

CRL Checking Over HTTP on a Cisco VPN 3000 Concentrator

Document ID: 26383

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions
- Network Diagram

Configure the VPN 3000 Concentrator

- Step-by-Step Instructions
- Monitoring

Verify

- Logs from Concentrator
- Successful Concentrator Logs
- Failed Logs

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how to enable certificate revocation list (CRL) checking for certification authority (CA) certificates installed in the Cisco VPN 3000 Concentrator using HTTP mode.

A certificate is normally expected to be valid for its entire validity period. However, if a certificate becomes invalid due to such things as a name change, change of association between the subject and the CA, and security compromise, the CA revokes the certificate. Under X.509, CAs revoke certificates by periodically issuing a signed CRL, where each revoked certificate is identified by its serial number. Enabling CRL checking means that every time the VPN Concentrator uses the certificate for authentication, it also checks the CRL to ensure that the certificate being verified has not been revoked.

CAs use Lightweight Directory Access Protocol (LDAP)/HTTP databases to store and distribute CRLs. They might also use other means, but the VPN Concentrator relies on LDAP/HTTP access.

HTTP CRL checking is introduced in VPN Concentrator version 3.6 or later. However, LDAP-based CRL checking was introduced in the earlier 3.x releases. This document only discusses CRL checking using HTTP.

Note: The CRL cache size of VPN 3000 Series Concentrators depends on the platform and it cannot be configured according to the wish of the administrator.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- You have successfully established the IPsec tunnel from the VPN 3.x Hardware Clients using

certificates for Internet Key Exchange (IKE) authentication (with no CRL checking enabled).

- Your VPN Concentrator has connectivity to the CA server at all times.
- If your CA server is connected out to the public interface, then you have opened necessary rules in the public (default) filter.

Components Used

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

- VPN 3000 Concentrator version 4.0.1 C
- VPN 3.x Hardware Client
- Microsoft CA server for certificate generation and CRL checking running on a Windows 2000 server.

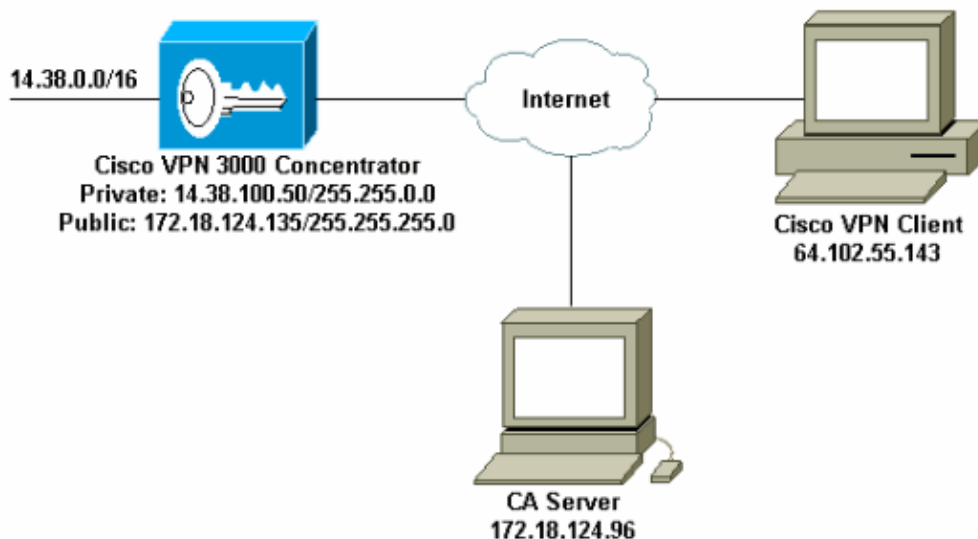
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Network Diagram

This document uses this network setup:



Configure the VPN 3000 Concentrator

Step-by-Step Instructions

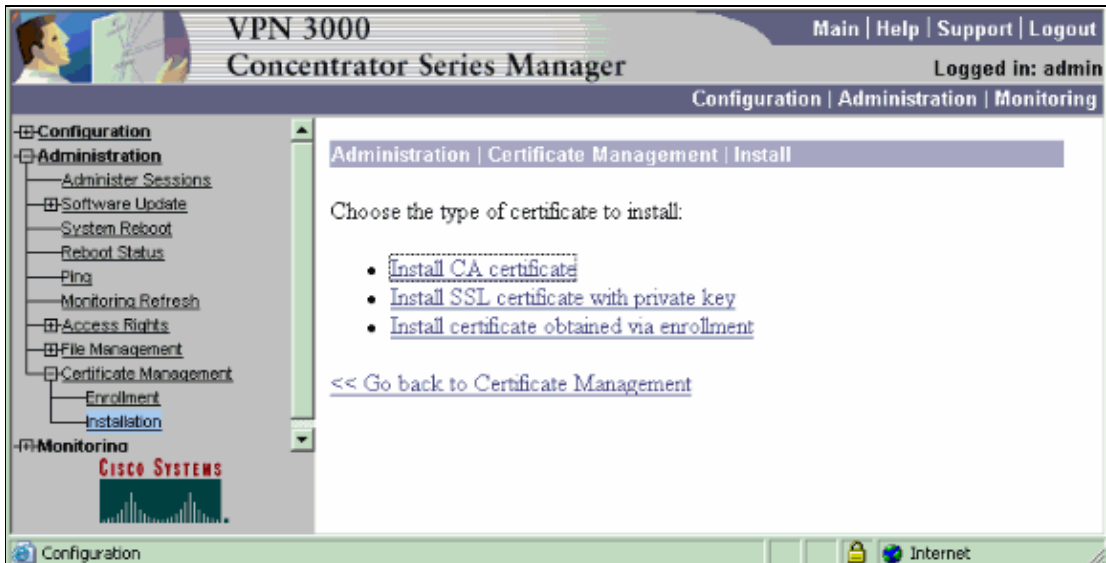
Complete these steps to configure the VPN 3000 Concentrator:

1. Select **Administration > Certificate Management** to request a certificate if you do not have a certificate.

Select **Click here to install a certificate** to install the root certificate on the VPN Concentrator.



2. Select **Install CA certificate**.

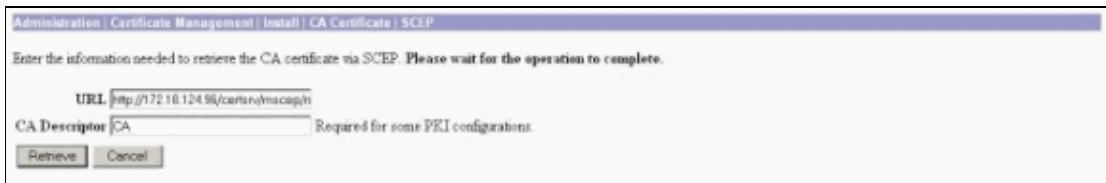


3. Select **SCEP (Simple Certificate Enrollment Protocol)** to retrieve the CA certificates.



4. From the SCEP window, enter the complete URL of the CA server in the URL dialog box.

In this example, the CA server's IP address is 172.18.124.96. Since this example uses Microsoft's CA server, the complete URL is `http://172.18.124.96/certsrv/mscep/mscep.dll`. Next, enter a one-word descriptor in the CA Descriptor dialog box. This example uses CA.



5. Click **Retrieve**.

Your CA certificate should appear under the Administration > Certificate Management window. If you do not see a certificate, go back to Step 1 and follow the procedure again.

Administration | Certificate Management Thursday, 15 August 2007 11:45:44
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 CAs](#) | [Clear All CAs](#) | [Clear CAs](#)) (current: 3, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
janb-ca-ra at Cisco Systems	janb-ca-ra at Cisco Systems	03/12/2005	Yes	View Configure Delete SCEP Show RSA

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificate ([Remove](#)) *Note: The public key in the SSL certificate is also used for the SSH host key.*

Subject	Issuer	Expiration	Actions
14.38.100.50 at Cisco Systems, Inc.	14.38.100.50 at Cisco Systems, Inc.	08/14/2005	View Renew Delete

Enrollment Status ([Remove All](#) | [Enrolled](#) | [Timed Out](#) | [Rejected](#) | [Cancelled](#) | [In Progress](#)) (current: 0 available: 20)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

6. Once you have the CA certificate, select **Administration > Certificate Management > Enroll**, and click **Identity certificate**.

Administration | Certificate Management | Enroll

This section allows you to create an SSL or identity certificate request. The identity certificate request allows the VPN 3000 Concentrator to be enrolled into the PKI. The certificate request can be sent to a CA, which will issue a certificate. The CA's certificate *must* be installed as a Certificate Authority before installing the certificate you requested.

Choose the type of certificate request to create:

- [Identity certificate](#)
- [SSL certificate](#)

[Go back to Certificate Management](#)

7. 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 janb-ca-ra at Cisco Systems](#)

[Go back and choose a different type of certificate](#)

8. Complete these steps to fill out the Enrollment form:
- Enter the common name for the VPN Concentrator to be used in the public-key infrastructure (PKI) in the Common Name (CN) field.
 - Enter your department in the Organizational Unit (OU) field. The OU should match the configured IPsec group name.
 - Enter your organization or company in the Organization (O) field.
 - Enter your city or town in the Locality (L) field.
 - Enter your state or province in the State/Province (SP) field.
 - Enter your country in the Country (C) field.
 - Enter the Fully Qualified Domain Name (FQDN) for the VPN Concentrator to be used in the PKI in the Fully Qualified Domain Name (FQDN) field.
 - Enter the email address for the VPN Concentrator to be used in the PKI in the Subject Alternative Name (email Address) field.
 - Enter the challenge password for the certificate request in the Challenge Password field.
 - Re-enter the challenge password in the Verify Challenge Password field.
 - Select the key size for the generated RSA key pair from the Key Size drop-down list.

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) Enter the common name for the VPN 3000 Concentrator to be used in this PKI

Organizational Unit (OU) Enter the department

Organization (O) Enter the Organization or company

Locality (L) Enter the city or town

State/Province (SP) Enter the State or Province

Country (C) Enter the two-letter country abbreviation (e.g. United States = US)

Subject AlternativeName (FQDN) Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI

Subject AlternativeName (E-Mail Address) Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI

Challenge Password

Verify Challenge Password

Key Size Select the key size for the generated RSA key pair.

9. Select **Enroll** and view the SCEP status in the polling state.
10. Go to your CA server to approve the identity certificate. Once it is approved on the CA server, your SCEP status should be Installed.

Administration | Certificate Management | Enrollment | Request Generated

A certificate request has been generated.

SCEP Status: Installed

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

11. Under Certificate Management, you should see your Identity Certificate.

If you do not, check the logs on your CA server for more troubleshooting.

Administration | Certificate Management Thursday, 15 August 2002 11:50:14
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 CAs](#)] [[Clear All CAs](#)] (current: 3, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
jamb-ca-ra at Circo Systems	jamb-ca-ra at Circo Systems	03/12/2005	Yes	View Configure Delete SCEP Show RSA

Identity Certificates (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
Concentrator_cert at Circo	jamb-ca-ra at Circo Systems	08/15/2003	View Enroll Delete

SSL Certificate [[Generate](#)] *Note: The public key in the SSL certificate is also used for the SSH host key.*

Subject	Issuer	Expiration	Actions
14.38.100.50 at Circo Systems, Inc.	14.38.100.50 at Circo Systems, Inc.	08/14/2005	View Renew Delete

Enrollment Status [[Remove All](#)] [[Enroll](#)] [[Timed-Out](#)] [[Rejected](#)] [[Cancelled](#)] [[In-Progress](#)] (current: 0 available: 19)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

12. Select **View** on your received certificate to see if your certificate has a CRL Distribution Point (CDP).

CDP lists all CRL distribution points from the issuer of this certificate. If you have CDP on your certificate, and you use a DNS name to send a query to the CA server, make sure that you have DNS servers defined in your VPN Concentrator to resolve the hostname with an IP address. In this case, the example CA server's host name is jazib-pc which resolves to an IP address of 172.18.124.96 on the DNS server.



13. Click **Configure** on your CA certificate to enable CRL checking on the received certificates.

If you have CDP on your received certificate and you would like to use it, then select **Use CRL distribution points from the certificate being checked**.

Since the system has to retrieve and examine the CRL from a network distribution point, enabling CRL checking might slow system response times. Also, if the network is slow or congested, CRL checking might fail. Enable CRL caching to mitigate these potential problems. This stores the retrieved CRLs in local volatile memory and therefore allows the VPN Concentrator to verify the revocation status of certificates more quickly.

With CRL caching enabled, the VPN Concentrator first checks whether the required CRL exists in the cache and checks the serial number of the certificate against the list of serial numbers in the CRL when it needs to check the revocation status of a certificate. The certificate is considered revoked if its serial number is found. The VPN Concentrator retrieves a CRL from an external server either when it does not find the required CRL in the cache, when the validity period of the cached CRL has expired, or when the configured refresh time has elapsed. When the VPN Concentrator receives a new CRL from an external server, it updates the cache with the new CRL. The cache can contain up to 64 CRLs.

Note: The CRL cache exists in memory. Therefore, rebooting the VPN Concentrator clears the CRL cache. The VPN Concentrator repopulates the CRL cache with updated CRLs as it processes new peer authentication requests.

If you select **Use static CRL distribution points**, then you can use up to five static CRL distribution points, as specified on this window. If you choose this option, you must enter at least one URL.

You can also select **Use CRL distribution points from the certificate being checked**, or select **Use static CRL distribution points**. If the VPN Concentrator cannot find five CRL distribution points in the certificate, it adds static CRL distribution points, up to a limit of five. If you choose this option, enable at least one CRL Distribution Point Protocol. You also must enter at least one (and no more than five) static CRL distribution points.

Select **No CRL Checking** if you want to disable CRL checking.

Under CRL Caching, select the **Enabled** box to allow the VPN Concentrator to cache retrieved CRLs. The default is not to enable CRL caching. When you disable CRL caching (unselect the box), the CRL cache is cleared.

If you configured a CRL retrieval policy that uses CRL distribution points from the certificate being checked, choose a distribution point protocol to use to retrieve the CRL. Choose **HTTP** in this case to retrieve the CRL. Assign HTTP rules to the public interface filter if your CA server is towards the

public interface.

Administration | Certificate Management | Configure CA Certificate

Certificate jazib-ca-ra at Cisco Systems

CRL Retrieval Policy

Use CRL distribution points from the certificate being checked
 Use static CRL distribution points
 Use CRL distribution points from the certificate being checked or else use static CRL distribution points
 No CRL checking

Choose the method to use to retrieve the CRL.

CRL Caching

Enabled

Refresh Time: 60

Check to enable CRL caching. Disabling will clear CRL cache.
Enter the refresh time in minutes (5 - 1440). Enter 0 to use the Next Update field in the cached CRL.

CRL Distribution Points Protocols

HTTP
 LDAP

Choose a distribution point protocol to use to retrieve the CRL. If you choose HTTP, be sure to assign HTTP rules to the public interface filter. (For more information, click Help.) If you choose LDAP, configure the LDAP distribution point defaults below.

LDAP Distribution Point Defaults

Server:
Server Port: 389
Login DN:
Password:
Verify:

Enter the hostname or IP address of the server.
Enter the port number of the server. The default port is 389.
Enter the login DN for access to the CRL on the server.
Enter the password for the login DN.
Verify the password for the login DN.

Static CRL Distribution Points

LDAP or HTTP URLs:

- Enter up to 5 URLs to use to retrieve the CRL from the server.
- Enter each URL on a new line.

Certificate Acceptance Policy

Accept Subordinate CA Certificates
 Accept Identity Certificates signed by this issuer

Apply Cancel

Monitoring

Select **Administration > Certificate Management** and click on **View All CRL caches** to see if your VPN Concentrator has cached any CRLs from the CA server.

Verify

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

Logs from Concentrator

Enable these events on the VPN Concentrator in order to make sure that CRL checking works.

1. Select **Configuration > System > Events > Classes** to set the logging levels.
2. Under Class Name select either **IKE, IKEDBG, IPSEC, IPSECDBG, or CERT**.
3. Click either **Add** or **Modify**, and choose **Severity to Log option 1–13**.
4. Click **Apply** if you want to modify, or **Add** if you want to add a new entry.

Successful Concentrator Logs

If your CRL checking is successful, these messages are seen in Filterable Event Logs.

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl

1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)
```

```
1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1
Certificate has not been revoked: session = 2
```

```
1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1
CERT_Callback(62f56e8, 0, 0)
```

```
1320 08/15/2002 13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53
Group [ipsecgroup]
Validation of certificate successful
(CN=client_cert, SN=61521511000000000086)
```

Refer to Successful Concentrator Logs for the complete output of a successful concentrator log.

Failed Logs

If your CRL checking is not successful, these messages are seen in the Filterable Event Logs.

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2
Failed to retrieve revocation list: session = 5
```

```
1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
have been configured.
```

```
1335 08/15/2002 18:00:36.730 SEV=7 CERT/8 RPT=2
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
from the server.
```

Refer to Revoked Concentrator Logs for the complete output of a failed concentrator log.

Refer to Successful Client Logs for the complete output of a successful client log.

Refer to Revoked Client Logs for the complete output of a failed client log.

Troubleshoot

Refer to Troubleshooting Connection Problems on the VPN 3000 Concentrator for more troubleshooting information.

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 3000 Series Concentrators Support Page](#)
 - [Cisco VPN 3000 Client Support Page](#)
 - [IPsec Negotiation/IKE Protocols](#)
 - [Technical Support & Documentation – 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: Mar 13, 2006

Document ID: 26383
