Configuring Authorization and Revocation of Certificates in a PKI

This module describes how to configure authorization and revocation of certificates in a public key infrastructure (PKI). It includes information on high-availability support for the certificate server.

Note

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

- Finding Feature Information, page 1
- Prerequisites for Authorization and Revocation of Certificates, page 2
- Restrictions for Authorization and Revocation of Certificates, page 2
- Information About Authorization and Revocation of Certificates, page 2
- How to Configure Authorization and Revocation of Certificates for Your PKI, page 10
- Configuration Examples for Setting Up Authorization and Revocation of Certificates, page 34
- Additional References, page 47
- Feature Information for Certificate Authorization and Revocation, page 47

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Prerequisites for Authorization and Revocation of Certificates

Plan Your PKI Strategy

Tip
It is strongly recommended that you plan your entire PKI strategy before you begin to deploy actual certificates.

Authorization and revocation can occur only after you or a network administrator have completed the following tasks:

• Configured the certificate authority (CA).
• Enrolled peer devices with the CA.
• Identified and configured the protocol (such as IP Security [IPsec] or secure socket layer [SSL]) that is to be used for peer-to-peer communication.

You should decide which authorization and revocation strategy you are going to configure before enrolling peer devices because the peer device certificates might have to contain authorization and revocation-specific information.

“crypto ca” to “crypto pk1” CLI Change
As of Cisco IOS Release 12.3(7)T, all commands that begin as “crypto ca” have been changed to begin as “crypto pki.” Although the router will still accept crypto ca commands, all output will be read back as crypto pki.

High Availability
For high availability, IPsec-secured Stream Control Transmission Protocol (SCTP) must be configured on both the active and the standby routers. For synchronization to work, the redundancy mode on the certificate servers must be set to ACTIVE/STANDBY after you configure SCTP.

Restrictions for Authorization and Revocation of Certificates

PKI High Availability (HA) support of intra-chassis stateful switchover (SSO) redundancy is currently not supported on all switches running the Cisco IOS Release 12.2 S software. See Cisco bug CSCtb59872 for more information.

Information About Authorization and Revocation of Certificates

PKI Authorization
PKI authentication does not provide authorization. Current solutions for authorization are specific to the router that is being configured, although a centrally managed solution is often required.
There is not a standard mechanism by which certificates are defined as authorized for some tasks and not for others. This authorization information can be captured in the certificate itself if the application is aware of the certificate-based authorization information. But this solution does not provide a simple mechanism for real-time updates to the authorization information and forces each application to be aware of the specific authorization information embedded in the certificate.

When the certificate-based ACL mechanism is configured as part of the trustpoint authentication, the application is no longer responsible for determining this authorization information, and it is no longer possible to specify for which application the certificate is authorized. In some cases, the certificate-based ACL on the router gets so large that it cannot be managed. Additionally, it is beneficial to retrieve certificate-based ACL indications from an external server. (For more information on using certificate-based ACLs for authentication, see the section "When to Use Certificate-Based ACLs for Authorization or Revocation, on page 7.)

Current solutions to the real-time authorization problem involve specifying a new protocol and building a new server (with associated tasks, such as management and data distribution).

PKI and AAA Server Integration for Certificate Status

Integrating your PKI with an authentication, authorization, and accounting (AAA) server provides an alternative online certificate status solution that leverages the existing AAA infrastructure. Certificates can be listed in the AAA database with appropriate levels of authorization. For components that do not explicitly support PKI-AAA, a default label of “all” from the AAA server provides authorization. Likewise, a label of “none” from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent, but “none” is included for completeness and clarity). If the application component does support PKI-AAA, the component may be specified directly; for example, the application component could be “ipsec,” “ssl,” or “osp.” (ipsec=IP Security, ssl=Secure Sockets Layer, and osp=Open Settlement Protocol.)

Note

Currently, no application component supports specification of the application label.

- There may be a time delay when accessing the AAA server. If the AAA server is not available, the authorization fails.

RADIUS or TACACS+ Choosing a AAA Server Protocol

The AAA server can be configured to work with either the RADIUS or TACACS+ protocol. When you are configuring the AAA server for the PKI integration, you must set the RADIUS or TACACS attributes that are required for authorization.

If the RADIUS protocol is used, the password that is configured for the username in the AAA server should be set to “cisco,” which is acceptable because the certificate validation provides authentication and the AAA database is only being used for authorization. When the TACACS protocol is used, the password that is configured for the username in the AAA server is irrelevant because TACACS supports authorization without requiring authentication (the password is used for authentication).

In addition, if you are using TACACS, you must add a PKI service to the AAA server. The custom attribute “cert-application=all” is added under the PKI service for the particular user or usergroup to authorize the specific username.
Attribute-Value Pairs for PKI and AAA Server Integration

The table below lists the attribute-value (AV) pairs that are to be used when setting up PKI integration with a AAA server. (Note the values shown in the table are possible values.) The AV pairs must match the client configuration. If they do not match, the peer certificate is not authorized.

Users can sometimes have AV pairs that are different from those of every other user. As a result, a unique username is required for each user. The all parameter (within the authorization username command) specifies that the entire subject name of the certificate will be used as the authorization username.

Table 1: AV Pairs That Must Match

<table>
<thead>
<tr>
<th>AV Pair</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco-avpair=pki:cert-application=all</td>
<td>Valid values are &quot;all&quot; and &quot;none.&quot;</td>
</tr>
<tr>
<td>cisco-avpair=pki:cert-trustpoint=msca</td>
<td>The value is a Cisco IOS command-line interface (CLI) configuration trustpoint label. Note: The cert-trustpoint AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.</td>
</tr>
<tr>
<td>cisco-avpair=pki:cert-serial=16318DB700010001671</td>
<td>The value is a certificate serial number. Note: The cert-serial AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.</td>
</tr>
<tr>
<td>cisco-avpair=pki:cert-lifetime-end=1:00 jan 1, 2003</td>
<td>The cert-lifetime-end AV pair is available to artificially extend a certificate lifetime beyond the time period that is indicated in the certificate itself. If the cert-lifetime-end AV pair is used, the cert-trustpoint and cert-serial AV pairs must also be specified. The value must match the following form: hours:minutes month day, year. Note: Only the first three characters of a month are used: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. If more than three characters are entered for the month, the remaining characters are ignored (for example Janxxxx).</td>
</tr>
</tbody>
</table>
CRLs or OCSP Server Choosing a Certificate Revocation Mechanism

After a certificate is validated as a properly signed certificate, a certificate revocation method is performed to ensure that the certificate has not been revoked by the issuing CA. Cisco IOS software supports two revocation mechanisms—Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP). Cisco IOS software also supports AAA integration for certificate checking; however, additional authorization functionality is included. For more information on PKI and AAA certificate authorization and status check, see the PKI and AAA Server Integration for Certificate Status section.

The following sections explain how each revocation mechanism works:

What Is a CRL

A certificate revocation list (CRL) is a list of revoked certificates. The CRL is created and digitally signed by the CA that originally issued the certificates. The CRL contains dates for when each certificate was issued and when it expires.

CAs publish new CRLs periodically or when a certificate for which the CA is responsible has been revoked. By default, a new CRL is downloaded after the currently cached CRL expires. An administrator may also configure the duration for which CRLs are cached in router memory or disable CRL caching completely. The CRL caching configuration applies to all CRLs associated with a trustpoint.

When the CRL expires, the router deletes it from its cache. A new CRL is downloaded when a certificate is presented for verification; however, if a newer version of the CRL that lists the certificate under examination is on the server but the router is still using the CRL in its cache, the router does not know that the certificate has been revoked. The certificate passes the revocation check even though it should have been denied.

When a CA issues a certificate, the CA can include in the certificate the CRL distribution point (CDP) for that certificate. Cisco IOS client devices use CDPs to locate and load the correct CRL. The Cisco IOS client supports multiple CDPs, but the Cisco IOS CA currently supports only one CDP; however, third-party vendor CAs may support multiple CDPs or different CDPs per certificate. If a CDP is not specified in the certificate, the client device uses the default Simple Certificate Enrollment Protocol (SCEP) method to retrieve the CRL. (The CDP location can be specified through the `cdp-url` command.)

When implementing CRLs, you should consider the following design considerations:

- CRL lifetimes and the security association (SA) and Internet Key Exchange (IKE) lifetimes.
- The CRL lifetime determines the length of time between CA-issued updates to the CRL. The default CRL lifetime value, which is 168 hours [1 week], can be changed through the `lifetime crl` command.
- The method of the CDP determines how the CRL is retrieved; some possible choices include HTTP, Lightweight Directory Access Protocol (LDAP), SCEP, or TFTP. HTTP, TFTP, and LDAP are the most commonly used methods. Although Cisco IOS software defaults to SCEP, an HTTP CDP is recommended for large installations using CRLs because HTTP can be made highly scalable.
- The location of the CDP determines from where the CRL is retrieved; for example, you can specify the server and file path from which to retrieve the CRL.

Querying All CDPs During Revocation Check

When a CDP server does not respond to a request, the Cisco IOS software reports an error, which may result in the peer’s certificate being rejected. To prevent a possible certificate rejection and if there are multiple
CDPs in a certificate, the Cisco IOS software will attempt to use the CDPs in the order in which they appear in the certificate. The router will attempt to retrieve a CRL using each CDP URL or directory specification. If an error occurs using a CDP, an attempt will be made using the next CDP.

Note

Prior to Cisco IOS Release 12.3(7)T, the Cisco IOS software makes only one attempt to retrieve the CRL, even when the certificate contains more than one CDP.

Tip

Although the Cisco IOS software will make every attempt to obtain the CRL from one of the indicated CDPs, it is recommended that you use an HTTP CDP server with high-speed redundant HTTP servers to avoid application timeouts because of slow CDP responses.

What Is OCSP

OCSP is an online mechanism that is used to determine certificate validity and provides the following flexibility as a revocation mechanism:

- OCSP can provide real-time certificate status checking.
- OCSP allows the network administrator to specify a central OCSP server, which can service all devices within a network.
- OCSP also allows the network administrator the flexibility to specify multiple OCSP servers, either per client certificate or per group of client certificates.
- OCSP server validation is usually based on the root CA certificate or a valid subordinate CA certificate, but may also be configured so that external CA certificates or self-signed certificates may be used. Using external CA certificates or self-signed certificates allows the OCSP servers certificate to be issued and validated from an alternative PKI hierarchy.

A network administrator can configure an OCSP server to collect and update CRLs from different CA servers. The devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every peer. When peers have to check the revocation status of a certificate, they send a query to the OCSP server that includes the serial number of the certificate in question and an optional unique identifier for the OCSP request, or a nonce. The OCSP server holds a copy of the CRL to determine if the CA has listed the certificate as being revoked; the server then responds to the peer including the nonce. If the nonce in the response from the OCSP server does not match the original nonce sent by the peer, the response is considered invalid and certificate verification fails. The dialog between the OCSP server and the peer consumes less bandwidth than most CRL downloads.

If the OCSP server is using a CRL, CRL time limitations will be applicable; that is, a CRL that is still valid might be used by the OCSP server although a new CRL has been issued by the CRL containing additional certificate revocation information. Because fewer devices are downloading the CRL information on a regular basis, you can decrease the CRL lifetime value or configure the OCSP server not to cache the CRL. For more information, check your OCSP server documentation.

When to Use an OCSP Server

OCSP may be more appropriate than CRLs if your PKI has any of the following characteristics:
• Real-time certificate revocation status is necessary. CRLs are updated only periodically and the latest CRL may not always be cached by the client device. For example, if a client does not yet have the latest CRL cached and a newly revoked certificate is being checked, that revoked certificate will successfully pass the revocation check.

• There are a large number of revoked certificates or multiple CRLs. Caching a large CRL consumes large portions of Cisco IOS memory and may reduce resources available to other processes.

• CRLs expire frequently, causing the CDP to handle a larger load of CRLs.

Note
As of Cisco IOS Release 12.4(9)T or later, an administrator may configure CRL caching, either by disabling CRL caching completely or setting a maximum lifetime for a cached CRL per trustpoint.

When to Use Certificate-Based ACLs for Authorization or Revocation

Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action.

Because certificate-based ACLs are configured on the device, they do not scale well for large numbers of ACLs; however, certificate-based ACLs do provide very granular control of specific device behavior. Certificate-based ACLs are also leveraged by additional features to help determine when PKI components such as revocation, authorization, or a trustpoint should be used. They provide a general mechanism allowing users to select a specific certificate or a group of certificates that are being validated for either authorization or additional processing.

Certificate-based ACLs specify one or more fields within the certificate and an acceptable value for each specified field. You can specify which fields within a certificate should be checked and which values those fields may or may not have.

There are six logical tests for comparing the field with the value—equal, not equal, contains, does not contain, less than, and greater than or equal. If more than one field is specified within a single certificate-based ACL, the tests of all of the fields within the ACL must succeed to match the ACL. The same field may be specified multiple times within the same ACL. More than one ACL may be specified, and ACL will be processed in turn until a match is found or all of the ACLs have been processed.

Ignore Revocation Checks Using a Certificate-Based ACL

Certificate-based ACLs can be configured to instruct your router to ignore the revocation check and expired certificates of a valid peer. Thus, a certificate that meets the specified criteria can be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does not have to be performed. You can also use a certificate-based ACL to ignore the revocation check when the communication with a AAA server is protected with a certificate.

Ignoring Revocation Lists

To allow a trustpoint to enforce CRLs except for specific certificates, enter the `match certificate` command with the `skip revocation-check` keyword. This type of enforcement is most useful in a hub-and-spoke configuration in which you also want to allow direct spoke-to-spoke connections. In pure hub-and-spoke configurations, all spokes connect only to the hub, so CRL checking is necessary only on the hub. For one spoke to communicate directly with another spoke, the `match certificate` command with the `skip`
revocation-check keyword can be used for neighboring peer certificates instead of requiring a CRL on each spoke.

Ignoring Expired Certificates

To configure your router to ignore expired certificates, enter the match certificate command with the allow expired-certificate keyword. This command has the following purposes:

- If the certificate of a peer has expired, this command may be used to "allow" the expired certificate until the peer can obtain a new certificate.
- If your router clock has not yet been set to the correct time, the certificate of a peer will appear to be not yet valid until the clock is set. This command may be used to allow the certificate of the peer even though your router clock is not set.

Note

If Network Time Protocol (NTP) is available only via the IPSec connection (usually via the hub in a hub-and-spoke configuration), the router clock can never be set. The tunnel to the hub cannot be "brought up" because the certificate of the hub is not yet valid.

- "Expired" is a generic term for a certificate that is expired or that is not yet valid. The certificate has a start and end time. An expired certificate, for purposes of the ACL, is one for which the current time of the router is outside the start and end times specified in the certificate.

Skipping the AAA Check of the Certificate

If the communication with an AAA server is protected with a certificate, and you want to skip the AAA check of the certificate, use the match certificate command with the skip authorization-check keyword. For example, if a virtual private network (VPN) tunnel is configured so that all AAA traffic goes over that tunnel, and the tunnel is protected with a certificate, you can use the match certificate command with the skip authorization-check keyword to skip the certificate check so that the tunnel can be established.

The match certificate command and the skip authorization-check keyword should be configured after PKI integration with an AAA server is configured.

Note

If the AAA server is available only via an IPSec connection, the AAA server cannot be contacted until after the IPSec connection is established. The IPSec connection cannot be "brought up" because the certificate of the AAA server is not yet valid.

PKI Certificate Chain Validation

A certificate chain establishes a sequence of trusted certificates -- from a peer certificate to the root CA certificate. Within a PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trustpoint.

When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trustpoint, is reached. In Cisco IOS Release 12.4(6)T and later releases,
an administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates.

Configuring the level to which a certificate chain is processed allows for the reauthentication of trusted certificates, the extension of a trusted certificate chain, and the completion of a certificate chain that contains a gap.

**Reauthentication of Trusted Certificates**

The default behavior is for the router to remove any trusted certificates from the certificate chain sent by the peer before the chain is validated. An administrator may configure certificate chain path processing so that the router does not remove CA certificates that are already trusted before chain validation, so that all certificates in the chain are re-authenticated for the current session.

**Extending the Trusted Certificate Chain**

The default behavior is for the router to use its trusted certificates to extend the certificate chain if there are any missing certificates in the certificate chain sent by the peer. The router will validate only certificates in the chain sent by the peer. An administrator may configure certificate chain path processing so that the certificates in the peer’s certificate chain and the router’s trusted certificates are validated to a specified point.

**Completing Gaps in a Certificate Chain**

An administrator may configure certificate chain processing so that if there is a gap in the configured Cisco IOS trustpoint hierarchy, certificates sent by the peer can be used to complete the set of certificates to be validated.

**Note**

If the trustpoint is configured to require parent validation and the peer does not provide the full certificate chain, the gap cannot be completed and the certificate chain is rejected and invalid.

**Note**

It is a configuration error if the trustpoint is configured to require parent validation and there is no parent trustpoint configured. The resulting certificate chain gap cannot be completed and the subordinate CA certificate cannot be validated. The certificate chain is invalid.

**High-Availability Support**

High-availability support for the certificate server is provided by:

- Synchronizing revoke commands with the standby certificate server
- Sending serial-number commands when new certificates are issued

The means that the standby certificate server is ready to issue certificates and certificate revocation lists (CRLs) if it becomes active.

Further high-availability support is provided by the following synchronizations with the standby:

- Certificate-server configuration
- Pending requests
Grant and reject commands

For box-to-box high availability, which does not support configuration synchronization, a basic configuration synchronization mechanism is layered over a redundancy facility.

Trustpoint configuration synchronization support.

How to Configure Authorization and Revocation of Certificates for Your PKI

Configuring PKI Integration with a AAA Server

Perform this task to generate a AAA username from the certificate presented by the peer and specify which fields within a certificate should be used to build the AAA database username.

Note

The following restrictions should be considered when using the **all** keyword as the subject name for the **authorization username** command:

- Some AAA servers limit the length of the username (for example, to 64 characters). As a result, the entire certificate subject name cannot be longer than the limitation of the server.

- Some AAA servers limit the available character set that may be used for the username (for example, a space [ ] and an equal sign [=] may not be acceptable). You cannot use the **all** keyword for a AAA server having such a character-set limitation.

- The **subject-name** command in the trustpoint configuration may not always be the final AAA subject name. If the fully qualified domain name (FQDN), serial number, or IP address of the router are included in a certificate request, the subject name field of the issued certificate will also have these components. To turn off the components, use the **fqdn**, **serial-number**, and **ip-address** commands with the **none** keyword.

- CA servers sometimes change the requested subject name field when they issue a certificate. For example, CA servers of some vendors switch the relative distinguished names (RDNs) in the requested subject names to the following order: CN, OU, O, L, ST, and C. However, another CA server might append the configured LDAP directory root (for example, O=cisco.com) to the end of the requested subject name.

- Depending on the tools you choose for displaying a certificate, the printed order of the RDNs in the subject name could be different. Cisco IOS software always displays the least significant RDN first, but other software, such as Open Source Secure Socket Layer (OpenSSL), does the opposite. Therefore, if you are configuring a AAA server with a full distinguished name (DN) (subject name) as the corresponding username, ensure that the Cisco IOS software style (that is, with the least significant RDN first) is used.

or

```
radius-server host hostname [key string]
```
SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authorization network listname [method]
5. crypto pki trustpoint name
6. enrollment [mode] [retry period minutes] [retry count number] url url [pem]
7. revocation-check method
8. exit
9. authorization username subjectname subjectname
10. authorization list listname
11. tacacs-server host hostname [key string]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td>Example: Router(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa authorization network listname [method]</td>
<td>Sets the parameters that restrict user access to a network.</td>
</tr>
<tr>
<td>• method —Can be group radius, group tacacs+, or group group-name.</td>
<td></td>
</tr>
<tr>
<td>Example: Router (config)# aaa authorization network maxaaa group tacacs+</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> crypto pki trustpoint name</td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td>Example: Route (config)# crypto pki trustpoint msc</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Step 6** | enrollment [mode] [retry period minutes] [retry count number] url url [pem]  
**Example:**  
Router (ca-trustpoint)# enrollment url http://caserver.myexample.com  
Router (ca-trustpoint)# enrollment url http://[2001:DB8:1::1]:80  
**Purpose:** Specifies the following enrollment parameters of the CA:  
|  |
| - (Optional) The **mode** keyword specifies the registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.  
- (Optional) The **retry period** keyword and **minutes** argument specifies the period, in minutes, in which the router waits before sending the CA another certificate request. Valid values are from 1 to 60. The default is 1.  
- (Optional) The **retry count** keyword and **number** argument specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. Valid values are from 1 to 100. The default is 10.  
- The **url** argument is the URL of the CA to which your router should send certificate requests.  
**Note:** With the introduction of Cisco IOS Release 15.2(1)T, an IPv6 address can be added to the http: enrolment method. For example: http://[ipv6-address]:80. The IPv6 address must be enclosed in brackets in the URL. See the enrollment url (ca-trustpoint) command page for more information on the other enrollment methods that can be used.  
|  |
| - (Optional) The **pem** keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request. |
| **Step 7** | revocation-check method  
**Example:**  
Router (ca-trustpoint)# revocation-check crl  
**Purpose:** (Optional) Checks the revocation status of a certificate. |
| **Step 8** | exit  
**Example:**  
Router (ca-trustpoint)# exit  
**Purpose:** Exits ca-trustpoint configuration mode and returns to global configuration mode. |
| **Step 9** | authorization username subjectname subjectname  
**Example:**  
Router (config)# authorization username subjectname serialnumber  
**Purpose:** Sets parameters for the different certificate fields that are used to build the AAA username.  
**The **subjectname** argument can be any of the following:**  
|  |
| - **all** -- Entire distinguished name (subject name) of the certificate.  
- **commonname** -- Certification common name.  
- **country** -- Certificate country.  
- **email** -- Certificate e-mail. |
## Configuring Authorization and Revocation of Certificates in a PKI

### Configuring PKI Integration with a AAA Server

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ipaddress --Certificate IP address.</td>
<td></td>
</tr>
<tr>
<td>• locality --Certificate locality.</td>
<td></td>
</tr>
<tr>
<td>• organization --Certificate organization.</td>
<td></td>
</tr>
<tr>
<td>• organizationalunit --Certificate organizational unit.</td>
<td></td>
</tr>
<tr>
<td>• postalcode --Certificate postal code.</td>
<td></td>
</tr>
<tr>
<td>• serialnumber --Certificate serial number.</td>
<td></td>
</tr>
<tr>
<td>• state --Certificate state field.</td>
<td></td>
</tr>
<tr>
<td>• streetaddress --Certificate street address.</td>
<td></td>
</tr>
<tr>
<td>• title --Certificate title.</td>
<td></td>
</tr>
<tr>
<td>• unstructuredname --Certificate unstructured name.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 10

**authorization list listname**

Specify the AAA authorization list.

**Example:**

```
Router (config)# authorization list maxaaa
```

### Step 11

**tacacs-server host hostname [key string]**

Specify a TACACS+ host.

**Example:**

```
Router(config)# tacacs-server host 192.0.2.2 key a_secret_key
```

**Example:**

```
radius-server host hostname [key string]
```

**Example:**

```
Router(config)# radius-server host 192.0.2.1 key another_secret_key
```

### Troubleshooting Tips

To display debug messages for the trace of interaction (message type) between the CA and the router, use the `debug crypto pki transactions` command. (See the sample output, which shows a successful PKI integration with AAA server exchange and a failed PKI integration with AAA server exchange.)
Successful Exchange

```
Router# debug crypto pki transactions
Apr 22 23:15:03.695: CRYPTO_PKI: Found a issuer match
Apr 22 23:15:03.955: CRYPTO_PKI: cert revocation status unknown.
Apr 22 23:15:03.955: CRYPTO_PKI: Certificate validated without revocation check
```

Each line that shows "CRYPTO_PKI_AAA" indicates the state of the AAA authorization checks. Each of the AAA AV pairs is indicated, and then the results of the authorization check are shown.

```
Apr 22 23:15:04.019: CRYPTO_PKI_AAA: checking AAA authorization (ipsecca_script_aaalist, PKIAAA-L, <all>)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
```

Failed Exchange

```
Router# debug crypto pki transactions
Apr 22 23:12:30.327: CRYPTO_PKI: Found a issuer match
```

```
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: parsed cert-lifetime-end as: 21:30:00
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end is expired
```

In the above failed exchange, the certificate has expired.

Configuring a Revocation Mechanism for PKI Certificate Status Checking

Perform this task to set up a CRL as the certificate revocation mechanism—CRLs or OCSP—that is used to check the status of certificates in a PKI.

The revocation-check Command

Use the `revocation-check` command to specify at least one method (OCSP, CRL, or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer’s certificate—unless you include the `none` keyword in your configuration. If the `none` keyword is configured, a revocation check will not be performed and the certificate will always be accepted.

Nonces and Peer Communications with OCSP Servers

When using OCSP, nonces, unique identifiers for OCSP requests, are sent by default during peer communications with your OCSP server. The use of nonces offers a more secure and reliable communication channel between the peer and OCSP server.

If your OCSP server does not support nonces, you may disable the sending of nonces. For more information, check your OCSP server documentation.
Before You Begin

- Before issuing any client certificates, the appropriate settings on the server (such as setting the CDP) should be configured.
- When configuring an OCSP server to return the revocation status for a CA server, the OCSP server must be configured with an OCSP response signing certificate that is issued by that CA server. Ensure that the signing certificate is in the correct format, or the router will not accept the OCSP response. See your OCSP manual for additional information.

Note

- OCSP transports messages over HTTP, so there may be a time delay when you access the OCSP server.
- If the OCSP server depends on normal CRL processing to check revocation status, the same time delay that affects CRLs will also apply to OCSP.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto pki trustpoint name
4. ocs url url
5. revocation-check method1 [method2 method3]
6. ocs disable-nonce
7. exit
8. exit
9. show crypto pki certificates
10. show crypto pki trustpoints [status | label [status]]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Revocation Mechanism for PKI Certificate Status Checking

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><code>crypto pki trustpoint name</code></td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# crypto pki trustpoint hazel</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>ocsp url url</code></td>
<td>The <code>url</code> argument specifies the URL of an OCSP server so that the trustpoint can check the certificate status. This URL overrides the URL of the OCSP server (if one exists) in the Authority Info Access (AIA) extension of the certificate. All certificates associated with a configured trustpoint are checked by the OCSP server. The URL can be a hostname, IPv4 address, or an IPv6 address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(ca-trustpoint)# ocsp url http://ocsp-server</code></td>
<td><code>- or -</code></td>
</tr>
<tr>
<td></td>
<td><code>Router(ca-trustpoint)# ocsp url http://10.10.10.1:80</code></td>
<td><code>- or -</code></td>
</tr>
<tr>
<td></td>
<td><code>Router(ca-trustpoint)# ocsp url http://2001DB8:1:1::2:80</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>revocation-check method1 [method2 method3]</code></td>
<td>Checks the revocation status of a certificate.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(ca-trustpoint)# revocation-check ocsp none</code></td>
<td></td>
</tr>
<tr>
<td><strong>Method Options:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>crl</code> --Certificate checking is performed by a CRL. This is the default option.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>none</code> --Certificate checking is ignored.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ocsp</code> --Certificate checking is performed by an OCSP server.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>ocsp disable-nonce</code></td>
<td>(Optional) Specifies that a nonce, or an OCSP request unique identifier, will not be sent during peer communications with the OCSP server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(ca-trustpoint)# ocsp disable-nonce</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(ca-trustpoint)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>exit</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Certificate Authorization and Revocation Settings

Perform this task to specify a certificate-based ACL, to ignore revocation checks or expired certificates, to manually override the default CDP location, to manually override the OCSP server setting, to configure CRL caching, or to set session acceptance or rejection based on a certificate serial number, as appropriate.

#### Configuring Certificate-Based ACLs to Ignore Revocation Checks

To configure your router to use certificate-based ACLs to ignore revocation checks and expired certificates, perform the following steps:

- Identify an existing trustpoint or create a new trustpoint to be used when verifying the certificate of the peer. Authenticate the trustpoint if it has not already been authenticated. The router may enroll with this trustpoint if you want. Do not set optional CRLs for the trustpoint if you plan to use the `match certificate` command and `skip revocation-check` keyword.

- Determine the unique characteristics of the certificates that should not have their CRL checked and of the expired certificates that should be allowed.

- Define a certificate map to match the characteristics identified in the prior step.

- You can add the `match certificate` command and `skip revocation-check` keyword and the `match certificate command` and `allow expired-certificate` keyword to the trustpoint that was created or identified in the first step.

> **Note**
> Certificate maps are checked even if the peer’s public key is cached. For example, when the public key is cached by the peer, and a certificate map is added to the trustpoint to ban a certificate, the certificate map is effective. This prevents a client with the banned certificate, which was once connected in the past, from reconnecting.
Manually Overriding CDPs in a Certificate

Users can override the CDPs in a certificate with a manually configured CDP. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate’s CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.

Manually Overriding the OCSP Server Setting in a Certificate

Administrators can override the OCSP server setting specified in the Authority Information Access (AIA) field of the client certificate or set by the issuing the \texttt{ocsp url} command. One or more OCSP servers may be manually specified, either per client certificate or per group of client certificates by the \texttt{match certificate override ocsp} command. The \texttt{match certificate override ocsp} command overrides the client certificate AIA field or the \texttt{ocsp url} command setting if a client certificate is successfully matched to a certificate map during the revocation check.

\begin{itemize}
  \item Only one OCSP server can be specified per client certificate.
\end{itemize}

Configuring CRL Cache Control

By default, a new CRL will be downloaded after the currently cached CRL expires. Administrators can either configure the maximum amount of time in minutes a CRL remains in the cache by issuing the \texttt{crl cache delete-after} command or disable CRL caching by issuing the \texttt{crl cache none} command. Only the \texttt{crl-cache delete-after} or the \texttt{crl-cache none} command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed.

Neither the \texttt{crl-cache none} command nor the \texttt{crl-cache delete-after} command affects the currently cached CRL. If you configure the \texttt{crl-cache none} command, all CRLs downloaded after this command is issued will not be cached. If you configure the \texttt{crl-cache delete-after} command, the configured lifetime will only affect CRLs downloaded after this command is issued.

This functionality is useful when a CA issues CRLs with no expiration date or with expiration dates days or weeks ahead.

Configuring Certificate Serial Number Session Control

A certificate serial number can be specified to allow a certificate validation request to be accepted or rejected by the trustpoint for a session. A session may be rejected, depending on certificate serial number session control, even if a certificate is still valid. Certificate serial number session control may be configured by using either a certificate map with the \texttt{serial-number} field or an AAA attribute, with the \texttt{cert-serial-not} command.

Using certificate maps for session control allows an administrator to specify a single certificate serial number. Using the AAA attribute allows an administrator to specify one or more certificate serial numbers for session control.

Before You Begin

\begin{itemize}
  \item The trustpoint should be defined and authenticated before attaching certificate maps to the trustpoint.
\end{itemize}
• The certificate map must be configured before the CDP override feature can be enabled or the **serial-number** command is issued.

• The PKI and AAA server integration must be successfully completed to use AAA attributes as described in "PKI and AAA Server Integration for Certificate Status."

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `crypto pki certificate map label sequence-number`
4. `field-name match-criteria match-value`
5. `exit`
6. `crypto pki trustpoint name`
7. Do one of the following:
   - `crl-cache none`
   - `crl-cache delete-after time`
8. `match certificate certificate-map-label [allow expired-certificate | skip revocation-check | skip authorization-check]`
9. `match certificate certificate-map-label override cdp {url | directory} string`
10. `match certificate certificate-map-label override ocsp [trustpoint trustpoint-label] sequence-number url ocsp-url`
11. `exit`
12. `aaa new-model`
13. `aaa attribute list list-name`
14. `attribute type \{name\} \{value\}`
15. `exit`
16. `exit`
17. `show crypto pki certificates`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Router&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

• Enter your password if prompted.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto pki certificate map label sequence-number</td>
<td>Defines values in a certificate that should be matched or not matched and enters ca-certificate-map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# crypto pki certificate map Group 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> field-name match-criteria match-value</td>
<td>Specifies one or more certificate fields together with their matching criteria and the value to match.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(ca-certificate-map)# subject-name co MyExample</td>
<td></td>
</tr>
</tbody>
</table>

**Note** Date field format is dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

The **field-name** is one of the following case-insensitive name strings or a date:

- alt-subject-name
- expires-on
- issuer-name
- name
- serial-number
- subject-name
- unstructured-subject-name
- valid-start

**Note** The **match-criteria** is one of the following logical operators:

- co --contains (valid only for name fields and serial number field)
- eq --equal (valid for name, serial number, and date fields)
- ge --greater than or equal (valid only for date fields)
- lt --less than (valid only for date fields)
- nc --does not contain (valid only for name fields and serial number field)
- ne --not equal (valid for name, serial number, and date fields)

The **match-value** is the name or date to test with the logical operator assigned by match-criteria.

**Note** Use this command only when setting up a certificate-based ACL--not when setting up a certificate-based ACL to ignore revocation checks or expired certificates.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Router(ca-certificate-map)# exit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>crypto pki trustpoint <em>name</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Declares the trustpoint, given name and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# crypto pki trustpoint Access2</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• crl-cache none</td>
</tr>
<tr>
<td></td>
<td>• crl-cache delete-after <em>time</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>(Optional) Disables CRL caching completely for all CRLs associated with the trustpoint.</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# crl-cache none</td>
</tr>
<tr>
<td></td>
<td>The <em>crl-cache none</em> command does not affect any currently cached CRLs. All CRLs downloaded after this command is configured will not be cached.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specifies the maximum time CRLs will remain in the cache for all CRLs associated with the trustpoint.</td>
</tr>
<tr>
<td></td>
<td>• <em>time</em> -- The amount of time in minutes before the CRL is deleted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The <em>crl-cache delete-after</em> command does not affect any currently cached CRLs. The configured lifetime will only affect CRLs downloaded after this command is configured.</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# crl-cache delete-after 20</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>match certificate <em>certificate-map-label</em> [allow expired-certificate] [skip revocation-check] [skip authorization-check]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>(Optional) Associates the certificate-based ACL (that was defined via the crypto pki certificate map command) to a trustpoint.</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# match certificate Group skip revocation-check</td>
</tr>
<tr>
<td></td>
<td>• <em>certificate-map-label</em> -- Must match the <em>label</em> argument specified via the crypto pki certificate map command.</td>
</tr>
<tr>
<td></td>
<td>• allow expired-certificate -- Ignores expired certificates.</td>
</tr>
<tr>
<td></td>
<td>• skip revocation-check -- Allows a trustpoint to enforce CRLs except for specific certificates.</td>
</tr>
<tr>
<td></td>
<td>• skip authorization-check -- Skips the AAA check of a certificate when PKI integration with an AAA server is configured.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>match certificate <em>certificate-map-label</em> override cdp {url</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>(Optional) Manually overrides the existing CDP entries for a certificate with a URL or directory specification.</td>
</tr>
<tr>
<td></td>
<td>Router(ca-trustpoint)# match certificate Group1 override cdp url <a href="http://server.cisco.com">http://server.cisco.com</a></td>
</tr>
<tr>
<td></td>
<td>• <em>certificate-map-label</em> -- A user-specified label that must match the <em>label</em> argument specified in a previously defined crypto pki certificate map command.</td>
</tr>
<tr>
<td></td>
<td>• url -- Specifies that the certificate's CDPs will be overridden with an HTTP or LDAP URL.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step 10</th>
<th>match certificate  certificate-map-label override ocs&lt;sup&gt;1&lt;/sup&gt;p [trustpoint trustpoint-label] sequence-number url ocs&lt;sup&gt;1&lt;/sup&gt;p-url</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(ca-trustpoint)# match certificate mycertmapname override ocs&lt;sup&gt;1&lt;/sup&gt;p trustpoint mytp 15 url <a href="http://192.0.2.2">http://192.0.2.2</a></td>
</tr>
</tbody>
</table>

*Optional* Specifies an OCSP server, either per client certificate or per group of client certificates, and may be issued more than once to specify additional OCSP servers and client certificate settings including alternative PKI hierarchies.

- **directory** -- Specifies that the certificate’s CDPs will be overridden with an LDAP directory specification.
- **string** -- The URL or directory specification.

**Note**

Some applications may time out before all CDPs have been tried and will report an error message. The error message will not affect the router, and the Cisco IOS software will continue attempting to retrieve a CRL until all CDPs have been tried.

- **certificate-map-label** -- The name of an existing certificate map.
- **trustpoint** -- The trustpoint to be used when validating the OCSP server certificate.
- **sequence-number** -- The order the match certificate override ocs<sup>1</sup>p command statements apply to the certificate being verified. Matches are performed from the lowest sequence number to the highest sequence number. If more than one command is issued with the same sequence number, it overwrites the previous OCSP server override setting.
- **url** -- The URL of the OCSP server.

When the certificate matches a configured certificate map, the AIA field of the client certificate and any previously issued ocs<sup>1</sup>p url command settings are overwritten with the specified OCSP server.

If no map-based match occurs, one of the following two cases will continue to apply to the client certificate.

- If OCSP is specified as the revocation method, the AIA field value will continue to apply to the client certificate.
- If the ocs<sup>1</sup>p url configuration exists, the ocs<sup>1</sup>p url configuration settings will continue to apply to the client certificates.

### Step 11

| exit |

**Example:**

Router(ca-trustpoint)# exit

Returns to global configuration mode.

### Step 12

| aaa new-model |

**Example:**

Router(config)# aaa new-model

(Optional) Enables the AAA access control model.
### Configuring Authorization and Revocation of Certificates in a PKI

**Configuring Certificate Authorization and Revocation Settings**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>aaa attribute list list-name</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config)# aaa attribute list crl</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><strong>attribute type {name} {value}</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-attr-list)# attribute type cert-serial-not 6C4A</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config-attr-list)# exit</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router(config)# exit</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td><strong>show crypto pki certificates</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Router# show crypto pki certificates</strong></td>
</tr>
</tbody>
</table>

**Example**

The following is a sample certificate. The OCSP-related extensions are shown using exclamation points.

```
Certificate:
  Data:
    Version: v3
    Serial Number:0x14
    Signature Algorithm:SHAwithRSA = 1.2.840.113549.1.1.4
    Issuer:CN=CA server,OU=PKI,O=Cisco Systems
```
The following example shows an excerpt of the running configuration output when adding a **match certificate override ocsp** command to the beginning of an existing sequence:

```
match certificate map3 override ocsp 5 url http://192.0.2.3/
```

The following example shows an excerpt of the running configuration output when an existing **match certificate override ocsp** command is replaced and a trustpoint is specified to use an alternative PKI hierarchy:

```
match certificate map4 override ocsp trustpoint tp4 10 url http://192.0.2.4/newvalue
```

**Troubleshooting Tips**

If you ignored revocation check or expired certificates, you should carefully check your configuration. Verify that the certificate map properly matches either the certificate or certificates that should be allowed or the
AAA checks that should be skipped. In a controlled environment, try modifying the certificate map and determine what is not working as expected.

**Configuring Certificate Chain Validation**

Perform this task to configure the processing level for the certificate chain path of your peer certificates.

**Before You Begin**

- The device must be enrolled in your PKI hierarchy.
- The appropriate key pair must be associated with the certificate.

**Note**

- A trustpoint associated with the root CA cannot be configured to be validated to the next level.

The `chain-validation` command is configured with the `continue` keyword for the trustpoint associated with the root CA, an error message will be displayed and the chain validation will revert to the default `chain-validation` command setting.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. crypto pki trustpoint name
4. chain-validation [{stop | continue} [parent-trustpoint]]
5. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Certificate Servers for High Availability

You can configure certificate servers to synchronize revoke commands and send serial-number commands when new certificates are issued, preparing the standby certificate server to issue certificates and CRLs if it becomes active.

#### Prerequisites

The following conditions must be met for high availability on certificate servers:

- IPsec-secured SCTP must be configured on both the active and the standby routers.
- For synchronization to work, the redundancy mode on the certificate servers must be set to ACTIVE/STANDBY after you configure SCTP.

This section contains the following subsections:

#### Setting Redundancy Mode on Certificate Servers to ACTIVE STANDBY

Perform this task on the active router to enable synchronization by setting the redundancy mode on the certificate servers to ACTIVE/STANDBY.
1. configure terminal
2. redundancy inter-device
3. scheme standby standby-group-name
4. exit
5. interface interface-name
6. ip address ip-address mask
7. no ip route-cache cef
8. no ip route-cache
9. standby ip ip-address
10. standby priority priority
11. standby name group-name
12. standby delay minimum [min-seconds] reload [reload-seconds]
13. Repeat Steps 1-12 on the standby router, r, configuring the interface with a different IP address from that of the active router (Step 6).
14. exit
15. exit
16. show crypto key mypubkey rsa

**SUMMARY STEPS**

1. configure terminal
2. redundancy inter-device
3. scheme standby standby-group-name
4. exit
5. interface interface-name
6. ip address ip-address mask
7. no ip route-cache cef
8. no ip route-cache
9. standby ip ip-address
10. standby priority priority
11. standby name group-name
12. standby delay minimum [min-seconds] reload [reload-seconds]
13. Repeat Steps 1-12 on the standby router, configuring the interface with a different IP address from that of the interface on the active router (Step 6).
14. exit
15. exit
16. show redundancy states
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong> redundancy inter-device</td>
<td>Configures redundancy and enters interdevice configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# redundancy inter-device</td>
</tr>
<tr>
<td><strong>Step 3</strong> scheme standby standby-group-name</td>
<td>Defines the redundancy scheme that is to be used.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-red-interdevice)# scheme standby SB</td>
</tr>
<tr>
<td>• The only supported scheme is “standby.”</td>
<td></td>
</tr>
<tr>
<td>• standby-group-name --Must match the standby name specified in the standby name interface configuration command. Also, the standby name must be the same on both routers.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits interdevice configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-red-interdevice)# exit</td>
</tr>
<tr>
<td><strong>Step 5</strong> interface interface-name</td>
<td>Configures an interface type for the router and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface gigabitethernet0/1</td>
</tr>
<tr>
<td><strong>Step 6</strong> ip address ip-address mask</td>
<td>Sets the local IP address for the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if) ip address 10.0.0.1 255.255.255.0</td>
</tr>
<tr>
<td><strong>Step 7</strong> no ip route-cache cef</td>
<td>Disables Cisco Express Forwarding operation on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# no ip route cache cef</td>
</tr>
<tr>
<td>Step 8</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>no ip route-cache</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# no ip route cache</td>
</tr>
<tr>
<td>Step 9</td>
<td>standby ip ip-address</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# standby ip 10.0.0.3</td>
</tr>
<tr>
<td>Step 10</td>
<td>standby priority priority</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# standby priority 50</td>
</tr>
</tbody>
</table>
| Step 11 | standby name group-name | Configures the name of the standby group.  
- The name specifies the HSRP group used. The HSRP group name must be unique on the router. |
| Example: | Router(config-if)# standby name SB | |
| Step 12 | standby delay minimum [ min-seconds ] reload [ reload-seconds ] | Sets a delay for HSRP group initialization as follows:  
- The minimum delay after the interface comes up before initializing the HSRP groups is 30 seconds.  
- The delay after the router has reloaded is 60 seconds. |
| Example: | Router(config-if)# standby delay minimum 30 reload 60 | |
| Step 13 | Repeat Steps 1-12 on the standby router, configuring the interface with a different IP address from that of the interface on the active router (Step 6). | -- |
| Step 14 | exit | Returns to global configuration mode. |
| Example: | Router(config-if)# exit | |
| Step 15 | exit | Returns to privileged EXEC mode. |
| Example: | Router(config)# exit | |
### Configuring SCTP on the Active and Standby Certificate Servers

Perform this task on the active router to configure SCTP on both the active and the standby certificate server.

#### SUMMARY STEPS

1. configure terminal
2. ipc zone default
3. association association-ID
4. no shutdown
5. protocol sctp
6. local-port local-port-number
7. local-ip device-real-ip-address [device-real-ip-address2]
8. exit
9. remote-port remote-port-number
10. remote-ip peer-real-ip-address
11. Repeat Steps 1 through 10 on the standby router, reversing the IP addresses of the local and remote peers specified in Steps 7 and 10.

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ipc zone default</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ipc zone default</td>
</tr>
<tr>
<td></td>
<td>Use this command to initiate the communication link between the active router and the standby router.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>association association-ID</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ipczone)# association 1</td>
</tr>
<tr>
<td>Configures an association between the two devices and enters IPC association configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>no shutdown</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ipczone-assoc)# no shutdown</td>
</tr>
<tr>
<td>Ensures that the server association is in the default (enabled) state.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>protocol sctp</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ipczone-assoc)# protocol sctp</td>
</tr>
<tr>
<td>Configures SCTP as the transport protocol and enters SCTP protocol configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>local-port local-port-number</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ipc-protocol-sctp)# local-port 5000</td>
</tr>
<tr>
<td>Defines the local SCTP port number that is used to communicate with the redundant peer and enters IPC transport SCTP local configuration mode.</td>
<td></td>
</tr>
<tr>
<td>• local-port-number -- There is not a default value. This argument must be configured for the local port to enable interdevice redundancy. Valid port values: 1 to 65535. The local port numbers should be the same as the remote port number on the peer router.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>local-ip device-real-ip-address [device-real-ip-address2]</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ipc-local-sctp)# local-ip 10.0.0.1</td>
</tr>
<tr>
<td>Defines at least one local IP address that is used to communicate with the redundant peer.</td>
<td></td>
</tr>
<tr>
<td>• The local IP addresses must match the remote IP addresses on the peer router. There can be either one or two IP addresses, which must be in global VPN routing and forwarding (VRF). A virtual IP address cannot be used.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ipc-local-sctp)# exit</td>
</tr>
<tr>
<td>Exits IPC transport - SCTP local configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>remote-port remote-port-number</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ipc-protocol-sctp)# remote-port 5000</td>
</tr>
<tr>
<td>Defines the remote SCTP port number that is used to communicate with the redundant peer and enters IPC transport SCTP remote configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**remote-port-number** -- There is not a default value. This argument must be configured for the remote port to enable interdevice redundancy. Valid port values: 1 to 65535. The remote port number should be the same as the local port number on the peer router.

**Note**

Defines a remote IP address of the redundant peer that is used to communicate with the local device.

All remote IP addresses must refer to the same device.

A virtual IP address cannot be used.

#### Step 10

**remote-ip**  peer-real-ip-address

**Example:**

```
Router(config-ipc-remote-sctp)# remote-ip 10.0.0.2
```

#### Step 11

Repeat Steps 1 through 10 on the standby router, reversing the IP addresses of the local and remote peers specified in Steps 7 and 10.

The virtual IP address (10.0.0.3) will be the same on both routers.

### Synchronizing the Active and Standby Certificate Servers

Perform this task to synchronize the active and standby servers.

#### SUMMARY STEPS

1. configure terminal
2. crypto key generate rsa general-keys redundancy label key-labe modulus modulus-size
3. exit
4. show crypto key mypubkey rsa
5. configure terminal
6. ip http server
7. crypto pki server cs-label
8. redundancy
9. no shutdown

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>crypto key generate rsa general-keys redundancy label key-labe modulus modulus-size</td>
</tr>
<tr>
<td></td>
<td>Generates an RSA key pair named HA for the certificate server.</td>
</tr>
<tr>
<td><strong>Step</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>4</strong></td>
<td><strong>show crypto key mypubkey rsa</strong></td>
</tr>
<tr>
<td><strong>5</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>6</strong></td>
<td><strong>ip http server</strong></td>
</tr>
<tr>
<td><strong>7</strong></td>
<td><strong>crypto pki server cs-label</strong></td>
</tr>
<tr>
<td><strong>8</strong></td>
<td><strong>redundancy</strong></td>
</tr>
<tr>
<td><strong>9</strong></td>
<td><strong>no shutdown</strong></td>
</tr>
</tbody>
</table>
Configuration Examples for Setting Up Authorization and Revocation of Certificates

Configuring and Verifying PKI AAA Authorization Examples

This section provides configuration examples of PKI AAA authorizations:

**Router Configuration Example**

The following `show running-config` command output shows the working configuration of a router that is set up to authorize VPN connections using the PKI Integration with AAA Server feature:

```
Router# show running-config
Building configuration...
!
version 12.3
!
hostname router7200
!
! aaa new-model

aaa authentication login default group tacacs+
! aaa authentication login no_tacacs enable
! aaa authentication ppp default group tacacs+
! aaa authorization exec ACSLab group tacacs+
! aaa authorization network ACSLab group tacacs+
! aaa accounting exec ACSLab start-stop group tacacs+
! aaa accounting network default start-stop group ACSLab
! aaa session-id common
!
ip domain name example.com
!
crypto pki trustpoint EM-CERT-SERV
! enrollment url http://192.0.2.33:80
! serial-number
! crl optional
! rsakeypair STOREVPN 2048
! auto-enroll
! authorization list ACSLab
!
crypto pki certificate chain EM-CERT-SERV
certificate 04
17311530 13060355 0403130c 454d2d43 4552542d 53455526 301e070d 30340301
31393232 30323535 5a170d03 35303131 38323230 3235355a 3030312e 300e0603
55040513 07314437 45424434 301c0609 30686488 f70d0109 02160f37 3230302d
312e6772 69c2e63f 6f683081 9f300d06 092a8648 86f70d01 01010500 30180d00
30819002 818100bd f9e873a7 df253f39 2864da14 9c2ea031 5a1203c4 92f5d6a8
7d2357a6 bcc8596f a38a9b10 47435626 d59a8f2a 123195bb be5a1e74 b1aa5ae0
5ca162ff 8c3aca4f b3ee9b27 8b031642 b618ae1b 40f2e3b4 f996befe 382c7283
3792a369 236f8661 8748a3af bc41f012 b859bd9c db4f75ee 3cee2829 704d6b8f
f9d04043 0f557072 03010001 a3573055 30250603 551d1f04 1e301c30 aa018a00
1e861468 7474703a 2f2f3e53 2e323437 2e313037 2e393330 0b060355 100f0404
03020545 03010f03 551d2304 18301680 1420fc04 cf80b1c6 f5bd6406 0af4d67f
341ae612 d1300006 092a8648 86f70d01 01040500 3818100 79e97b01 f8955108
12f42a56 2a6384bc ac8e22fe f1d6187f da5d6737 e0e241ac aaacc75d 3c74f59f
08dee5e2 0813a873 d79e0f99 d62dc20d 8e2798cd 2cd1c3ec 382505a1 3897330c
15a605a8 8a3f96d5 51043d37 e56e49df a65f43d7 46836093 9689784d 4c45d61d
ec1f160c 1abc8003 49fb11b1 da08ed6c 463e1090 f34c59e4
quit
```
Configuring Authorization and Revocation of Certificates in a PKI

Configuring and Verifying PKI AAA Authorization Examples

certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 454D2D43 4552542D 54355256 30E170D 3033132
31363231 34373432 5A170D30 36313231 35323134 3734325A 30173115 30130603
55040313 0C454D2D 43455254 2D534552 5630819F 300D0609 2A864886 F70D0101
01050003 818D0085 D2E386F5 4107116B AD3AC990 CBE84063 5FB2A6B5
quit
!
! crypto isakmp policy 10
encr aes
group 14
!
! crypto ipsec transform-set ISC_TS_1 esp-aes esp-sha-hmac
! crypto ipsec profile ISC_IPSEC_PROFILE_2
set security-association lifetime kilobytes 53000000
set security-association lifetime seconds 14400
set transform-set ISC_TS_1
!
! controller ISA 1/1
!
! interface Tunnel0
description MGRE Interface provisioned by ISC
bandwidth 10000
ip address 192.0.2.172 255.255.255.0
no ip redirects
ip mtu 1408
ip nhrp map multicast dynamic
ip nhrp network-id 101
ip nhrp holdtime 500
ip nhrp server-only
no ip split-horizon eigrp 101
tunnel source FastEthernet2/1
tunnel mode gre multipoint
tunnel key 101
tunnel protection ipsec profile ISC_IPSEC_PROFILE_2
!
interface FastEthernet2/0
ip address 192.0.2.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet2/1
ip address 192.0.2.2 255.255.255.0
duplex auto
speed auto
!
tacacs-server host 192.0.2.55 single-connection
tacacs-server directed-request
tacacs-server key company lab
!
ntp master 1
!
end
Debug of a Successful PKI AAA Authorization Example

The following `show debugging` command output shows a successful authorization using the PKI Integration with AAA Server feature:

```
Router# show debugging
General OS:
   TACACS access control debugging is on
   AAA Authentication debugging is on
   AAA Authorization debugging is on
Cryptographic Subsystem:
   Crypto PKI Trans debugging is on
Router#
May 28 19:36:11.117: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:36:12.789: CRYPTO_PKI: Found a issuer match
May 28 19:36:12.813: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com, <all>)
May 28 19:36:12.813: AAA/BIND(00000042): Bind i/f
May 28 19:36:12.813: AAA/AUTHOR (0x42): Pick method list 'ACSLab'
May 28 19:36:12.813: TPLUS: processing authorization request id 66
May 28 19:36:12.813: TPLUS: Protocol set to None .....Skipping
May 28 19:36:12.813: TPLUS: Sending AV service=pki
May 28 19:36:12.813: TPLUS: Authorization request created for 66(POD5.example.com)
May 28 19:36:12.813: TPLUS: Using server 192.0.2.55
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT/203A4628: Started 5 sec timeout
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27 bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27 bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27 bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27 bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS: Processed the reply packet
May 28 19:36:12.817: TPLUS: Processed AV cert-application=all
May 28 19:36:12.817: TPLUS: received authorization response for 66: PASS
May 28 19:36:12.817: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
May 28 19:36:12.817: CRYPTO_PKI_AAA: authorization passed
```

Debugs of a Failed PKI AAA Authorization Example

The following `show debugging` command output shows that the router is not authorized to connect using VPN. The messages are typical of those that you might see in such a situation.

In this example, the peer username was configured as not authorized, by moving the username to a Cisco Secure ACS group called VPN_Router_Disabled in Cisco Secure ACS. The router, router7200.example.com, has been configured to check with a Cisco Secure ACS AAA server prior to establishing a VPN connection to any peer.

```
Router# show debugging
General OS:
   TACACS access control debugging is on
   AAA Authentication debugging is on
   AAA Authorization debugging is on
Cryptographic Subsystem:
   Crypto PKI Trans debugging is on
Router#
```
Configuring Authorization and Revocation of Certificates in a PKI

Configuring a Revocation Mechanism Examples

This section contains the following configuration examples that can be used when specifying a revocation mechanism for your PKI:
Configuring an OCSP Server Example

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp

Specifying a CRL and Then an OCSP Server Example

The following example shows how to configure the router to download the CRL from the CDP. If the CRL is unavailable, the OCSP server that is specified in the AIA extension of the certificate will be used. If both options fail, certificate verification will also fail.

Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp

Specifying an OCSP Server Example

The following example shows how to configure your router to use the OCSP server at the HTTP URL “http://myocspserver:81.” If the server is down, the revocation check will be ignored.

Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none

Disabling Nonces in Communications with the OCSP Server Example

The following example shows communications when a nonce, or a unique identifier for the OCSP request, is disabled for communications with the OCSP server:

Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
Router(ca-trustpoint)# ocsp disable-nonce

Configuring a Hub Router at a Central Site for Certificate Revocation Checks Example

The following example shows a hub router at a central site that is providing connectivity for several branch offices to the central site.

The branch offices are also able to communicate directly with each other using additional IPSec tunnels between the branch offices.

The CA publishes CRLs on an HTTP server at the central site. The central site checks CRLs for each peer when setting up an IPSec tunnel with that peer.

The example does not show the IPSec configuration--only the PKI-related configuration is shown.
Home Office Hub Configuration

crypto pki trustpoint VPN-GW
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Central VPN Gateway
revocation-check crl

Central Site Hub Router

Router# show crypto ca certificate
Certificate
Status: Available
Certificate Serial Number: 2F62BE140000000000CA0
Certificate Usage: General Purpose
Issuer:
cn=Central Certificate Authority
o=Home Office Inc
Subject:
Name: Central VPN Gateway
cn=Central VPN Gateway
o=Home Office Inc
CRL Distribution Points:
http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
start date: 00:43:26 GMT Sep 26 2003
date: 00:53:26 GMT Sep 26 2004
renew date: 00:00:00 GMT Jan 1 1970
Associated Trustpoints: VPN-GW

CA Certificate
Status: Available
Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
Certificate Usage: Signature
Issuer:
cn=Central Certificate Authority
o=Home Office Inc
Subject:
cn=Central Certificate Authority
o=Home Office Inc
CRL Distribution Points:
http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
start date: 22:19:29 GMT Oct 31 2002
date: 22:27:27 GMT Oct 31 2017
Associated Trustpoints: VPN-GW

Trustpoint on the Branch Office Router

crypto pki trustpoint home-office
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Branch 1
revocation-check crl

A certificate map is entered on the branch office router.

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
branch1(config)# crypto pki certificate map central-site 10
branch1(config)#
The output from the `show certificate` command on the central site hub router shows that the certificate was issued by the following:

```
cn=Central Certificate Authority
o=Home Office Inc
```

These two lines are combined into one line using a comma (,) to separate them, and the original lines are added as the first criteria for a match.

```
Router (ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home Office Inc
```

The above line wrapped but should be shown on one line with the line above it.

The same combination is done for the subject name from the certificate on the central site router (note that the line that begins with "Name:" is not part of the subject name and must be ignored when creating the certificate map criteria). This is the subject name to be used in the certificate map.

```
Router (ca-certificate-map)# subject-name eq cn=central vpn gateway, o=home office inc
```

Now the certificate map is added to the trustpoint that was configured earlier.

```
Router (ca-certificate-map)# crypto pki trustpoint home-office
Router (ca-trustpoint)# match certificate central-site skip revocation-check
Router (ca-trustpoint)# exit
Router (config)# exit
```

The configuration is checked (most of configuration is not shown).

```
Router# write term
```

```
crypto pki trustpoint home-office
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Branch 1
  revocation-check crl
  match certificate central-site skip revocation-check

crypto pki certificate map central-site 10
  issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
  subject-name eq cn = central vpn gateway, o = home office inc
```

Note that the issuer-name and subject-name lines have been reformatted to make them consistent for later matching with the certificate of the peer.

If the branch office is checking the AAA, the trustpoint will have lines similar to the following:

```
crypto pki trustpoint home-office
  auth list allow_list
  auth user subj Commonname
```

After the certificate map has been defined as was done above, the following command is added to the trustpoint to skip AAA checking for the central site hub.

```
machine certificate central-site skip authorization-check
```

In both cases, the branch site router has to establish an IPsec tunnel to the central site to check CRLs or to contact the AAA server. However, without the `match certificate` command and `central-site skip authorization-check` (argument and keyword), the branch office cannot establish the tunnel until it has
checked the CRL or the AAA server. (The tunnel will not be established unless the match certificate command and central-site skip authorization-check argument and keyword are used.)

The match certificate command and allow expired-certificate keyword would be used at the central site if the router at a branch site had an expired certificate and it had to establish a tunnel to the central site to renew its certificate.

Trustpoint on the Central Site Router

crypto pki trustpoint VPN-GW
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc, cn=Central VPN Gateway
  revocation-check crl

Trustpoint on the Branch 1 Site Router

Router# show crypto ca certificate
Certificate
  Status: Available
  Certificate Serial Number: 2F62BE140000000000000CA0
  Certificate Usage: General Purpose
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    Name: Branch 1 Site
    cn=Branch 1 Site
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 00:43:26 GMT Sep 26 2003
    end date: 00:53:26 GMT Oct 3 2003
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: home-office
CA Certificate
  Status: Available
  Certificate Serial Number: 1244325DE036080465F977A18F61CA8
  Certificate Usage: Signature
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    cn=Central Certificate Authority
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end date: 22:27:27 GMT Oct 31 2017
  Associated Trustpoints: home-office

A certificate map is entered on the central site router.

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# crypto pki certificate map branch1 10
Router (ca-certificate-map)# issuer-name eq cn=Central Certificate Authority, ou=Home Office Inc
!The above line wrapped but should be part of the line above it.
Router (ca-certificate-map)# subject-name eq cn=Branch 1 Site, o=home office inc
The certificate map is added to the trustpoint.

Router (ca-certificate-map)# crypto pki trustpoint VPN-GW
Router (ca-trustpoint)# match certificate branch1 allow expired-certificate
Router (ca-trustpoint)# exit
Router (config) # exit

The configuration should be checked (most of the configuration is not shown).

Router# write term
!many lines left out
crypto pki trustpoint VPN-GW
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Central VPN Gateway
  revocation-check crl
  match certificate branch1 allow expired-certificate

crypto pki certificate map central-site 10
  issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
  subject-name eq cn = central vpn gateway, o = home office inc
  many lines left out

The match certificate command and branch1 allow expired-certificate (argument and keyword) and the certificate map should be removed as soon as the branch router has a new certificate.

Configuring Certificate Authorization and Revocation Settings Examples

This section contains the following configuration examples that can be used when specifying a CRL cache control setting or certificate serial number session control:

Configuring CRL Cache Control

The following example shows how to disable CRL caching for all CRLs associated with the CA1 trustpoint:

crypto pki trustpoint CA1
  enrollment url http://CA1:80
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
  revocation-check crl
  crl-cache none

The current CRL is still cached immediately after executing the example configuration shown above:

Router# show crypto pki crls

CRL Issuer Name:
  cn-name Cert Manager,ou-pki,o-example.com,c-US
  LastUpdate: 18:57:42 GMT Nov 26 2005
  NextUpdate: 22:57:42 GMT Nov 26 2005
  Retrieved from CRL Distribution Point:
    ldap://ldap.example.com/CN=CA1_Manager,O=example.com

When the current CRL expires, a new CRL is then downloaded to the router at the next update. The crl-cache none command takes effect and all CRLs for the trustpoint are no longer cached; caching is disabled. You can verify that no CRL is cached by executing the show crypto pki crls command. No output will be shown because there are no CRLs cached.
The following example shows how to configure the maximum lifetime of 2 minutes for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
enrollment url http://CA1:80
ip-address FastEthernet0/0
crl query ldap://ldap_CA1
revocation-check crl
crl-cache delete-after 2
```

The current CRL is still cached immediately after executing the example configuration above for setting the maximum lifetime of a CRL:

```
Router# show crypto pki crls

CRL Issuer Name: cn=name Cert Manager,ou=pki,o=example.com,c=US
LastUpdate: 18:57:42 GMT Nov 26 2005
NextUpdate: 22:57:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point: ldap://ldap.example.com/CN=name Cert Manager,O=example.com
```

When the current CRL expires, a new CRL is downloaded to the router at the next update and the `crl-cache delete-after` command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after a maximum lifetime of 2 minutes. You can verify that the CRL will be cached for 2 minutes by executing the `show crypto pki crls` command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.

```
Router# show crypto pki crls

CRL Issuer Name: cn=name Cert Manager,ou=pki,o=example.com,c=US
LastUpdate: 22:57:42 GMT Nov 26 2005
NextUpdate: 22:59:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point: ldap://ldap.example.com/CN=name Cert Manager,O=example.com
```

**Configuring Certificate Serial Number Session Control**

The following example shows the configuration of certificate serial number session control using a certificate map for the CA1 trustpoint:

```
crypto pki trustpoint CA1
enrollment url http://CA1
chain-validation stop
crl query ldap://ldap_server
revocation-check crl
match certificate crl
!
crypto pki certificate map crl 10
serial-number co 279d
```

**Note**

If the `match-criteria` value is set to `eq` (equal) instead of `co` (contains), the serial number must match the certificate map serial number exactly, including any spaces.

The following example shows the configuration of certificate serial number session control using AAA attributes. In this case, all valid certificates will be accepted if the certificate does not have the serial number "4ACA."

```
crypto pki trustpoint CA1
```
The server log shows that the certificate with the serial number “4ACA” was rejected. The certificate rejection is shown using exclamation points.

Configuring Certificate Chain Validation Examples

This section contains the following configuration examples that can be used to specify the level of certificate chain processing for your device certificates:

Configuring Certificate Chain Validation from Peer to Root CA

In the following configuration example, all of the certificates will be validated--the peer, SubCA11, SubCA1, and RootCA certificates.

crypto pki trustpoint RootCA
enrollment terminal
chain-validation stop
Configuring Certificate Chain Validation from Peer to Subordinate CA

In the following configuration example, the following certificates will be validated--the peer and SubCA1 certificates.

```conf
crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
rsa keypair RootCA
crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
rsa keypair SubCA1
```

Configuring Certificate Chain Validation Through a Gap

In the following configuration example, SubCA1 is not in the configured Cisco IOS hierarchy but is expected to have been supplied in the certificate chain presented by the peer.

If the peer supplies the SubCA1 certificate in the presented certificate chain, the following certificates will be validated--the peer, SubCA1, and SubCA1 certificates.

If the peer does not supply the SubCA1 certificate in the presented certificate chain, the chain validation will fail.

```conf
crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
rsa keypair RootCA
crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
rsa keypair SubCA1
```

Configuring Certificate Servers for High Availability Example

The following example shows the configuration of SCTP and redundancy on the active and the standby certificate server, and activation of synchronization between them:
On the Active Router

ipc zone default
association 1
no shutdown
protocol sctp
local-port 5000
local-ip 10.0.0.1
exit
remote-port 5000
remote-ip 10.0.0.2

On the Standby Router

ipc zone default
association 1
no shutdown
protocol sctp
local-port 5000
local-ip 10.0.0.2
exit
remote-port 5000
remote-ip 10.0.0.1

On the Active Router

redundancy inter-device
scheme standby SB
interface GigabitEthernet0/1
ip address 10.0.0.1 255.255.255.0
no ip route-cache cef
no ip route-cache
standby 0 ip 10.0.0.3
standby 0 priority 50
standby 0 name SB
standby delay min 30 reload 60

On the Standby Router

redundancy inter-device
scheme standby SB
interface GigabitEthernet0/1
ip address 10.0.0.2 255.255.255.0
no ip route-cache cef
no ip route-cache
standby 0 ip 10.0.0.3
standby 0 priority 50
standby 0 name SB
standby delay min 30 reload 60

On the Active Router

crypto pki server mycertsaver
crypto pki server mycertsaver redundancy
### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td><em>Cisco IOS Security Command Reference</em></td>
</tr>
<tr>
<td>Overview of PKI, including RSA keys, certificate enrollment, and CAs</td>
<td>“Cisco IOS PKI Overview: Understanding and Planning a PKI” module</td>
</tr>
<tr>
<td>RSA key generation and deployment</td>
<td>“Deploying RSA Keys Within a PKI” module</td>
</tr>
<tr>
<td>Certificate enrollment: supported methods, enrollment profiles, configuration tasks</td>
<td>“Configuring Certificate Enrollment for a PKI” module</td>
</tr>
<tr>
<td>Cisco IOS certificate server overview information and configuration tasks</td>
<td>“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment ” module</td>
</tr>
<tr>
<td>Recommended cryptographic algorithms</td>
<td><em>Next Generation Encryption</em></td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

### Feature Information for Certificate Authorization and Revocation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Table 2: Feature Information for PKI Certificate Authorization and Revocation

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Cache Control Enhancements for Certification Revocation Lists | 12.4(9)T  | This feature provides users the ability to disable CRL caching or to specify the maximum lifetime for which a CRL will be cached in router memory. It also provides functionality to configure certificate serial number session control.  
The following sections provide information about this feature:  
  • What Is a CRL, on page 5  
  • Configuring Certificate Authorization and Revocation Settings, on page 17  
  • Configuring SCTP on the Active and Standby Certificate Servers, on page 30  
The following commands were introduced or modified by this feature: crl-cache delete-after, crl-cache none, crypto pki certificate map |
### Feature Information

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Certificate-Complete Chain Validation           | 12.4(6)T | This feature provides users the ability to configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates. The following sections provide information about this feature:  
  - PKI Certificate Chain Validation, on page 8  
  - Configuring Certificate Chain Validation, on page 25  
  - Configuring Certificate Chain Validation Examples, on page 44  
  The following command was introduced by this feature: chain-validation |
| OCSP - Server Certification from Alternate Hierarchy | 12.4(6)T | This feature provides users with the flexibility to specify multiple OCSP servers, either per client certificate or per group of client certificates, and provides the capability for OCSP server validation based on external CA certificates or self-signed certificates.  
  The following sections provide information about this feature:  
  - What Is OCSP, on page 6  
  - Configuring Certificate Authorization and Revocation Settings, on page 17  
  The following command was introduced by this feature: match certificate override ocs
### Feature Information

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Optional OCSP Nonce           | 12.2(33)SR 12.4(4)T | This feature provides users with the ability to configure the sending of a nonce, or unique identifier for an OCSP request, during OCSP communications. The following sections provide information about this feature:  
  - What Is OCSP, on page 6  
  - Configuring a Revocation Mechanism for PKI Certificate Status Checking, on page 14  
  - Disabling Nonces in Communications with the OCSP Server Example, on page 38 |
Under the IPSec protocol, CA interoperability permits Cisco IOS devices and a CA to communicate so that the Cisco IOS device can obtain and use digital certificates from the CA. Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action. This feature adds fields to the certificate that allow specifying an ACL, creating a certificate-based ACL.

The following sections provide information about this feature:

- **When to Use Certificate-Based ACLs for Authorization or Revocation**, on page 7
- **Configuring Certificate Authorization and Revocation Settings**, on page 17

The following commands were introduced or modified by this feature: `crypto pki certificate map`, `crypto pki trustpoint match certificate`
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Online Certificate Status Protocol (OCSP)               | 12.3(2)T | This feature allows users to enable OCSP instead of CRLs to check certificate status. Unlike CRLs, which provide only periodic certificate status, OCSP can provide timely information regarding the status of a certificate. The following sections provide information about this feature:  
  - CRLs or OCSP Server Choosing a Certificate Revocation Mechanism, on page 5  
  - Configuring a Revocation Mechanism for PKI Certificate Status Checking, on page 14  
  The following commands were introduced by this feature: `ocsp url, revocation-check` |
| PKI AAA Authorization Using the Entire Subject Name     | 12.3(11)T| This feature provides users with the ability to query the AAA server using the entire subject name from the certificate as a unique AAA username. The following sections provide information about this feature:  
  - Attribute-Value Pairs for PKI and AAA Server Integration, on page 4  
  - Configuring PKI Integration with a AAA Server, on page 10  
  The following command was modified by this feature: `authorization username` |
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| PKI Integration with AAA Server | 12.3(1)  | This feature provides additional scalability for authorization by generating a AAA username from the certificate presented by the peer. A AAA server is queried to determine whether the certificate is authorized for use by the internal component. The authorization is indicated by a component-specified label that must be present in the AV pair for the user. The following sections provide information about this feature:  
• PKI and AAA Server Integration for Certificate Status, on page 3  
• Configuring PKI Integration with a AAA Server, on page 10  
The following commands were introduced by this feature:  
authorization list, authorization username |
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| PKI: Query Multiple Servers During Certificate Revocation Check               | 12.3(7)T| This feature introduces the ability for Cisco IOS software to make multiple attempts to retrieve the CRL, allowing operations to continue when a particular server is not available. In addition, the ability to override the CDPs in a certificate with a manually configured CDP has been introduced. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate’s CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP. The following sections provide information about this feature:  
- Querying All CDPs During Revocation Check, on page 5  
- Manually Overriding CDPs in a Certificate, on page 18 |

The following command was introduced by this feature: `match certificate override cdp`
### Feature Information

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Using Certificate ACLs to Ignore Revocation Check and Expired Certificates | 12.3(4)T | This feature allows a certificate that meets specified criteria to be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does not have to be performed. Certificate ACLs are used to specify the criteria that the certificate must meet to be accepted or to avoid revocation checking. In addition, if AAA communication is protected by a certificate, this feature provides for the AAA checking of the certificate to be ignored. The following sections provide information about this feature:

- Ignore Revocation Checks Using a Certificate-Based ACL, on page 7
- Configuring Certificate-Based ACLs to Ignore Revocation Checks, on page 17

The following command was modified by this feature: `match certificate`

| Query Mode Definition Per Trustpoint | Cisco IOS XE Release 2.1 | This feature was introduced on the Cisco ASR 1000 series routers.

<p>| PKI High Availability | 15.0(1)M | The following commands were introduced or modified: <code>crypto pki server</code>, <code>crypto pki server start</code>, <code>crypto pki server stop</code>, <code>crypto pki trustpoint</code>, <code>crypto key generate rsa</code>, <code>crypto key import pem</code>, <code>crypto key move rsa</code>, <code>show crypto key mypubkey rsa</code>. |</p>
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI IPv6 Support for VPN Solutions</td>
<td>15.2(1)T</td>
<td>The <strong>enrollment url (ca-trustpoint)</strong> command was modified to specify an IPv6 address in the CA URL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The <strong>ocsp url</strong> command was modified to specify the IPv6 address in a URL for the OCSP server.</td>
</tr>
</tbody>
</table>