

Configuring the Cisco VPN 3000 Concentrator 4.1 to Get a Digital Certificate Using SCEP

Document ID: 11090

Introduction

Prerequisites

Requirements

Components Used

Conventions

Install Digital Certificates on the VPN Concentrator Using SCEP

Related Information

Introduction

This document includes step-by-step instructions on how to configure the Cisco VPN 3000 Series Concentrators to authenticate using digital certificates using Simple Certificate Enrollment Protocol (SCEP).

Prerequisites

Requirements

Please make sure that you meet these requirements before attempting this procedure:

- If you are trying to install the certificates on the VPN 3000 Concentrator using SCEP using the Microsoft Certificate Server, make sure that you have installed the add-on package for SCEP before installation.
- Before you apply and receive the certificates, make sure that your clock is set to the right date and time.
- Make sure you have IP connectivity to the certificate server.

Components Used

The information in this document is based on Cisco VPN 3000 Series Concentrator 4.1.

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 Digital Certificates on the VPN Concentrator Using SCEP

Complete these steps:

1. To install the root certificate on the VPN 3000 Concentrator, select **Administration > Certificate Management**, and choose **Click here to install a CA certificate**.

The screenshot shows the 'Administration | Certificate Management' page. The page title is 'Administration | Certificate Management' and the date/time is 'Wednesday, 03 March 2004 15:52:26'. There is a 'Refresh' button. The main content area contains the following text: 'This section lets you view and manage certificates on the VPN 3000 Concentrator. Installation of a CA certificate is required before identity and SSL certificates can be installed.' Below this text are three bullet points: 'Click here to install a CA certificate', 'Click here to enroll with a Certificate Authority', and 'Click here to install a certificate'. The 'Certificate Authorities' section shows a table with columns: Subject, Issuer, Expiration, SCEP Issuer, and Actions. The table is currently empty, displaying 'No Certificate Authorities'. Below this is the 'Identity Certificates' section, also with columns: Subject, Issuer, Expiration, and Actions. This table is also empty, displaying 'No Identity Certificates'.

2. Select **SCEP (Simple Certificate Enrollment Protocol)** as the method to get the Certification Authority (CA) certificates.

The screenshot shows the 'Administration | Certificate Management | Enroll | Identity Certificate' page. The main content area contains the following text: 'Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. Click here to install a new CA using SCEP before enrolling.' Below this text is a bullet point: 'Enroll via PKCS10 Request (Manual)'. At the bottom of the page, there is a link: '<< Go back to Certificate Management'.


3. In the URL box, enter the complete URL of the CA server.

In the following example, the CA server has DNS name garrison (you can use the IP address if the VPN Concentrator is not configured for DNS). Since this example uses Microsoft's CA server, the complete URL is **http://garrison/certsrv/mscep/mscep.dll**.

Then, put a one-word descriptor in the CA Descriptor box. This example uses "CA".

The screenshot shows the 'Administration | Certificate Management | Install | CA Certificate | SCEP' page. The main content area contains the following text: 'Enter the information needed to retrieve the CA certificate via SCEP. Please wait for the operation to complete.' Below this text are two input fields: 'URL' with the value 'http://garrison/certsrv/mscep/mscep.dll' and 'CA Descriptor' with the value 'CA'. To the right of the 'CA Descriptor' field is the text 'Required for some PKI configurations.' At the bottom of the page are two buttons: 'Retrieve' and 'Cancel'.

4. Once you click **Retrieve**, you should see your CA certificate under **Administration > Certificate Management**. If you do not see a certificate, go back to step 1 and follow the procedure again.

Administration | Certificate Management Wednesday, 03 March 2004 15:58:29
Refresh 

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 3, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
garry at cisco	garry at cisco	02/20/2006	Yes	View Configure Delete SCEP Show RAs

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

5. Once you have the CA certificate, select **Administration > Certificate Management > Enroll**, choose **Identity certificate** and click **Enroll via SCEP at ...** to apply for the identity certificate.

Administration | Certificate Management | Enroll | Identity Certificate

Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. [Click here to install a new CA using SCEP before enrolling.](#)

- [Enroll via PKCS10 Request \(Manual\)](#)
- [Enroll via SCEP at garry at cisco](#)

[<< Go back to Certificate Management](#)

6. On the next screen, fill out the Enrollment form.

The following example uses:

- ◆ Common Name (CN) = APT3000
- ◆ Organizational Unit (OU) = APT-TAC
- ◆ Organization (O) = Cisco
- ◆ Locality (L) = Chatswood
- ◆ State/Province (SP) = NSW
- ◆ Country(C) = AU
- ◆ Fully Qualified Domain Name (FQDN) = (not used here)
- ◆ Subject Alternative Name (Email Address) = admin@cisco.com
- ◆ Challenge Password = (not used here)
- ◆ Verify Challenge Password = (not used here)
- ◆ Key Size = 512

Administration | Certificate Management | Enroll | Identity Certificate | SCEP

Enter the information to be included in the certificate request. **Please wait for the operation to finish.**

Common Name (CN)	<input type="text" value="APT3000"/>	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	<input type="text" value="APT-TAC"/>	Enter the department.
Organization (O)	<input type="text" value="Cisco"/>	Enter the Organization or company.
Locality (L)	<input type="text" value="Chatswood"/>	Enter the city or town.
State/Province (SP)	<input type="text" value="NSW"/>	Enter the State or Province.
Country (C)	<input type="text" value="AU"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	<input type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E-Mail Address)	<input type="text" value="admin@cisco.com"/>	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Challenge Password	<input type="text"/>	Enter and verify the challenge password for this certificate request.
Verify Challenge Password	<input type="text"/>	
Key Size	<input type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA key pair.

7. After selecting **Enroll**, you should see the SCEP Status in the Polling State. Go to your CA server to approve the identity certificate.

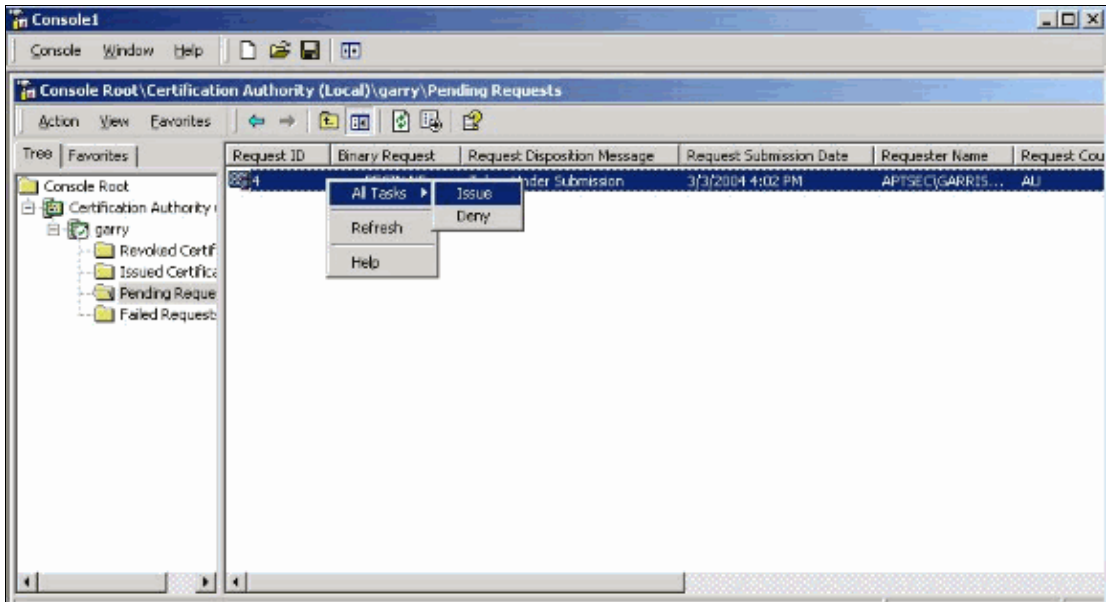
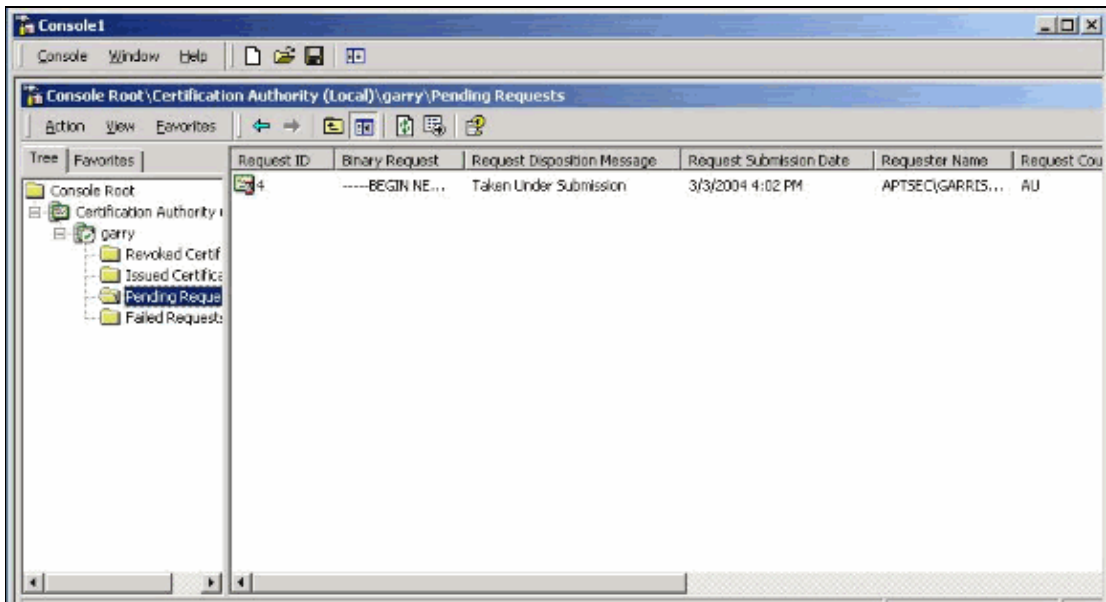
Administration | Certificate Management | Enrollment | Request Generated

A certificate request has been generated.

SCEP Status: Polling

- [Go to Certificate Management](#)
- [Go to Certificate Enrollment](#)
- [Go to Certificate Installation](#)

8. On the Microsoft CA server, bring up **Certificate Authority** and issue the pending certificate.



9. Once the identity certificate is issued, select **Administration > Certificate Management** to make sure that your VPN 3000 Concentrator has received it.

Administration | Certificate Management Wednesday, 03 March 2004 16:07:32

[Refresh](#)

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 3, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
garry at cisco	garry at cisco	02/20/2006	Yes	View Configure Delete SCEP Show RAs

Identity Certificates (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
APT3000 at Cisco	garry at cisco	03/03/2005	View Renew Delete

Note: For complete information about digital certificates see the Administration | Certificate Management section of the VPN 3000 Concentrator Series User Guide (in PDF).

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
 - [Cisco VPN 3000 Series Client Support Page](#)
 - [IPSec 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: 11090
