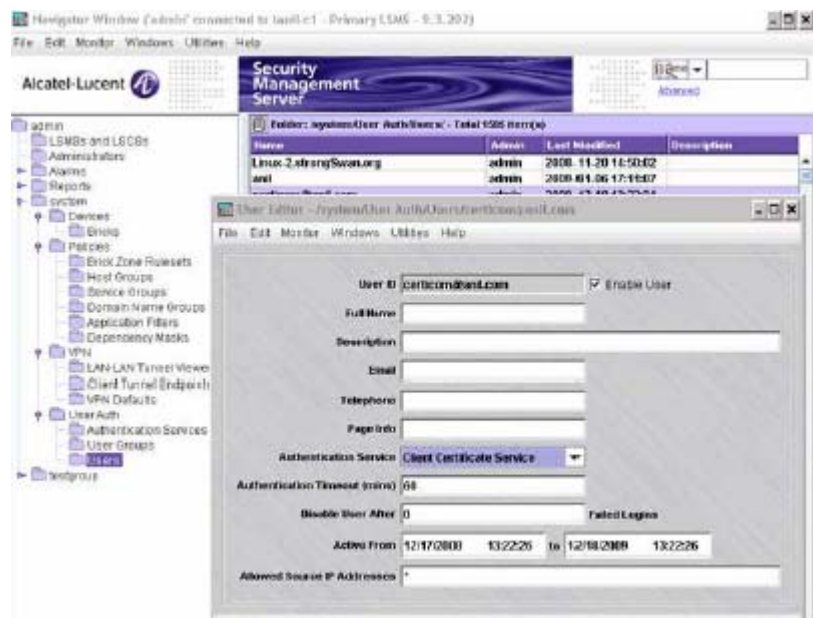
Configuring Users on the SMS

Task

Complete the following steps:

- 1 Go to **SMS Navigator->User Auth->Users**, then right-click and select **New User**.
- 2 Enter the user name, select the Authentication Service from the drop-down list, and enter other parameters.

Note: the Brick uses the remote ID field as the User ID and sends it to the SMS for authentication. When configuring the user on the SMS, make sure that the client is using the configured attribute, in other words, the subjectAlternateName (email/domain name) defined in the certificate, and that the client sends this ID.



- 3 Click on **File->Save and Close** to create the new user.

END OF STEPS

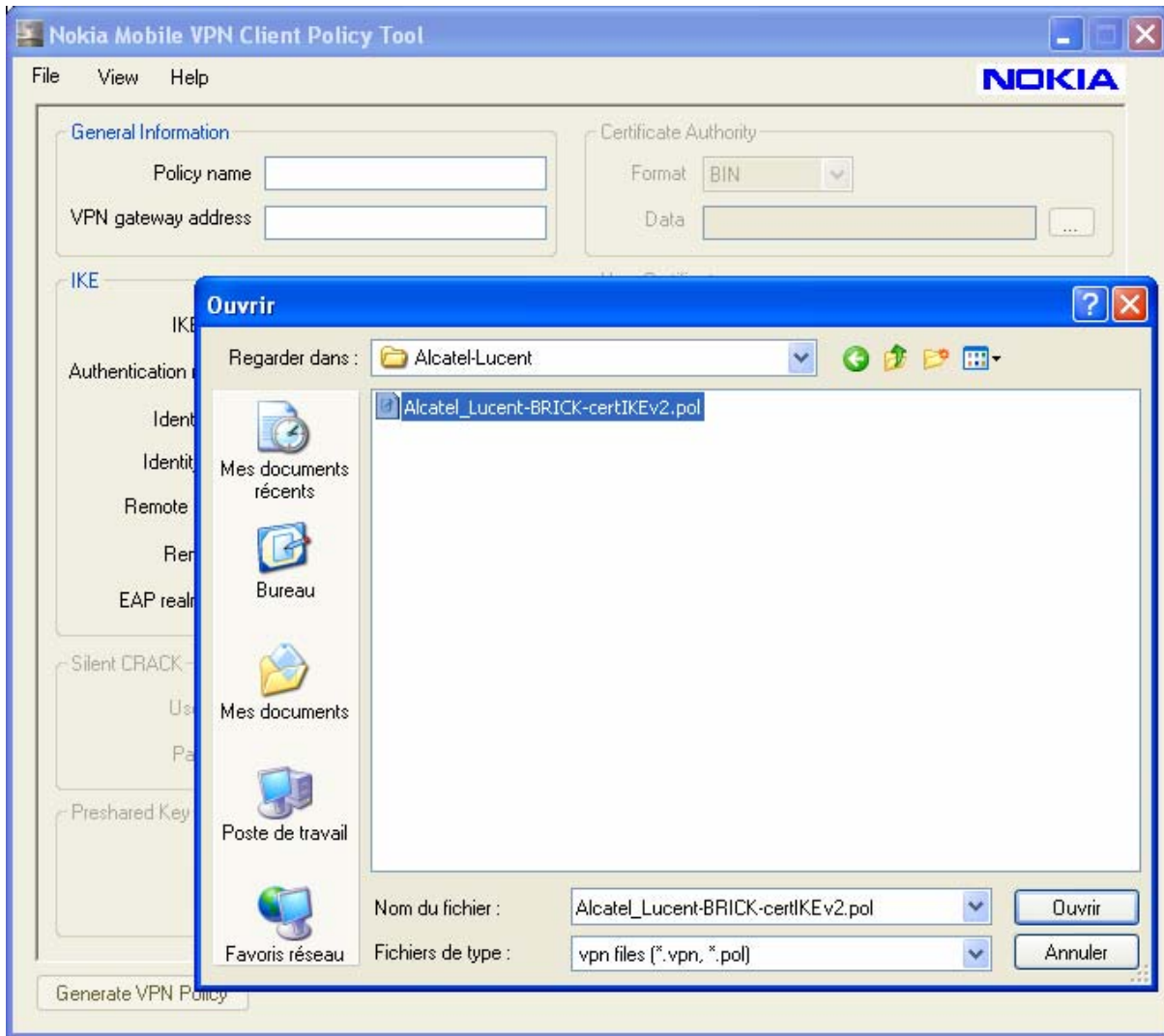
3 Nokia mVPN Client configuration

Policy creation with Policy Tool using exported CA certificate

Before the Nokia Mobile VPN Client policy can be created, a device certificate and CA certificate for Nokia Mobile VPN Client must be available.

In this example, the PKCS#12 packet is used to deliver the device certificate, and the CA certificate is delivered separately in its own file.

Start Nokia VPN Client Policy Tool and press the Load Template button. Select the Alcatel_Lucent-BRICK-certIKEv2.pol policy from the Alcatel-Lucent directory.



Add the proper VPN gateway address and get path to the CA certificate (if the CA certificate is in the PKCS#12 packet, then the automatically generated path should be left as is). Make sure that the “Format in Certificate Authority” selection is set to BIN. Do the same for the PKCS#12 packet. If silent authentication is desired (the PIN code for the certificate is not requested), it needs to be activated from Advanced View. Go to Advanced View, open the IKE tree, and select “Cert store” to be DEVICE instead of USER. Note that only selected S60 3rd Edition, Feature Pack 1 devices support

Device store. See the release note (<http://www.nokiaforbusiness.com/> > Security products > Nokia Mobile VPN > Resources) for more information.

Add the Remote ID type and value that is configured as the Subject Alt Name of the Brick VPN gateway certificate.

Export the VPN policy by pressing the Generate VPN Policy button. Store Alcatel-Lucent.vpn to your PC. For more information on how to install a given policy file to your device, see the Nokia Mobile VPN Client User’s Guide ,Chapter 6.1.

