

Certificate Manager Configuration Guide

Version 1.1

Author: Dave Bousfield
Date: October 11, 1999
Purpose: To describe how to configure Certificate Manager, LDAP Server, and the Account Management GUI. Once configured, this document shows how to create a VPN between SecuRemote and VPN-1 using the PKI strong authentication.

© 1999 Check Point Software Technologies LTD.

Installing and Configuring FW-1 with Certificate Manager

The goal of this document is to guide you through the installation and configuration of the CM v1.0 product, as well as the configuration of FW-1 v4.1 and SecuRemote, so an ISAKMP VPN can be established from a SecuRemote client to FW-1 using digital certificates.

The Certificate Manager product is a bundle of the Account Management Client, Netscape LDAP server, and a “trimmed down” version of the Entrust Certificate Manager.

This document is divided into the following sections:

- **Installation of CM components (AMC, LDAP server and CA)**
- **FW-1 configuration**
- **Configuring the Rule Base**
- **Creating a FW-1 LDAP user and certificate**
- **Creating a SecuRemote LDAP user and certificate**
- **Configuring SecuRemote client and installing certificate**

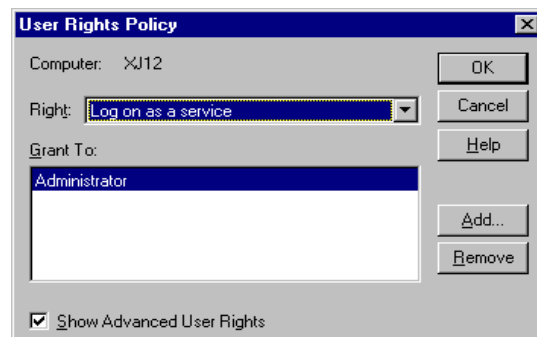
Things to do Before Installation:

- 1) You must install Netscape Navigator version 4.04 or higher before installing VPN-1 Certificate Manager.
- 2) You must install VPN-1 Certificate Manager as a user with Administrative privileges. This user must also be given “**Log as a service**” rights, as follows: Bring up the **User Manager for Domains**. From the Users manager, select **Policies/Users Rights**. Click the box for **Show Advanced User Rights**. Now click on the scroll down bar labeled **Right**. Select **Log as a Service**. If **administrator** is not listed in the **Grant to** field, add it. After you have done this you must **reboot the system** for these settings to take effect.

Note – You must make your changes at the User Manager for Domains Submenu. Otherwise the Entrust CA component won’t be installed and you will receive an error message regarding a problem with log on as a service.

Note – You must add the individual user. Giving “Log in as service” rights to a user group does not work.

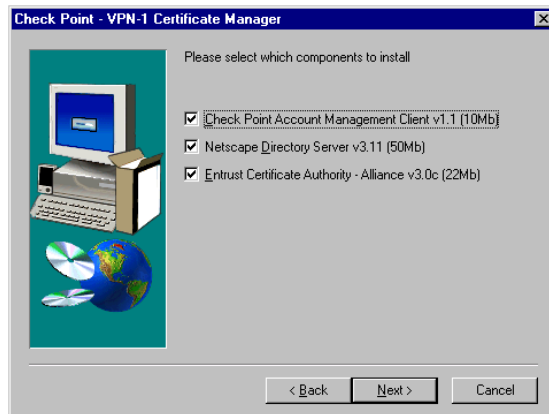
Note -If an earlier version of the CM was installed, remove it by uninstalling it. If any directories related to CM have been left after the installation, remove them manually before reinstalling.



Note –If using a domain controller, it is not enough that the administrator is defined on the domain, but on the specific machine. Moreover the “logon as service” should be granted to the local administrator.

Installing AM, LDAP Server, and CA:

- 1) Insert the CD-ROM, open NT Explorer and double-click on setup.exe. The Install Shield will walk you through the installation of the AM, LDAP and CA components. Select all three components to install.



Note –This option of installing all Certificate Managers’ three components is just a recommendation. Users who familiar with the CM product can install all components on one machine or can install each component on separate machine. This document describes the installation of all three-CM components on one machine.

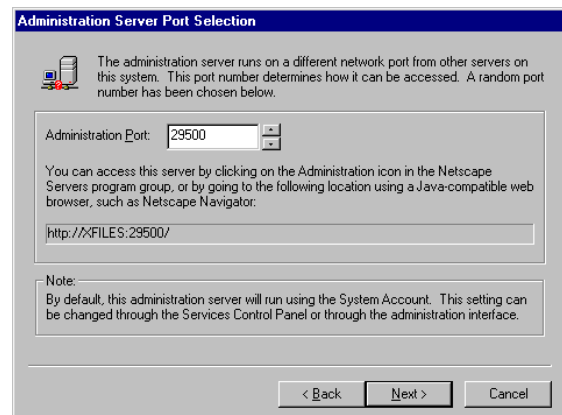
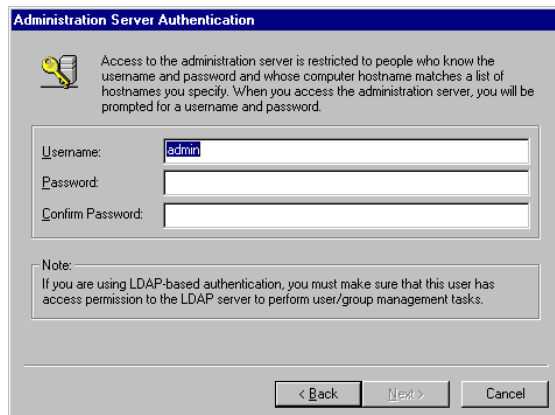
Note -If for some reason each component does not install properly, you will need to uninstall each one and start over. Uninstalling doesn’t remove all of the directories created by the install script so make sure to delete them before reinstalling.

AM Client Installation:

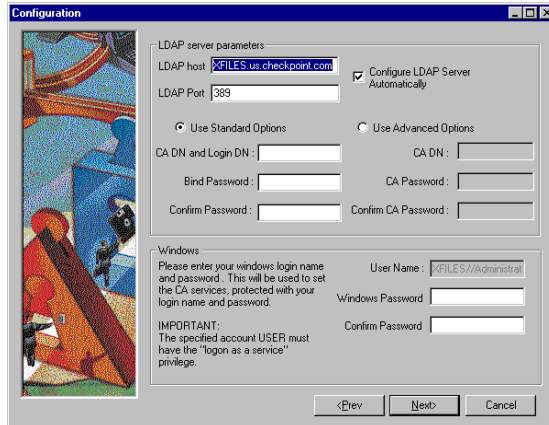
- 2) This is the first component that gets installed and it should install without prompts.

LDAP Server Installation:

- 3) The first prompt will be for the LDAP server Administrator **Username** and **Password**. Do not change the username! Leave it set to admin.
- 4) Choose any port you want for the administration server to bind to or accept the random port number chosen.

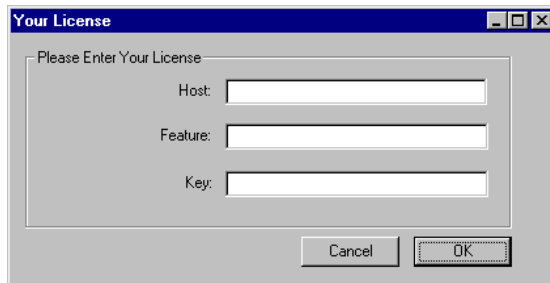


- 5) Leave the **LDAP Port - 389**, which is the standard, Well Known Port for LDAP. Select **Use Standard Options** and enter the **CA DN and Login DN: o=ABCcorp,c=US**. The DN must be of type o=(organization) or ou=(organizational unit). **Bind Password: Abc12345**. The password must be 8 or more characters with mixed case and at least one number. The CA login and LDAP Server administration login will use the same DN and password. **Windows Password: (the NT Administrator password.)** This will be used to set the Entrust services and authenticate them. Press Next and the installation program will generate all the needed files for the LDAP server using o=ABCcorp,c=US.



Certificate Authority Installation:

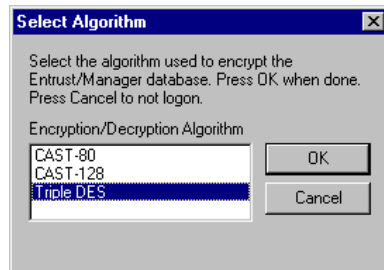
- 6) Next, the Entrust component will start up and immediately ask for a CheckPoint License. **Enter your license** or take your certificate to <http://license.checkpoint.com> to obtain one. Press OK and the Entrust component will be installed, and the Install Shield program will finish.



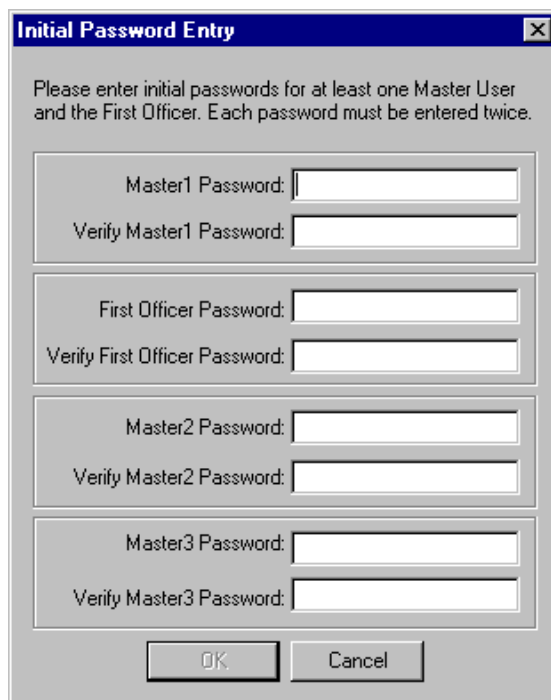
- 7) Press **Finish** to **Launch Certificate Authority Now**. The Entrust/Master Control GUI can also be started from the Check Point VPN Certificate Manager program group, by selecting the Entrust/Master control and pressing the Logon button.



- 8) First, select an encryption algorithm – **Triple DES**.

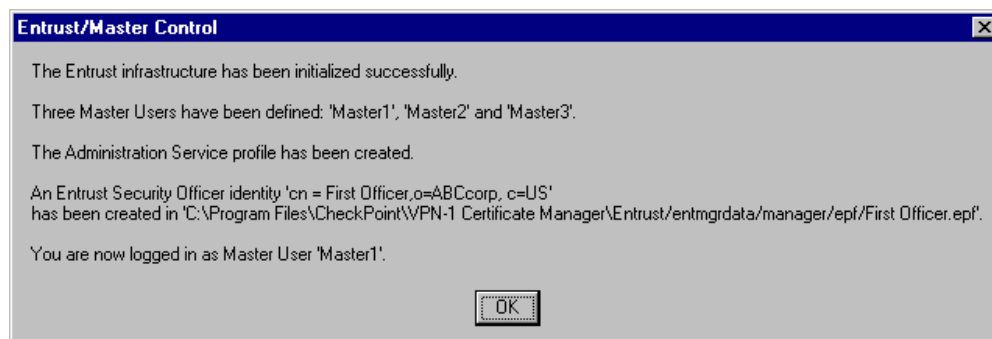


- 9) Now you must supply at least the **Master1 password** and the **First Officer password**. The Master1 user has authority to control the Entrust service. The First Officer user has authority to logon to the Account Unit from the Check Point Account Management Client. **Master1 – Abc12345, First Officer – Def12345**. The password must be mixed case with 8 or more characters and at least one number.



- 10) If everything worked, you should get a message window, notifying that the Entrust Infrastructure has been successfully initialized.

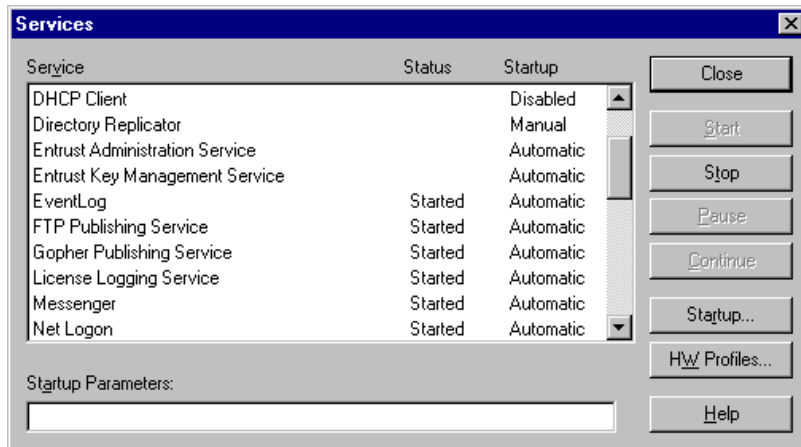
Note – It is recommended to make a backup of the database after the initialization is successfully done.



- 11) Now you need to start the Entrust service. Click on the **Services** menu item from the **Entrust/Master control**. Choose **Start Administrator**.



- 12) Remember to go to the **Services** manager from the **NT control panel** and set the startup for the two Entrust services to automatic so you don't have to do this step anymore. Remember that the password that it will ask for is the NT Administrator account for this system.

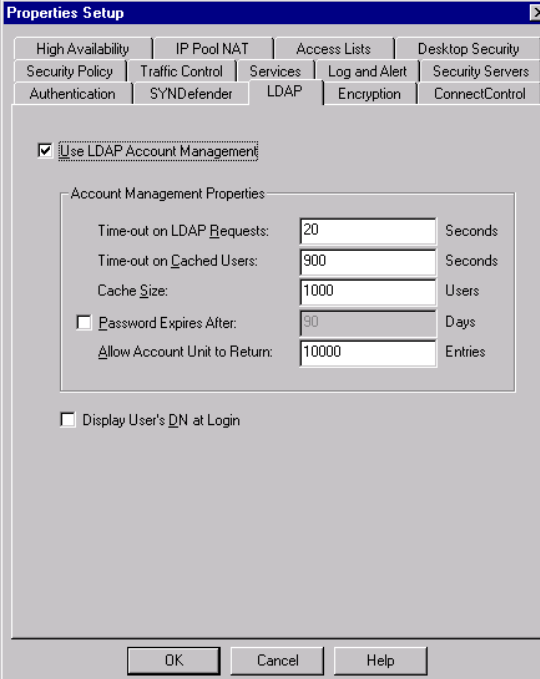


Making it all work together:

The following steps will cover the configuration of all components so they will work together. All modules should now be installed and running.

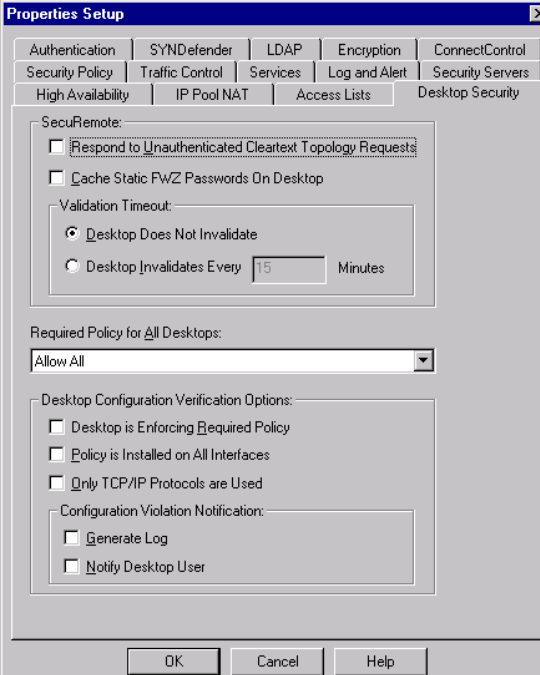
FW-1 V4.1 Configuration:

- 13) Insert the CM CD into your firewall system and install the AMC v1.1 on the firewall. (This component is actually installed on the Management Server if they are separate.) Log into the policy editor. Go to **Policy->Properties**, select the **LDAP** tab, and enable **Use LDAP Account Management**.



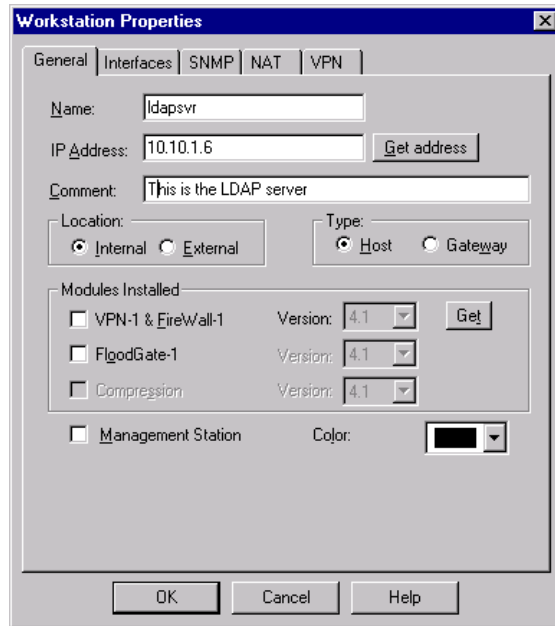
The screenshot shows the 'Properties Setup' dialog box with the 'LDAP' tab selected. The 'Use LDAP Account Management' checkbox is checked. Below it, the 'Account Management Properties' section contains several fields: 'Time-out on LDAP Requests' (20 Seconds), 'Time-out on Cached Users' (900 Seconds), 'Cache Size' (1000 Users), 'Password Expires After' (90 Days, unchecked), and 'Allow Account Unit to Return' (10000 Entries). There is also an unchecked checkbox for 'Display User's DN at Login'. The dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.

- 14) Select **Desktop Security** and verify that **Respond to Unauthenticated Cleartext Topology Requests** is not enabled.



The screenshot shows the 'Properties Setup' dialog box with the 'Desktop Security' tab selected. The 'SecuRemote' section has the 'Respond to Unauthenticated Cleartext Topology Requests' checkbox unchecked. Other options include 'Cache Static FWZ Passwords On Desktop' (unchecked), 'Validation Timeout' (radio buttons for 'Desktop Does Not Invalidate' selected and 'Desktop Invalidates Every 15 Minutes'), 'Required Policy for All Desktops' (set to 'Allow All'), and 'Desktop Configuration Verification Options' (all unchecked). There is also a 'Configuration Violation Notification' section with 'Generate Log' and 'Notify Desktop User' checkboxes unchecked. The dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.

15) Go to **Manage->Network objects**, and create a new **host** object for the LDAP server (**ldapsvr**).



16) Select **Manage->Servers**, and create a new **LDAP Account Unit**.

Name: ldap_account_unit,

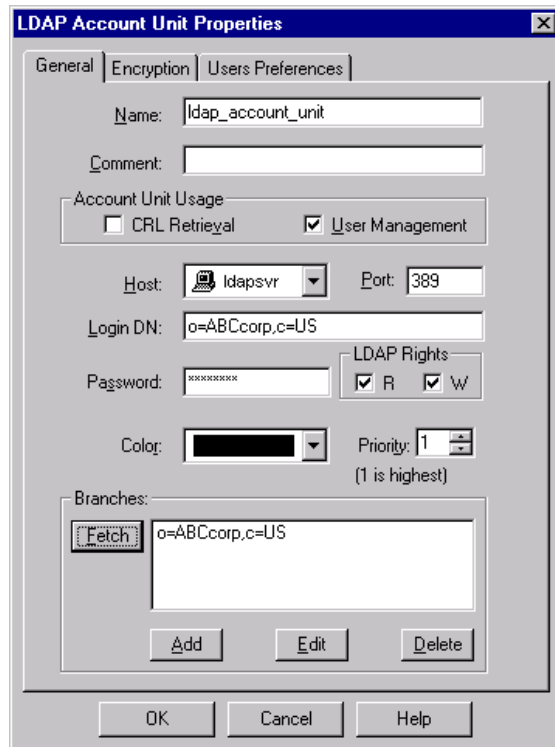
Host: ldapsvr

Port: 389

Login DN: o=ABCcorp,c=US

Password: (LDAP bind password) **Abc12345**

Press the **fetch** button to make sure that the firewall can talk to the LDAP server. Press **Ok** to save.



17) Edit the **hosts** file on the firewall system and verify that there is an entry for **ldapsvr**.

18) Test the ability for FW-1 to access the LDAP server. From the Policy Editor, select **Manage->Users on Account Unit** from the toolbar, select your LDAP server in the window, and click on **Manage**. You must be able to log into the LDAP server. If you can't log in, check the LDAP Account Unit Properties and passwords that you used. You must get this to work, before FireWall-1 can authenticate using the LDAP Directory Server. Once you are successfully logged in, notice that you can't manage the CA keys! To manage the CA keys remotely, you will have to define and login to the LDAP server from the AMC outside of the Firewall User Interface.

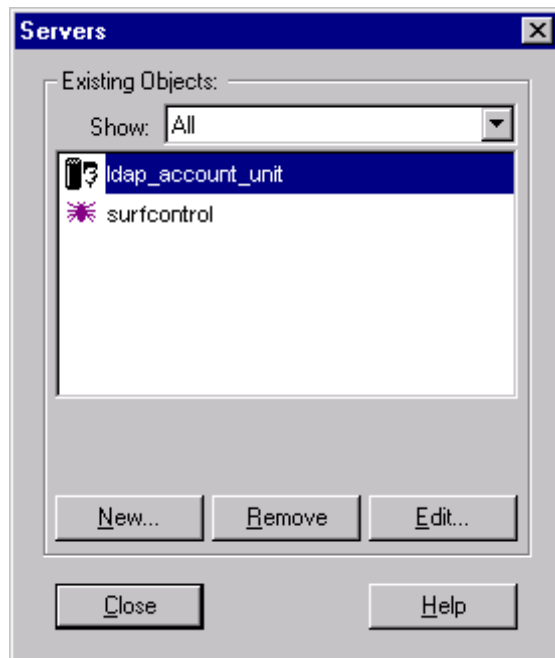
Note – all remote changes are stored on the main server and your system. I suggest that you setup a share for all remote administrators to store any changes to.

19) To test that the LDAP is working properly – create a user that uses **FireWall-1 (internal) Password**. Test with User authentication. If it is successful, go to the next step. If not – troubleshoot the network connections (most common problem).

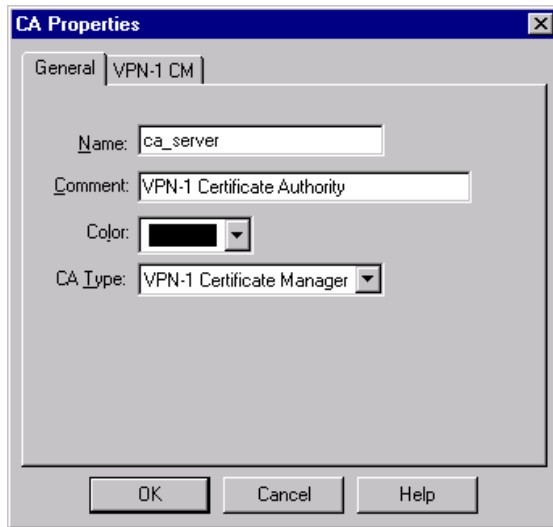
he **edit** button. In the **ISAKMP properties**, click on the **Public Key Signatures** box, and select the **configure** button. Now make sure that the **DN** checkbox is turned on and press the **Generate Key** button.

Creating a FW-1 V4.1 LDAP user and certificate:

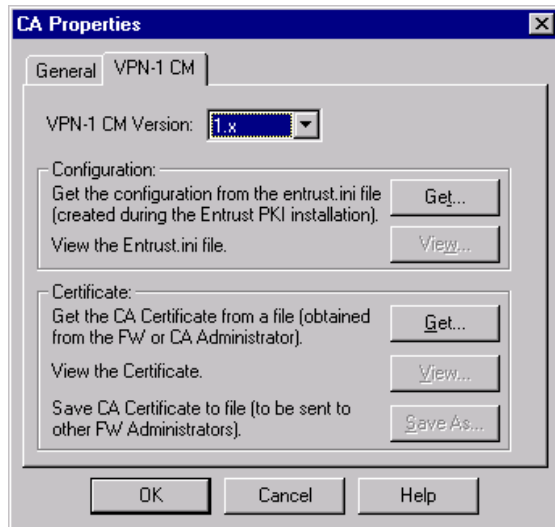
20) Define the Certificate Authority by selecting **Manage->Servers**. Click on **New** and select **CA**.



- 21) Select the **General** tab of the **CA Properties** window and fill in the **Name** of the CA, for this example the CA has been named CA_Server. Specify the **CA Type** as VPN-1 Certificate Manager 1.0. Don't close this window yet.



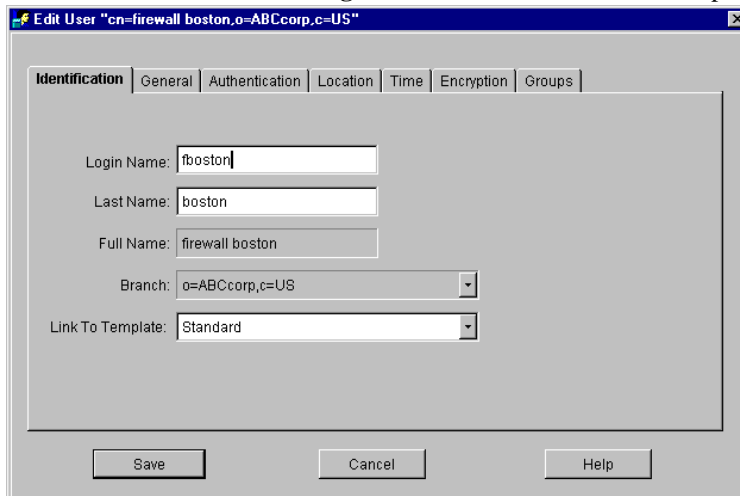
- 22) Select the **VPN-1 CM** tab and press the **Get** button, under Configuration, to get the entrust.ini file. The entrust.ini file specifies the location and other parameters of an Entrust CA. You can browse for the entrust.ini file. *Note -There is no need to explicitly obtain the CA's own certificate – it will be obtained as a by—product of generating other certificates.*



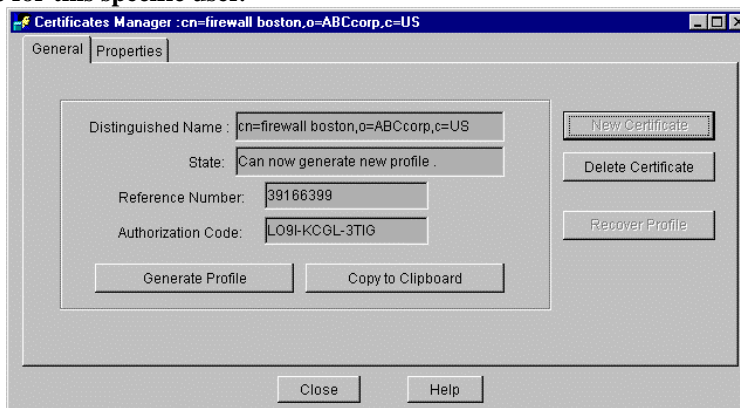
- 23) An LDAP user profile must be created for FW-1 before a certificate can be generated. The process of creating a new LDAP user is performed with the AM Client GUI. Start the AM Client GUI on the CA server and enter the **Password** for the First Officer account (**Def12345**).



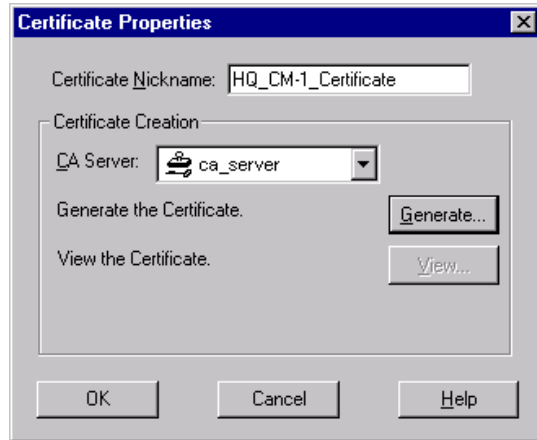
- 24) Select **File->New User**. Fill in the **Login Name** and the **Full Name** and press **Save**.



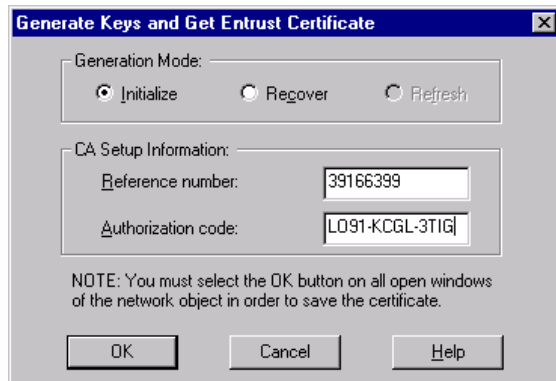
- 25) In the AMC toolbar, you will have two certificate icons. One is for managing the Certificates and the other is the Certificate properties. Highlight your new user, and select the **Certificate properties**. Once in the **certificate properties**, select **create a new certificate**. The AMC will then ask for an **expiration date**, press **ok**. On the next screen you will have the **Reference Number** and **Authorization Code**. Write these down, but don't quit this window. Moreover, do not generate a profile for this specific user.



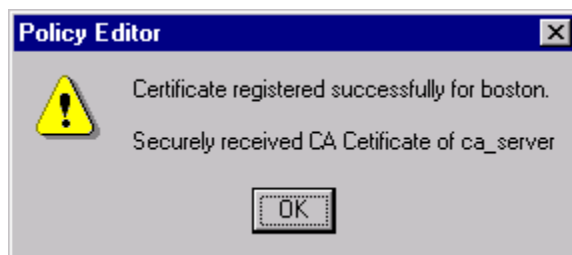
- 26) From the Policy Editor, select **Manage->Network Objects**. **Edit** the FW-1 object and select the **Certificates** tab of the FW-1 object **Workstation Properties** window. Click on **Add** to open the **Certificate Properties** window. Specify a **Certificate Nickname** (HQ_CM-1_Certificate) that will remind you of which CA this certificate is from. You must specify a nickname for each certificate because a FW-1 module can have more than one certificate. Select the **CA Server** in the pull down box. Click on **Generate**.



- 27) In the **Generate Keys and Get Entrust Certificate** window, select **Initialize** to generate a new certificate. Enter the Reference Number and Authorization Code that were generated earlier with the AM GUI. Click on **OK**.

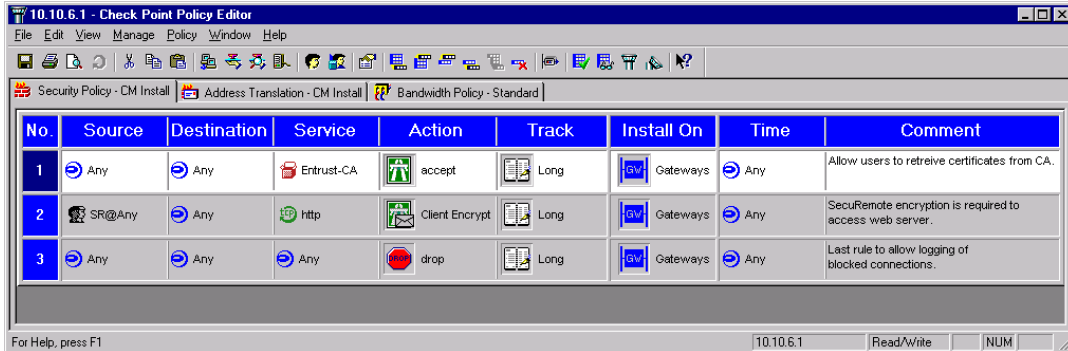


- 28) If everything worked you should get the following message. The FW-1 certificate is generated and saved in the Management Station's database. The certificate can be viewed by clicking on **View** in the **Certificate Properties** window. In addition, the CA's own certificate can be viewed by clicking on **View** in the **VPN-1 CM** tab of the **CA Properties** window.



Configuring the RuleBase:

- 29) If the CA/LDAP server is behind a firewall, create a rule to allow the Entrust_CA service and FW1_key. This rule should precede the encryption rule of the SecuRemote Client to the Encryption Domain. You should have created an External user group to test your earlier LDAP settings. Use this to create your rules. Install the policy.

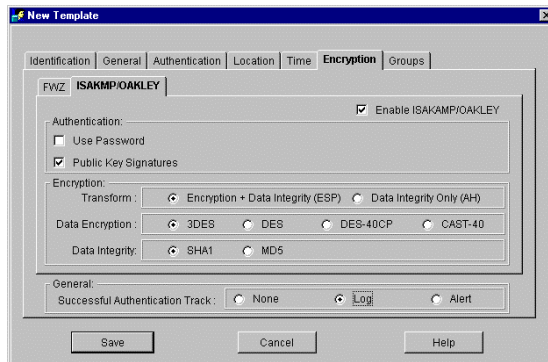


Creating a new SecuRemote user and certificate

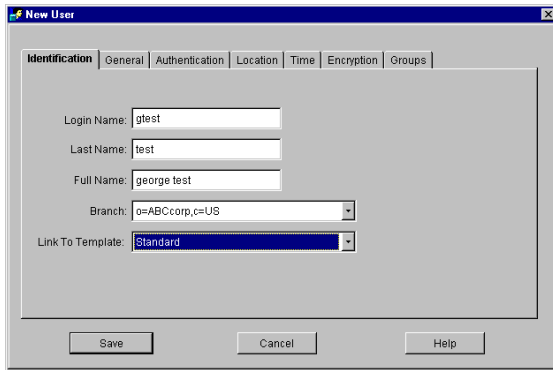
- 30) The process of creating a new user on the LDAP server is performed with the AM client GUI. The AMC GUI allows you to manage the LDAP server, including the Check Point and Entrust directory attributes and object class definitions. Start the AM client GUI on the CA server and enter the Password for the First Officer account (**Def12345**).



- 31) Modify the default user template, or create a new one, to simplify the creation of multiple users. Select the Encryption tab and enable ISAKMP/OAKLEY, Public Key Signatures, and Data Encryption method desired. These are the only required changes to enable SecuRemote users to use ISAKMP with PKI authentication.

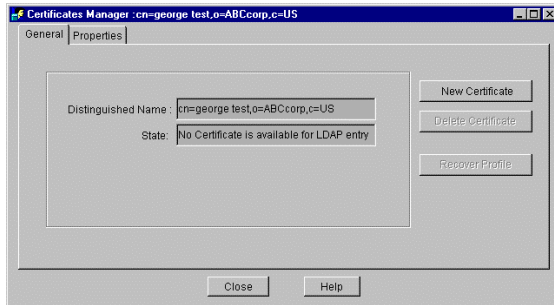


32) Create a new user named gtest and select the Standard template. Save your changes.

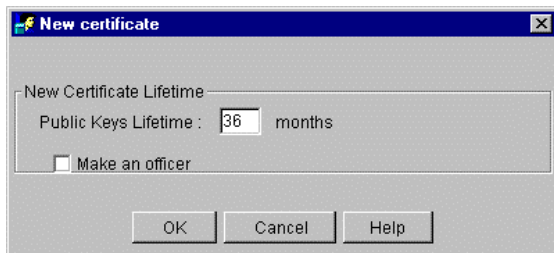


There are two ways to generate digital certificates. Generate a .epf file or generate a Ref and Auth #.

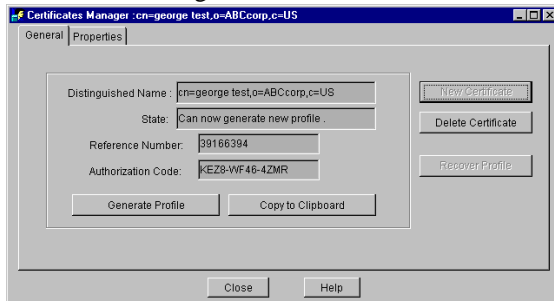
33) After defining the user's properties you should create a **certificate** or a **profile file** (.epf) for the user. For this example we'll create a certificate and use the Reference Number and Authentication code. Select certificate from the Edit menu. On the General tab click on New Certificate button.



34) The AMC will then ask for the New Certificate Lifetime, **press ok**.



35) On the next screen you will have **the Reference Number** and the **authentication code**. Generate the **user profile** by clicking on Generate Profile. Before generating, you should enter the password for using the certificate and specify the name of the profile file. After successfully generating the profile, the state box would change to **“Has an Active Certificate”**.



Configuring the SecuRemote client and installing the certificate:

This version of VPN-1 CM is compatible with FW-1 version 4.1 and SecuRemote versions 4.0 and higher.

Before we install SecuRemote on the client system, go to the LDAP server and set up a **user account**.

Login name: **johns**

Full name: **John Smith**

Authentication – **Internal (FW1) password: abc123**

Encryption: **Deselect FWZ, Select ISAKMP and select Public Key Signatures.**

Now go to the Client and install SecuRemote. When you are back in the System bring up the **sites manager interface** for SecuRemote. Click on the **Add a new Site** button and create the FireWall system.

From the menu items ,choose **Entrust**. Click on the **configure entrust.ini** item:

CA manager:**CA server IP port number (709)**

LDAP server:**LDAP servers IP port number (389)**

Note that if CA/LDAP server's IP address is translated,put the valid IP address in the above information.

Next select **Create a User** from the **Entrust** menu item.

Profile: *use the browse button to save the information locally c:\winnt\John Smith. The profile name is case sensitive to the LDAP server.*

User password: **(This is a local password to protect the certificate stored on the client)**

Reference Number: **From the CA/LDAP server**

Authorization Code: **From the CA/LDAP server**

The SecuRemote client should now successfully create a new certificate. If so, go back to the LDAP server and save the new certificate. If not, check your network connections.

Notice that you have created a profile file (John Smith.epf) which resides in the SecuRemote local machine. There is indeed a "local" way to obtain this file:

Go to the LDAP server and find the profile file (.epf) for your SecuRemote user.

It should be resided in Program Files/CheckPoint/VPN-1 Certificate Manager/Account Management.

Remember that this user has to be defined with ISAKMP encryption and with PKI.

Copy the file to the SecuRemote machine and you are done.

Remember that the password to be inserted in the SecuRemote user authentication window is the Profile password which was defined in the LDAP server prior to the profile generation.

Now you are ready to test.

Test the SecuRemote session. When SecuRemote asks for the authentication:

Click the **use certificate box**, and use the **browse** button to find your profile. In the password field type the password that you entered with the Reference Number and Authorization Code. If everything is set up properly, it should take about 5-10 seconds to generate the keys (*this depends on network speeds*). If everything works, you are done.