

# Table of Contents

<b><u>Configuring an Entrust Certificate Server for Use With the VPN 5000 Concentrator and VPN 5000 Client Connections</u></b> .....	<b>1</b>
<u>Document ID: 17950</u> .....	1
<u>Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, refer to the End-of-Sales Announcement</u> .....	1
<u>Introduction</u> .....	1
<u>Prerequisites</u> .....	1
<u>Requirements</u> .....	1
<u>Components Used</u> .....	2
<u>Conventions</u> .....	2
<u>Install and Configure for Certificates</u> .....	2
<u>VPN 5000 Certificate Request and Certificate Installation</u> .....	2
<u>Set Up Users on the Entrust Certificate Server</u> .....	7
<u>Install Entrust/Entelligence and Configure the VPN Client to Use Entrust Certificates</u> .....	13
<u>Verify</u> .....	14
<u>Troubleshoot</u> .....	15
<u>Troubleshooting Commands</u> .....	16
<u>NetPro Discussion Forums – Featured Conversations</u> .....	16
<u>Related Information</u> .....	16

# Configuring an Entrust Certificate Server for Use With the VPN 5000 Concentrator and VPN 5000 Client Connections

Document ID: 17950

---

**Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, refer to the End-of-Sales Announcement.**

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### Install and Configure for Certificates

- VPN 5000 Certificate Request and Certificate Installation
- Set Up Users on the Entrust Certificate Server
- Install Entrust/Entelligence and Configure the VPN Client to Use Entrust Certificates

### Verify

### Troubleshoot

- Troubleshooting Commands

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

This document describes how to configure an Entrust Certificate Server for use with Cisco VPN 5000 Client and Concentrator. Cisco Systems does not endorse any one particular certificate server.

## Prerequisites

### Requirements

Before you attempt this configuration, ensure that you meet these requirements:

- The **certificate request** and **certificate import** commands need to be run through console access to the VPN 5000 Concentrator. A Telnet connection can produce undesirable results.
- System time is very important when you deal with certificates. If the VPN 5000 Concentrator does not have a time server configured, the administrator must set the time manually with the **sys clock mm/dd/yy hh:mm** command. A **sys clock** time adjustment is not permanent across reboots of the VPN 5000 Concentrator.
- Before the VPN 5000 Concentrator can accept VPN Client connections from Entrust-capable clients, the address of the Lightweight Directory Access Protocol (LDAP) server that contains the certificate revocation list (CRL) must be configured in the Certificates section on the VPN 5000 Concentrator.

## Components Used

The information in this document is based on the Cisco VPN 5000 Concentrator.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Install and Configure for Certificates

### VPN 5000 Certificate Request and Certificate Installation

Follow this procedure.

1. Issue the **certificate generate request** command on the VPN 5000 Concentrator.

Type **certificate generate request ?** in order to see available options. The VPN Concentrator takes a few moments to generate the request and the length of time depends on key length. The **show certificate generator** command displays the status of the request generation. If you are logged into the console, the "Certificate request is ready" message appears when the generation is complete.

This output shows an example.

```
VPN5000: Main# certificate generate request ?

request command information:
  REquest                Generate a certificate request

Usage: request <key length> [ locality <city>] [ state <state>]
      [country <country code>] [ organization <organization name> ]
      [ commonname <common name> ]

VPN5000: Main# certificate generate request 1024 locality
Anytown State CO
country US organization CompanyA commonname Marketing
Generate Certificate Request

VPN5000: Main# show certificate generator
Certificate generator busy

VPN5000: Main# Certificate request is ready
```

2. Run the **certificate request show** command in order to display the certificate request.

Copy the entire certificate request into a text editor, and make sure to include the carriage after the last line. Save the file and FTP it to the Entrust server.

This output shows an example.

```
VPN5000: Main# certificate request show
-----BEGIN CERTIFICATE REQUEST-----
MIIBkjCB/AIBADBTMRAwDgYDVQQHEwdBbnl10b3duMQswCQYDVQQIEwJDTzELMAkG
```

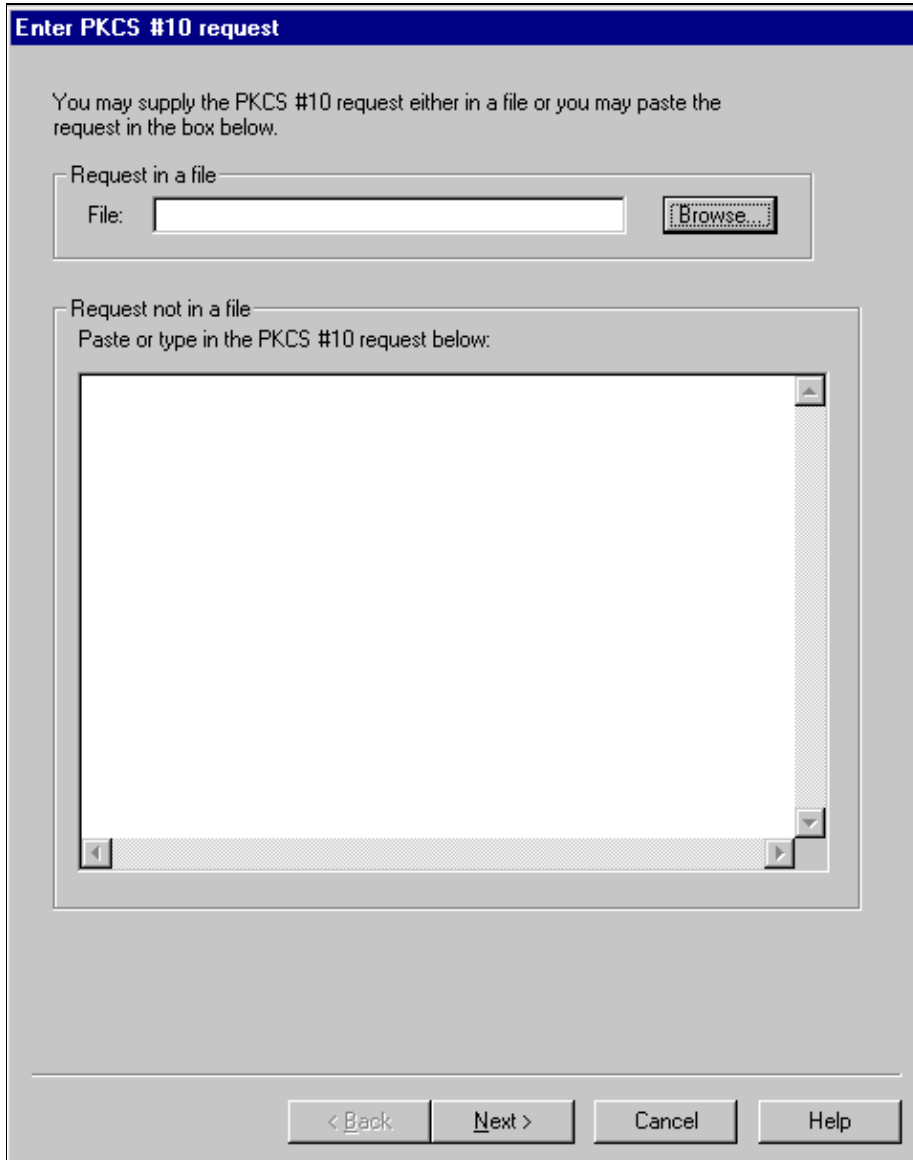
```

A1UEBhMCVVMxETAPBgNVBAoTCENvbXBhbnlBMRlWEAYDVQQDEw1NYXJrZXRpbmcw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALkYmd01ZvBXuwcYh0DFTvt9brkZ
SijN8JCMKJfkmNmxic5dcLEEEjBVoVd0LypA3LzYg3UMtdwDY5s504jfkjgwXB
A7JjEfzmzTJ9tPgQX3/0hdH4P0FWThuMczcEB1Eju2xNIj7xXyDgTQKiD15ZV8xWJ
4DX6eOkF5uRXYcCVAgMBAAGgADANBgkqhkiG9w0BAQQFAAQBQAAVf8dbYjQy5CH
54/sYuovOv3nzcQLGoc9dWoh3pj04e/TPFaZT1C3J1rLvMYT/wqrNxMxLGtd0KgD
EZeRjXs4qAdpzn5ELhUALmsLLyrWbcIF06Dgu/zUEahXkLYZA/mfkkIVnrJ8CEg
ZUsp71Bb4zfbrICJt7fk+74ywkoq/w==
-----END CERTIFICATE REQUEST-----
VPN5000: Main#

```

3. Log into the Entrust VPN Connector.

Click the **Request** menu selection and choose **Read PKCS #10**. In the Request in a file field, click **Browse** and navigate to the location where the certificate request is stored.



4. Double-click on the desired file, which opens the PKCS #10 Request Information window, as shown in this image.

Accept the default value for the **Use this searchbase** field, but specify the path for the certificate output in the **Save the output to** field. Check the boxes for **Wrap the output with PKCS-7** and **Include CA Certificates in PKCS-7 wrap**. When you check these boxes, it tells the Entrust VPN

Connector to produce a PKCS #7 structure that contains both the root and server certificate. Click **Finish** when you are done.

The screenshot shows the 'PKCS #10 Request Information' dialog box. It is divided into three main sections: 'Contents', 'Fingerprints', and 'When processing this request'.  
- **Contents:** Includes text boxes for 'Searchbase', 'Common name' (containing 'Marketing'), 'Serial number', 'Description', and 'Subject alternate names'.  
- **Fingerprints:** Shows 'MD5' and 'SHA1' hashes. The MD5 hash is '58:E0:C8:EC:CC:08:00:8D:DB:4F:18:9D:A6:D3:0B:0C' and the SHA1 hash is 'D8:D5:C9:0B:A5:AC:51:43:D9:D6:FC:2B:37:BD:4C:5E:1E:EE:F6'.  
- **When processing this request:** Features two radio buttons: 'Use the searchbase contained in the request.' (unselected) and 'Use this searchbase' (selected). Below the selected option is a dropdown menu with the text 'ou=crlab,o=cisco,c=US'. There is also a 'Save the output to:' field with the path 'C:\crlab\SampleReq.out' and a 'Browse...' button. Two checkboxes are checked: 'Wrap the output with PKCS-7' and 'Include CA Certificates in PKCS-7 wrap'.  
At the bottom, there are four buttons: '< Back', 'Finish', 'Cancel', and 'Help'.

5. When the Verify Fingerprint window appears, click **Yes** in order to continue.

The screenshot shows the 'Verify Fingerprint' dialog box. It displays the same MD5 and SHA1 hashes as the previous dialog. Below the hashes is a 'Note' box with the following text: 'Please verify one of the above fingerprints with that obtained from the IPsec Device Administrator. If they match, it is a valid request and you may click 'Yes' to continue. Otherwise, click 'No' to cancel the PKCS10 request.' At the bottom, there are two buttons: 'Yes' and 'No'.

- When the VPN Connector window appears and displays the path to the PKCS# structure, click **OK** in order to accept.



- FTP the PKCS# structure to the computer through which you are consoled into the VPN Concentrator.

Remember that the PKCS# structure produced by the Entrust Certificate Server is not in a format that the VPN Concentrator accepts. The VPN Concentrator needs the PKCS# structure in a blocked format with exactly 64 characters per line.

In order to convert to this format, complete these steps with the use of this template:

```
-----BEGIN PKCS7-----
MIIF1QYJKoZIhvcNAQcCoIIIFhJCcBYICAQEExADALBgkqhkiG9w0BBwGgggVqMIIC
-----END PKCS7-----
```

- Paste the PKCS# structure into the template after the first line (do not include the header).
  - Position the cursor at the end of the first line. Press the down arrow so that the cursor is placed on the second line, then press **Enter**. Repeat this step on each subsequent line.
  - Once the entire PKCS# structure is truncated to 64 characters per line, remove the first line of the certificate that was used as the marker.
- Copy the formatted PKCS# structure.

On the VPN Concentrator console, issue the **certificate import** command. When you are prompted, paste the structure into the VPN Concentrator.

This output shows an example.

```
VPN5000: Main# certificate import
Begin Pasting Certificate Now
To terminate input, enter a . on a line all by itself.
-----BEGIN PKCS7-----
MIIF8wYJKoZIhvcNAQcCoIIIF5DCCBeACAQEExADALBgkqhkiG9w0BBwGgggXIMIIC
3DCCAkWgAwIBAgIEOs40bJANBgkqhkiG9w0BAQUFADAtMQswCQYDVQQGEwJVVzEO
MAwGA1UEChMFY2l2Y28xMjY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2
DTA1MDIxMTE2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2
DAYDVQQLEwVjcmxhYjESMBAGA1UEAxMjTWF5a2V0aW5nMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQC5GJnTtWbwV7sHModAxU70/W65GUoozfCQjCiX5JjZsYnO
XXCxBH10YwVaFXdC8qQNY82IN1DLXcA20b0TuI35I4MFwQOyYxH5s0yfbt4EF9/9
IXR+D9BVk4bjHM3BAAdRI7tsTSI+8V8g4E0Cog9eWVfMvieA1+njpBebkV2HALQID
AQABo4H0MIHxMASGALUdDwQEAWIAoDarBgNVHRAEJDAigA8yMDAyMDIxMTE2MDk1
NVqBDzIwMDQwMzE5MjAzOTU1WjBPBgNVHR8ESDBGMESgQqBAPd4wPDELMAkGALUE
BhMCMVVMxMjY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2
Q1JMMTAFBgNVHSMEGDAWgBTXKbA2cgxDMtUAn3eBFvom+M1O4zAdBgNVHQ4EFgQU
W1c43zktW2m85eFelRCv6eFGkqUwCQYDVROTBAlwADAZBgkqhkiG9w0HQQAEDDAK
GwRWNs4wAwIESDANBgkqhkiG9w0BAQUFAAOBgQAiK7crKU+oPoX/XE+mW6UIiyI
WTKUsSiZl jpluSiGq9Wpbe5aTSFqqWLIBY9+g71h/vMpfds00RK1JV7MzoJfluYw
siORD9jYCdLcJ7mhIdkYhf2WtF/KGalzq1MKEaAf5j5HGRu5HJQNzVWjJIXxx9kZ
w6vCMmwC3J36E3o77zCCAuQwggJNoAMCAQICBDrOBs8wDQYJKoZIhvcNAQEFBQAQ
LTELMAkGALUEBhMCMVVMxMjY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2
MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2MzY2
```



```
Validity
  Not Before: Feb 11 16:09:55 2002 GMT
  Not After : Feb 11 16:39:55 2005 GMT
MD5 Fingerprint: 74:2C:73:29:CA:AA:28:56:BA:BD:8D:86:84:AC:F9:E9
```

Do you want to import this certificate? **y**

```
Root Certificate:
  Serial Number: 986580687
  Issuer: OU=crlab,O=cisco,C=US
  Subject: OU=crlab,O=cisco,C=US
  Validity
    Not Before: Apr  6 17:41:27 2001 GMT
    Not After : Apr  6 18:11:27 2021 GMT
  MD5 Fingerprint: 89:84:6E:87:82:CC:E9:A4:C3:64:0A:21:6D:02:43:AD
```

Do you want to import this certificate? **y**  
VPN5000: Main#

**Note:** The validity period of the certificate is based on Greenwich Mean Time(GMT). Time and date are critical to the operation of public-key infrastructure. If you do not use a time server, it is probable that after you import the certificates into the VPN Concentrator, that the certificate does not correctly verify until the GMT listed in the certificate details equals the time in your particular time zone.

10. Verify that the server certificate is signed by the root certificate with the **certificate verify** command.

In order to display the certificate details, issue the **show certificate installed** command, as this example output illustrates.

```
VPN5000: Main# show certificate installed
Root Certificate:
  Serial Number: 986580687
  Issuer: OU=crlab,O=cisco,C=US
  Subject: OU=crlab,O=cisco,C=US
  Validity
    Not Before: Apr  6 17:41:27 2001 GMT
    Not After : Apr  6 18:11:27 2021 GMT
  MD5 Fingerprint: 89:84:6E:87:82:CC:E9:A4:C3:64:0A:21:6D:02:43:AD
Server Certificate:
  Serial Number: 986582534
  Issuer: OU=crlab,O=cisco,C=US
  Subject: CN=Marketing,OU=crlab,O=cisco,C=US
  Validity
    Not Before: Feb 11 16:09:55 2002 GMT
    Not After : Feb 11 16:39:55 2005 GMT
  MD5 Fingerprint: 74:2C:73:29:CA:AA:28:56:BA:BD:8D:86:84:AC:F9:E9
VPN5000: Main#
```

## Set Up Users on the Entrust Certificate Server

Follow this procedure.

1. Open the Entrust/RA application.
2. Before you set up users on the Entrust Certificate Server for use with the VPN 5000 Concentrator, a VPN 5000-specific usertype template file must be imported into the Entrust/RA application.

The contents of this template file are shown in this output. Copy and paste the contents of this file into a text editor and save the text file as **usertype.template**.

The contents of the usertypes.template file are as shown here.

```

[Instructions]
;
;This file defines the types of users and entities you can add to
;Entrust/PKI 5.0 as well as the attributes you can assign to each
;user type. Unless you have a special need to add new user types or
;add or remove attributes, you should not edit this file.
;Information here defines what you see in the New User and Change DN
;dialogs as well as the information you must add in each.
;Note that all text appearing after a semicolon is a comment
;and is not read by Entrust/Authority or Entrust/RA.
;Use comments (like these)to guide those who will edit this file.
;Following the instructions is the working template definition file.
;
;USER TYPE TEMPLATE LIST SECTION, PART 1
;
;This section lists the different types of users and entities.
;For every user type in this section, there must be a corresponding
;section that defines the user type, that is, the user type attributes.
;After "count=", type the number of user types in this list.
;There are five user types in the default template, therefore the
;default reads "count=5". If you add a single new user type,
;increase this value to 6. Below "count=" are the user type names.
;To add a new user type, add the user type number (next in sequence)
;and type the user type name. For example, "5=CA".
;The number 0 identifies the default setting in the New User and Change DN
;dialog boxes. This is the user type that appears first in the user type
;drop down box. Here, "Person" is the default user type.
;
;[User Type Template List]
;count=6
;0=Person
;1=Web Server
;2=Organizational Unit
;3=Hardware
;4=Person 4.0 PKI
;5=VPN User
;
;USER TYPE TEMPLATE DESCRIPTION
;
;The sections that follow the User Type Template List section include
;information about each user type, including the user type attributes.
;Using the Person user type section as an example, each line is explained below.
;
;[Person]
;id=0
;count=4
;Structural Object Class=organizationalPerson,person
;description=This is the user type to be used for most Entrust users.
;0=First Name,cn,1,0,0 (see USER TYPE TEMPLATE LIST SECTION, PART 2 below )
;1=Last Name,sn,2,1,0
;2=Serial Number,serialNumber,0,0,1,uniquelyIdentifiedUser
;3=Email,mail,2,0,0,rfc822MailUser
;
;[Person] Type the name of the user type. Begin a new heading with the name of
;the user type.
;id= Type the id number for the user type using the number listed in the User
;Type Template List section.
;count= Type the total number of attributes for this user type. A field for each
;attribute appears in the Add User and Change DN dialog boxes for the user type.
;Structural Object Class= Type the structural object class name for this user
;type. User types are modeled after the structural object classes defined by
;your Directory. Enter the name of the user type as it is listed in the Directory.
;Note that the syntax for the structural object class is different than the user
;type (in this example, organizationalPerson,person). Check your Directory for

```

```

;the correct syntax for the structural object class before typing this information.
;description= Type a description of the user type here. This description appears
;in the New User dialog box. This should be a user-friendly description to help
;administrators choose the correct user type for each new user or entity added
;to the PKI.
;
;USER TYPE TEMPLATE LIST SECTION, PART 2
;
;Under the information described above are the user type attributes.
;Using the Person user type section as an example, each line is explained below.
;
;overrideCommonNameFormat=1
;This override specifies how the cn or common name value is formed
;If the overrideCommonNameFormat is missing then the value entered
;is applied to the cn.
;If the overrideCommonNameFormat is invalid, an error will be
;displayed and logged to the log file.
;If the overrideCommonNameFormat is 1, the fields are combined in the
;following manner to create the cn:
;"cn=First Name Last Name"
;If the overrideCommonNameFormat is 2, the fields are combined in the
;following manner to create the cn:
;cn="Last Name, First Name"
;
;0=First Name,cn,1,0,0
;
;0= Type the number of the attribute in sequence beginning with 0.
;First Name represents the label as it will appear in the New User dialog box.
;cn, represents the common name of the user type, or commonly used first and
;last name.
;The next three values accomplish the results explained below.
;The first value determines how the In DN checkbox appears in the New User and
;Change DN dialog boxes and indicates whether the field is mandatory
;for the DN or not.
;0=enabled and unchecked, 1=mandatory - disabled and checked
;2=cannot be in DN - disabled and unchecked, 3= enabled and checked

;The second value indicates whether the field must be filled out and written to
;the Directory (even if it is not in the DN). For the second numeric field:
;0=optional, 1=mandatory.
; Note that the attributes that the Directory must be
;configured to support the attributes and naming choices that are made here. If
;you wish to add a new attribute to an entry, you need to ensure that the
;Directory will allow that attribute to be added to an entry. This usually means
;ensuring that the attribute is supported by the structural object class that is
;being used for the entry, or using an auxiliary object class on the entry that
;allows the new attribute to be added.

;The third value specifies whether the attribute value should be unique across all
;available searchbases in the Directory.
;Type 1 to make this attribute unique. SerialNumber is a common
;example of an attribute that is used this way.
;A final field can be added. This is Auxiliary Object Class information that you add
;to the Directory entry when created by Entrust.
;
;END OF INSTRUCTIONS
;
;-----
;
;THE TEMPLATE DEFINITION FILE
;

[User Type Template List]
count=4

```

```

0=Person
1=Web Server
2=Organizational Unit
3=VPN User

[Person]
id=0
count=4
Structural Object Class=organizationalPerson,person
description=This is the user type to be used for most Entrust users.
overrideCommonNameFormat=1
0=First Name,cn,1,0,0
1=Last Name,sn,2,1,0
2=Serial Number,serialNumber,0,0,1,uniquelyIdentifiedUser
3=Email,mail,2,0,0,rfc822MailUser

[Web Server]
id=1
count=2
Structural Object Class=applicationProcess
description=This type should be used for software components such as Web
_continue_= Servers.
0=Name,cn,1,0,0
1=Description,description,2,0,0
;You can only add the Organizational Unit user type using the Directory Browser.
;Note the DirBrowserOnly=1 line. Add Organizational units to Entrust/PKI after
;which to model searchbases.
;

[Organizational Unit]
id=2
count=1
Structural Object Class=organizationalUnit
DirBrowserOnly=1
description=<DESCRIPTION type user ou for>
0=Organizational Unit,ou,1,0,0
;
;Sample templates
;To add these templates to the product, increment the count in the
;[User Type Template List] section and assign the template the next id.
;For example, to add the Person 4.0 PKI template,
;increment the count to "count=4" in [User Type Template List]
;the next available id is "3"
;add "3=Person 4.0 PKI" below "2=Organizational Unit"
;change "id=3" in the [Person 4.0 PKI] definition
;
;[User Type Template List]
;count=4
;0=Person
;1=Web Server
;2=Organizational Unit
;3=Person 4.0 PKI
;4=VPN User
;
;[Person 4.0 PKI]
;id=3
;count=4
;Structural Object Class=organizationalPerson,person
;description=This is the user type to be used for most Entrust users.
;overrideCommonNameFormat=1
;0=First Name,cn,1,0,0
;1=Last Name,sn,2,1,0
;2=Serial Number,serialNumber,0,0,1,uniquelyIdentifiedUser
;3=Email,email,0,0,0,emailAddressUser

```

```
[Hardware]
id=<NEXT available>
count=3
Structural Object Class=device
description=This type should be used for hardware devices such as router
_continue_=s and VPN devices.
0=Name,cn,1,0,0
1=Serial Number,serialNumber,0,0,1,uniquelyIdentifiedUser
2=Description,description,2,0,0
```

```
[Person 4.0 PKI]
id=<NEXT available>
count=4
Structural Object Class=organizationalPerson,person
description=This is the user type to be used for most Entrust users.
overrideCommonNameFormat=1
0=First Name,cn,1,0,0
1=Last Name,sn,2,1,0
2=Serial Number,serialNumber,0,0,1,uniquelyIdentifiedUser
3=Email,email,0,0,0,emailAddressUser
```

```
[VPN User]
id=3
count=5
Structural Object Class=organizationalPerson,person
description=This is the user type to be used for VPN users.
overrideCommonNameFormat=1
0=First Name,cn,1,0,0
1=Last Name,sn,2,1,0
2=Serial Number,serialNumber,0,0,1,uniquelyIdentifiedUser
3=Email,mail,2,1,0,rfc822MailUser
4=Group,ou,3,0,0
```

3. Select **File** from the menu and then choose **Import** in order to import the **usertypes.template** file into Entrust.

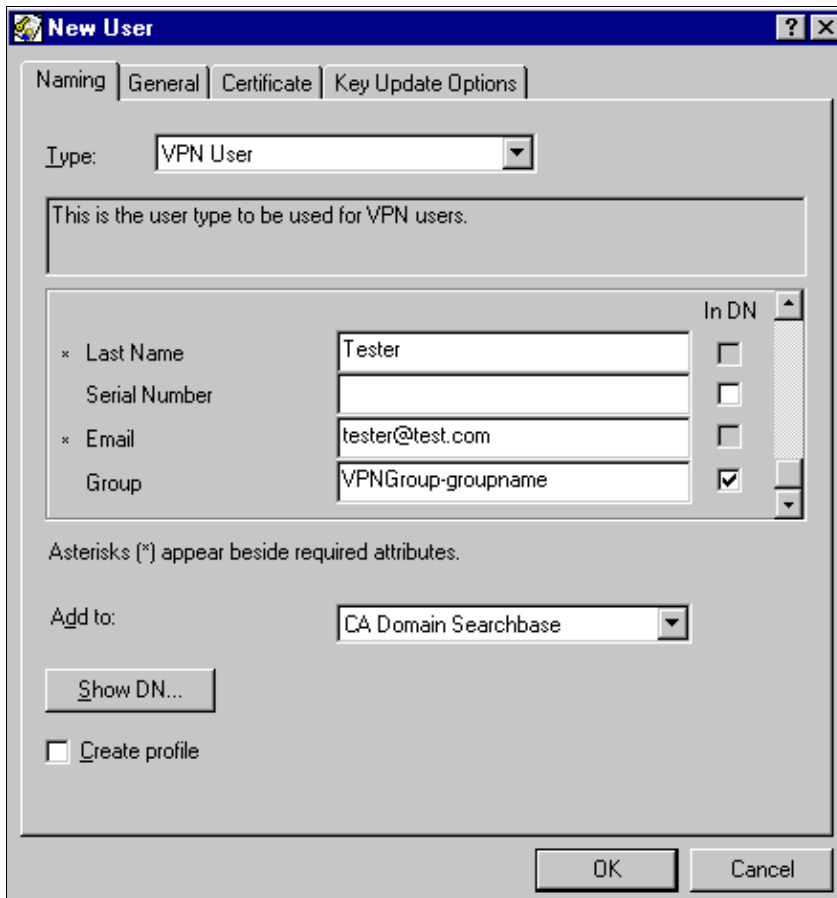
Navigate to the location of usertype.templates and select the file. The Operation Completed Successfully window appears with the message "Import User Templates completed successfully" when the user template is properly installed.

4. In order to add a user, select **Users** from the menu and then select **New User**. The New User window appears, with the Naming tab open.

5. Enter this user information.

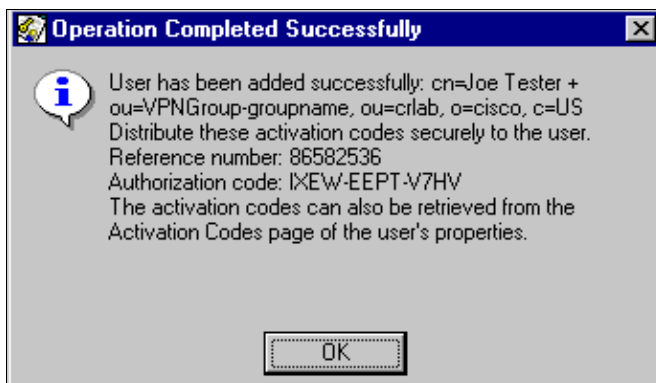
- ◆ Click on the pull-down menu next to the Type field and select **VPN User**.
- ◆ Enter the first and last name of the user in the appropriate fields.
- ◆ Enter the E-mail address of the user in the appropriate field.
- ◆ Scroll down in order to reveal the Group field, and enter the name of the VPNGroup of the user. Use the syntax **VPNGroup-groupname** , where *groupname* is the name of the VPNGroup that is configured on the VPN 5000 Concentrator to which the user is to be assigned. For example, if the VPNGroup that is configured on the VPN 5000 Concentrator is named "TestGroup", the Group field in Entrust needs to be specified as **VPNGroup-TestGroup**.
- ◆ Click on the pull-down menu next to the **Add to:** field and select the searchbase to which the user is to be assigned.

When you have entered all the information, click **OK**.



6. Once you successfully add the user to the Entrust Certificate server, the Operation Completed Successfully window appears.

This window contains the "Reference number" and "Activation code" that the user needs in order to log into Entrust and establish a profile. Record these values in order to distribute to the user.



## Install Entrust/Entelligence and Configure the VPN Client to Use Entrust Certificates

Follow this procedure.

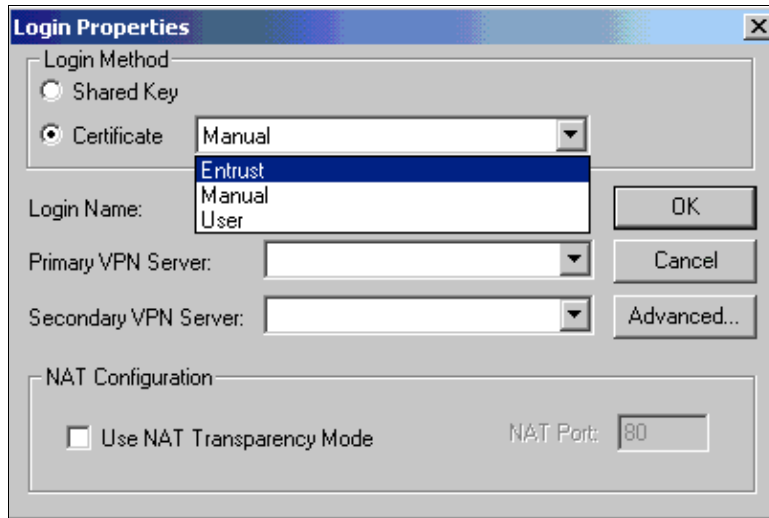
1. Copy the **entrust.ini** file into the Windows directory (for Windows 95, 98, and ME) or WinNT directory (for Windows NT) on the client workstation.
2. Install Entrust/Entelligence and create a user profile.

3. Ensure that the kmpapi32.dll file is in the system32 directory.

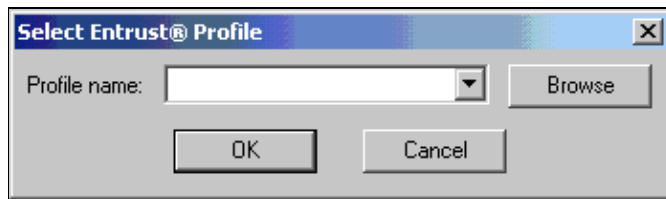
If this file is not present, locate the file on the Entrust Desktop Solutions CD and copy the file into the system32 directory.

4. Open the VPN Client and click **Add** to add a user.
5. Under Login Method, select **Certificate** and then choose **Entrust** from the pull-down menu.

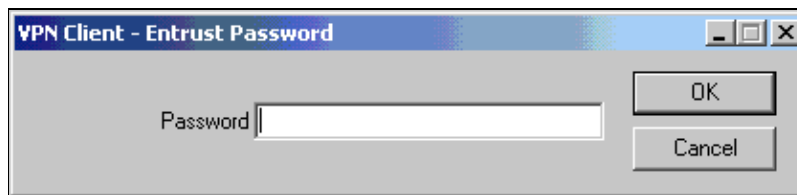
Enter the Login Name (E-mail address of the user) and the address of the VPN server in the appropriate fields. Click **OK** when you finish.



6. When you configure the VPN Client as an Entrust user, the user is prompted to browse to the location of the Entrust profile.



7. When the user has located the profile, the user is prompted for the Entrust password.



8. In order to initiate a VPN Client connection to the VPN Concentrator, click **Connect**. The user is prompted for the Entrust password in order to obtain the connection.

## Verify

This section provides information you can use in order to confirm that your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool ( registered customers only) , which allows you to view an analysis of **show** command output.

- **show version** Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.
- **show configuration** Displays the configuration.
- **show certificate installed** Displays certificates installed in the concentrator.
- **certificate verify** Verifies that the server certificate was installed successfully.

## Sample Configuration

```

[ General ]
VPNGateway                = 10.0.51.1
EthernetAddress           = 00:04:c1:57:a6:10
DeviceType                = VPN 5001 Concentrator
ConfiguredOn              = 4/11/01 12:13:34
ConfiguredFrom            = Command Line, from Console
IPSecGateway              = 10.0.51.1
DeviceName                = "VPN5001_ONE"
EnablePassword            =
Password                  =

[ IP Ethernet 0 ]
RIPVersion                 = None
SubnetMask                 = 255.255.255.0
IPAddress                 = 10.0.50.2
Mode                       = Routed

[ IP Ethernet 1 ]
SubnetMask                 = 255.255.255.0
IPAddress                 = 10.0.51.2
Mode                       = Routed

[ IKE Policy ]
Protection                 = MD5_3DES_G1

[ IP Static ]
0.0.0.0 0.0.0.0 10.0.50.1 1

[ Logging ]
Enabled                    = On
LogToAuxPort              = On
Level                     = 7

[ Certificates ]
LdapServer                 = 10.0.52.10

[ VPN Group "TestGroup" ]
TunnelNetBT               = On
WINSPrimaryServer         = 10.0.50.98
DNSPrimaryServer          = 10.0.50.97
KeepaliveInterval         = 120
InactivityTimeout         = 600
MaxConnections            = 25
BindTo                    = "ether 0"
StartIPAddress             = 10.0.50.129
IPNet                     = 0.0.0.0/0
Transform                  = esp(md5,3des)

```

## Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

## Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool ( registered customers only) , which allows you to view an analysis of **show** command output.

**Note:** Before you issue **debug** commands, refer to Important Information on Debug Commands.

In order to troubleshoot certificate–related connection problems, issue the commands shown here from a console Telnet connection on the VPN 5000 Concentrator.

- **show sys log buffer** Displays previously buffered events.
- **vpn trace dump all** Displays Internet Key Exchange (IKE) negotiation messages.

In order to review the actual login of a VPN session while in progress, collect the contents of the **vpnsession log** file, located in the IntraPort Client directory on the VPN 5000 Client.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

## Related Information

- [Cisco VPN 5000 Series Concentrators End–of–Sales Announcement](#)
- [Cisco VPN 5000 Concentrator Support Page](#)
- [Cisco VPN 5000 Client Support Page](#)
- [IPSec Support Page](#)
- [Technical Support – Cisco Systems](#)

---

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: May 08, 2005

Document ID: 17950

---