

IPSec Between PIX and Cisco VPN Client Using Smartcard Certificates Configuration Example

Document ID: 24020

Introduction

Prerequisites

Requirements

Components Used

Conventions

Enroll and Configure the PIX

Configurations

Enroll Cisco VPN Client Certificates

Configure the Cisco VPN Client in order to Use the Certificate for Connection to the PIX

Install eToken Smartcard Drivers

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document demonstrates how to configure an IPSec VPN tunnel between a PIX Firewall and a Cisco VPN Client 4.0.x. The configuration example in this document also highlights the certification authority (CA) enrollment procedure for both the Cisco IOS® router and the Cisco VPN Client, as well as the use of a Smartcard as a certificate storage.

Refer to [Configuring IPSec Between Cisco IOS Routers and Cisco VPN Client Using Entrust Certificates](#) in order to learn more about Configuring IPSec between Cisco IOS routers and Cisco VPN Client using Entrust Certificates.

Refer to [Configuring Multiple–Identity Certificate Authorities on Cisco IOS Routers](#) in order to learn more about Configuring Multiple–Identity Certificate Authorities on Cisco IOS routers.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco PIX Firewall running software version 6.3(3)
- Cisco VPN Client 4.0.3 on a PC running Windows XP
- A Microsoft Windows 2000 CA server is used in this document as the CA server.
- Certificates on the Cisco VPN Client are stored using Aladdin e–Token Smartcard.

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.

Enroll and Configure the PIX

In this section, you are presented with the information in order to configure the features described in this document.

Note: In order to find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Configurations

This document uses these configurations.

- Certificate Enrollment on PIX Firewall
- PIX Firewall Configuration

Certificate Enrollment on PIX Firewall

```
!--- Define a hostname and domain name for the router.
!--- The fully qualified domain name (FQDN) is used
!--- as the identity of the router during certificate enrollment.

pix(config)#hostname sv2-11
sv2-11(config)#domain-name cisco.com

!--- Confirm that you have the correct time set on the PIX.

show clock
clock set <hh:mm:ss> {<day> <month> | <month> <day>} <year>

!--- This command clears the PIX RSA keys.

ca zeroize rsa

!--- Generate RSA (encryption and authentication) keys.

ca gen rsa key

!--- Select the modulus size (512 or 1024).
!--- Confirm the keys generated.

show ca mypub rsa

!--- Define the CA identity.

ca ident kobe 10.1.1.2:/certsrv/mscep/mscep.dll
ca conf kobe ra 1 20 crlopt
ca auth kobe
ca enroll kobe [ipaddress]

!--- Confirm the certificate and validity.
```

```
show ca cert
```

PIX Firewall Configuration

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname sv2-11
domain-name cisco.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list 101 permit tcp any host 209.165.201.21 eq www
access-list 120 permit ip 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
ip address outside 209.165.201.20 255.255.255.224
ip address inside 10.1.1.10 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
ip audit info action alarm
ip audit attack action alarm
ip local pool vpnpool 10.0.0.10-10.0.0.100
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
```

```

nat (inside) 0 access-list 120
static (inside,outside) 209.165.201.21 10.1.1.2 netmask 255.255.255.255 0 0
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.30 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
isakmp policy 10 authentication rsa-sig
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup vpncert address-pool vpnpool
vpngroup vpncert idle-time 1800
vpngroup vpncert password *****
ca identity kobe 10.1.1.2:/certsrv/mscep/mscep.dll
ca configure kobe ra 1 20 crloptional
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:2ae252ac69e5218d13d35acdf1f30e55
: end
[OK]
sv2-11(config)#

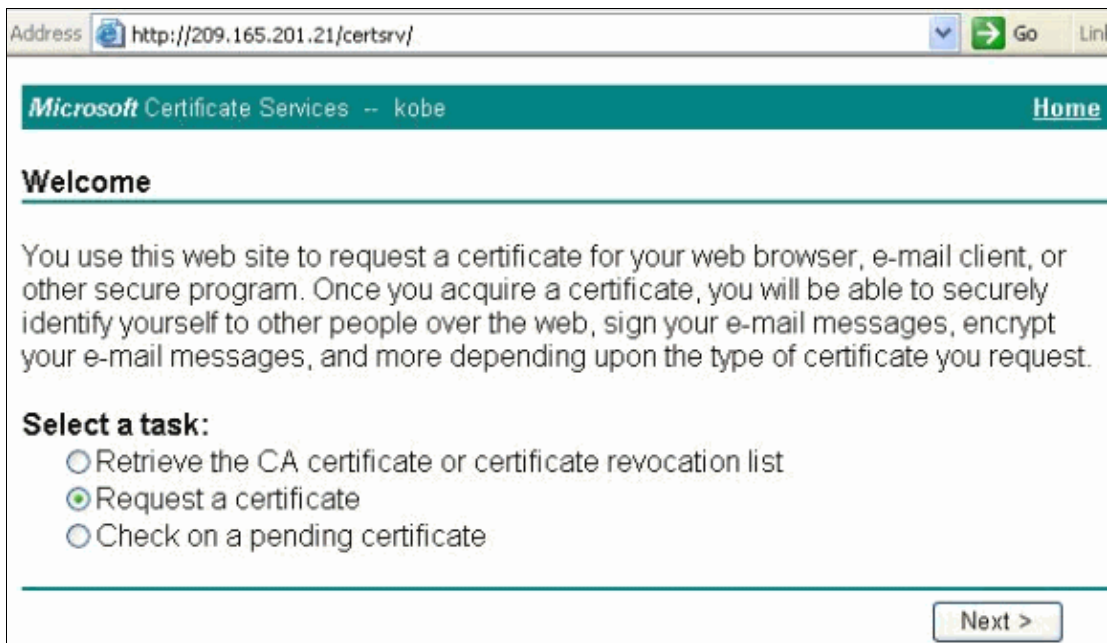
```

Enroll Cisco VPN Client Certificates

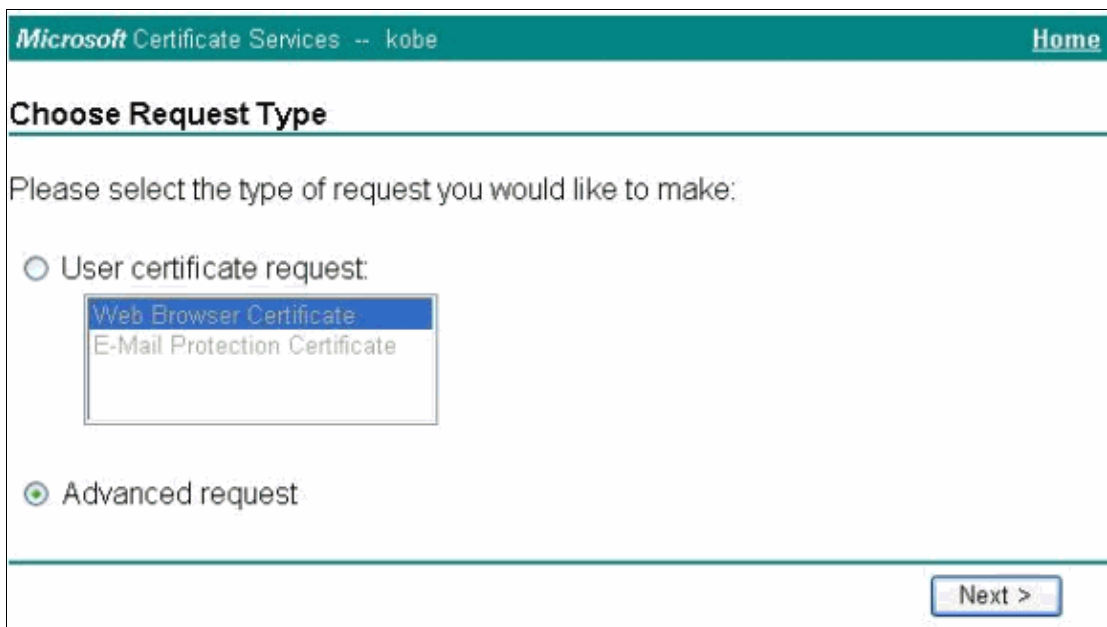
Remember to install all the necessary drivers and utilities that come with the Smartcard device on the PC to be used with the Cisco VPN Client.

These steps demonstrate the procedures used to enroll the Cisco VPN Client for MS certificates. The certificate is stored on the Aladdin e-Token Smartcard store.

1. Launch a browser and go to the certificate server page (<http://CAServeraddress/certsrv/>, in this example).
2. Select **Request a certificate** and click **Next**.



3. In the Choose Request Type window, select **Advanced request** and click **Next**.



4. Select **Submit a certificate request to this CA using a form** and click **Next**.

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

[Next >](#)

5. Fill in all the items on the Advanced Certificate Request form.

Be sure that the Department or organizational unit (OU) corresponds to the Cisco VPN Client group name, as configured in the PIX vpngroup name. Select the correct Certificate Service Provider (CSP) appropriate for your setup.

Advanced Certificate Request

Identifying Information:

Name:	<input type="text" value="ericetoken"/>
E-Mail:	<input type="text"/>
Company:	<input type="text" value="cisco"/>
Department:	<input type="text" value="vpncert"/>
City:	<input type="text" value="ctd"/>
State:	<input type="text" value="nsw"/>
Country/Region:	<input type="text" value="AU"/>

Intended Purpose:

Key Options:

CSP:

Key Usage: Exchange Signature Both

Key Size: Min: 384
Max: 1024 (common key sizes: [512](#) [1024](#))

- Create new key set
 Set the container name
 Use existing key set
 Enable strong private key protection
 Mark keys as exportable
 Use local machine store

You must be an administrator to generate

Additional Options:

Hash Algorithm:

Only used to sign request.

Save request to a PKCS #10 file

Attributes:

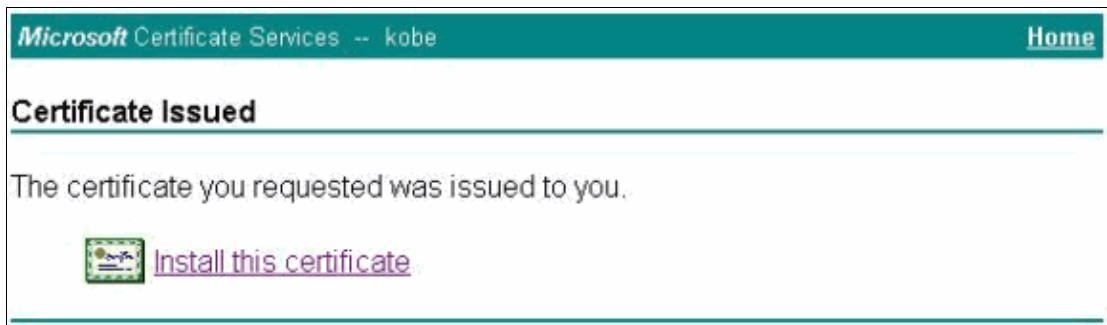
6. Select **Yes** in order to continue the installation when you get the Potential Scripting Validation warning.



7. The certificate enrollment invokes the eToken store. Enter the password and click **OK**.



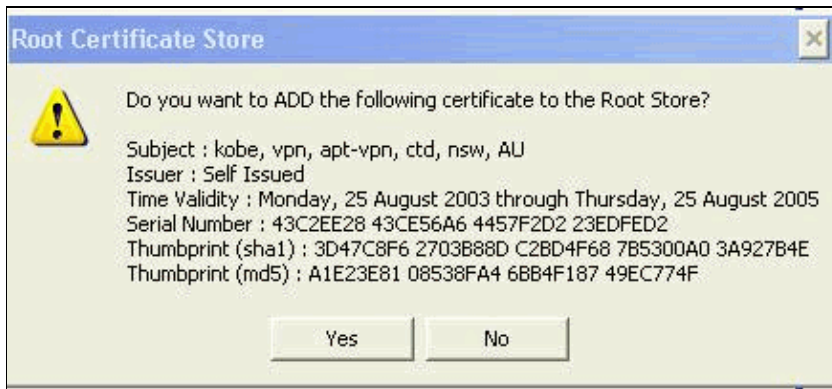
8. Click **Install this certificate**.



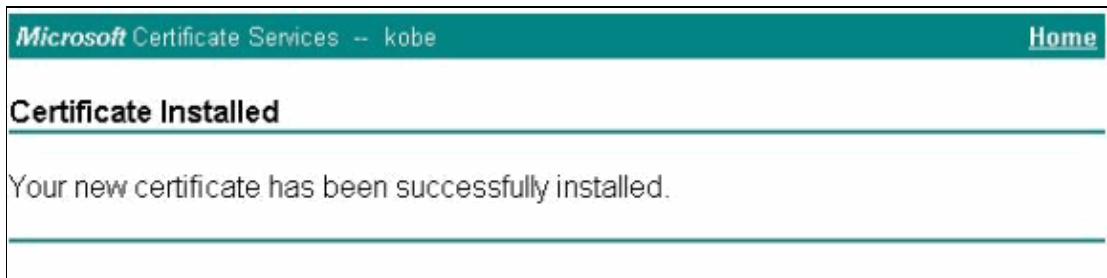
9. Select **Yes** in order to continue the installation when you get the Potential Scripting Validation warning.



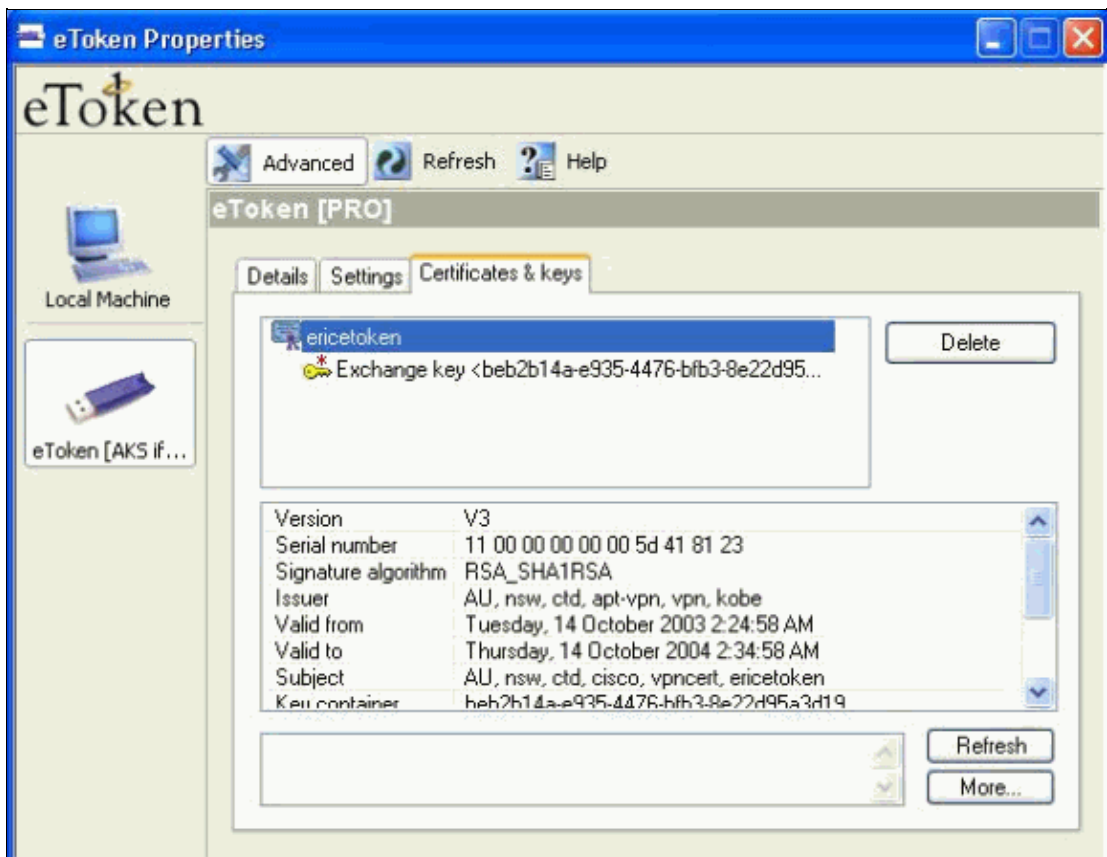
10. Select **Yes** in order to add the root certificate to the Root Store.



11. The Certificate Installed window appears and confirms the successful installation.



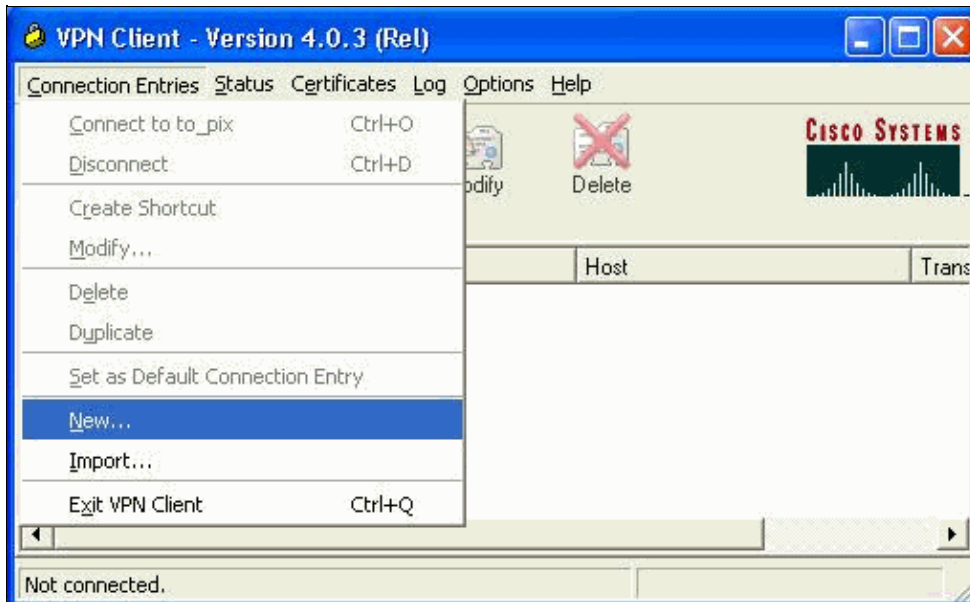
12. Use the eToken Application Viewer in order to view the certificate stored on the Smartcard.



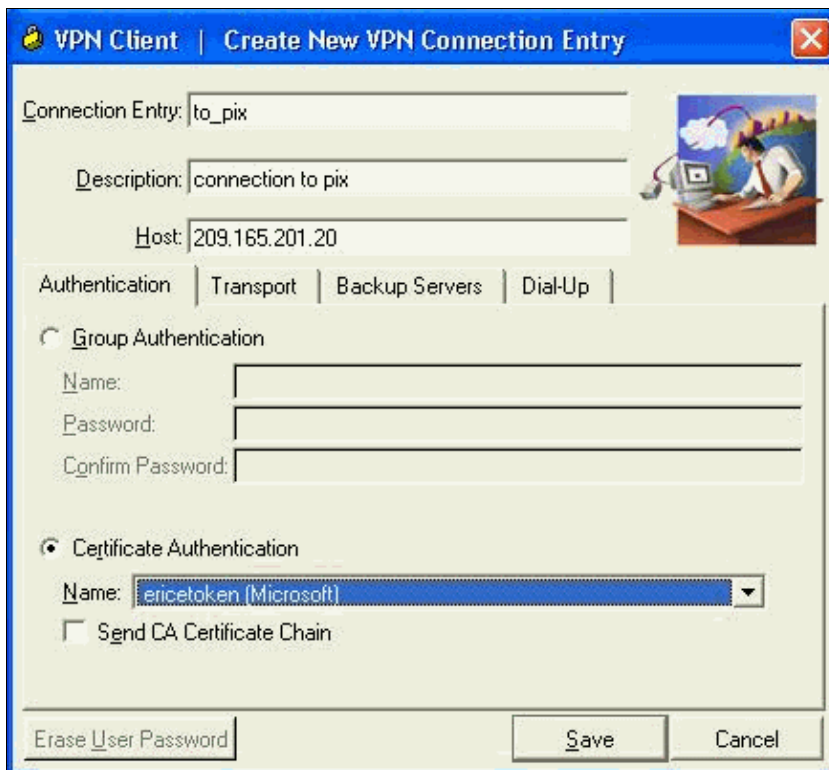
Configure the Cisco VPN Client in order to Use the Certificate for Connection to the PIX

These steps demonstrate the procedures used to configure the Cisco VPN Client to use the certificate for PIX connections.

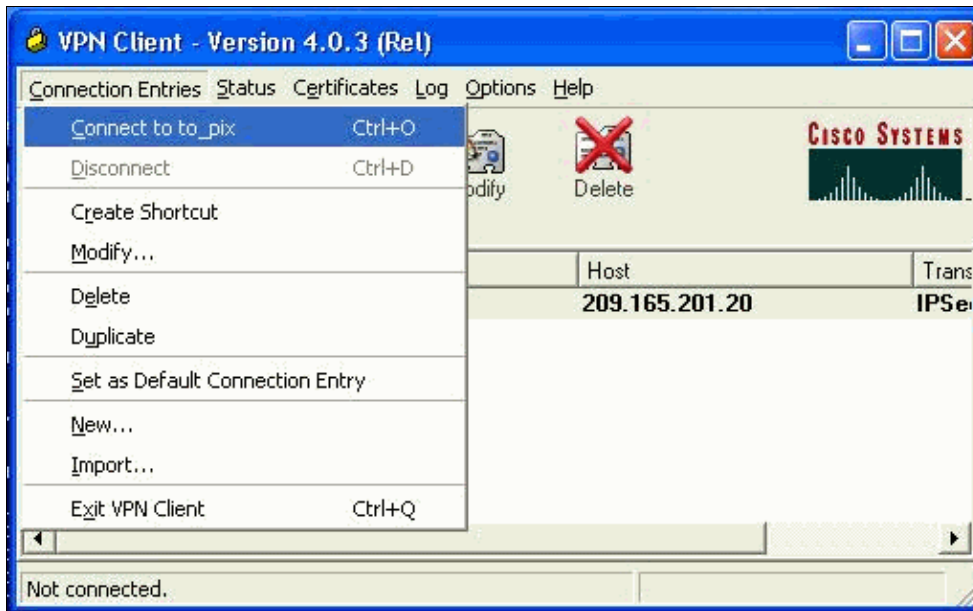
1. Launch the Cisco VPN Client. Under Connection Entries click **New** in order to create a new connection.



2. Complete the connection detail, specify Certificate Authentication, select the certificate obtained from enrollment. Click **Save**.



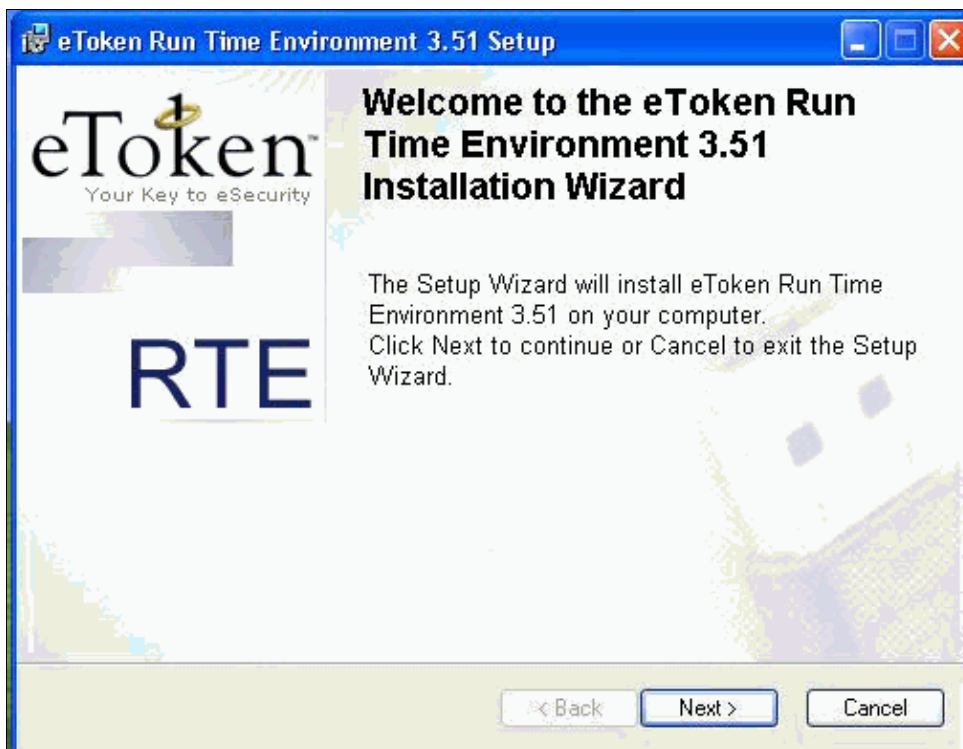
3. In order to start the Cisco VPN Client connection to the PIX, select the desired Connection Entry and click **Connect**.



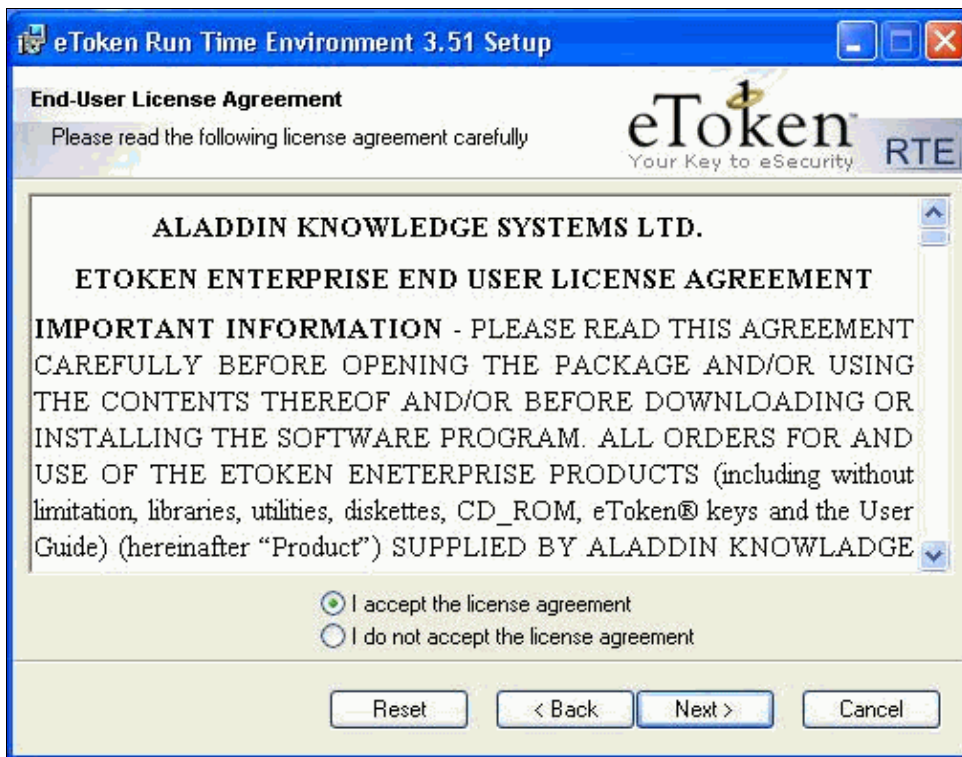
Install eToken Smartcard Drivers

These steps demonstrate the installation of the Aladdin eToken Smartcard drivers.

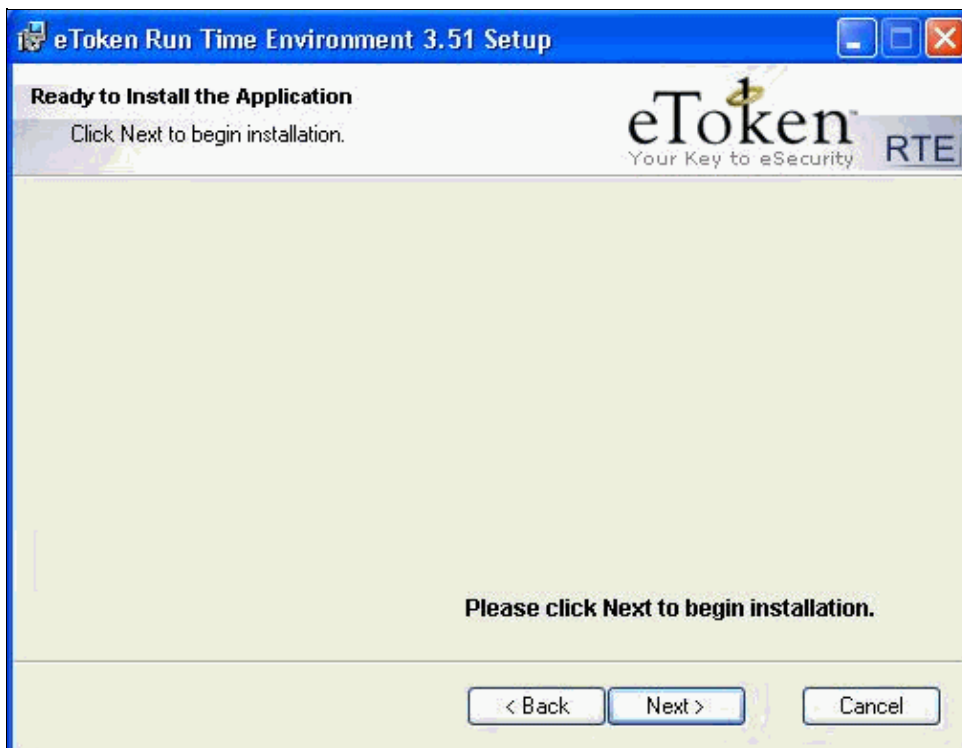
1. Open the eToken Run time Environment 3.51 setup wizard.



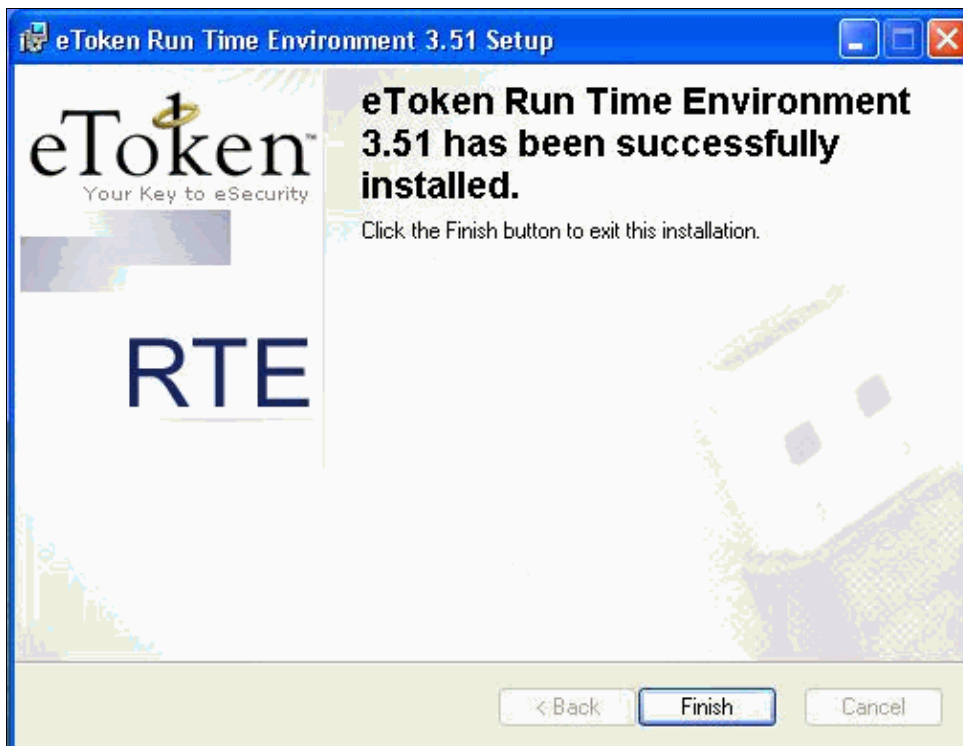
2. Accept the License Agreement terms and click **Next**.



3. Click **Install**.



4. The eToken Smartcard drivers are now installed. Click **Finish** in order to exit the setup wizard.



Verify

This section provides information you can use in order to confirm 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 crypto isakmp sa** Displays all current Internet Key Exchange (IKE) security associations (SAs) at a peer.

```
SV2-11(config)#show crypto isa sa
Total      : 1
Embryonic  : 0
          dst          src          state      pending    created
          209.165.201.20 209.165.201.19  QM_IDLE    0          1
```

- **show crypto ipsec sa** Displays the settings used by current security associations.

```
SV1-11(config)#show crypto ipsec sa
interface: outside
  Crypto map tag: mymap, local addr. 209.165.201.20
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.0.0.10/255.255.255.255/0/0)
current_peer: 209.165.201.19:500
dynamic allocated peer ip: 10.0.0.10
PERMIT, flags={}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 209.165.201.20, remote crypto endpt.: 209.165.201.19
  path mtu 1500, ipsec overhead 56, media mtu 1500
  current outbound spi: c9a9220e
inbound esp sas:
spi: 0xa9857984(2844096900)
transform: esp-3des esp-md5-hmac ,
```

```
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607996/28746)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xc9a9220e(3383304718)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4608000/28748)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Troubleshoot

Refer to Troubleshooting the PIX to Pass Data Traffic on an Established IPSec Tunnel for further information on troubleshooting this configuration.

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

- [Documentation for Cisco PIX Firewall](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Requests for Comments \(RFCs\)](#)
- [IPSec \(IP Security Protocol\) Support Page](#)
- [Cisco VPN Client Support Page](#)
- [PIX 500 Series Firewalls Support Page](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 14, 2008

Document ID: 24020
