Configuring Authorization and Revocation of Certificates in a PKI

Last Updated: July 18, 2012

This module describes how to configure authorization and revocation of certificates in a public key infrastructure (PKI).

• Finding Feature Information, page 1
• Prerequisites for Authorization and Revocation of Certificates, page 1
• Information About Authorization and Revocation of Certificates, page 2
• How to Configure Authorization and Revocation of Certificates for Your PKI, page 9
• Configuration Examples for Setting Up Authorization and Revocation of Certificates, page 26
• Additional References, page 38
• Feature Information for Certificate Authorization and Revocation, page 39

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 certification 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 pki” CLI Change

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.

Information About Authorization and Revocation of Certificates

- PKI Authorization, page 2
- PKI and AAA Server Integration for Certificate Status, page 3
- CRLs or OCSP Server Choosing a Certificate Revocation Mechanism, page 4
- When to Use Certificate-Based ACLs for Authorization or Revocation, page 7
- PKI Certificate Chain Validation, page 8
- PKI High Availability Support, page 9

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
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, page 3
• Attribute-Value Pairs for PKI and AAA Server Integration, page 3

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>
<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 “all” and “none.”</td>
</tr>
<tr>
<td>cisco-avpair=pki:cert-trustpoint=msca</td>
<td>The value is a Cisco IOS XE command-line interface (CLI) configuration trustpoint label. Note: The cert-trustpoint AV pair is normally optional. If it is specified, the Cisco IOS XE 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=16318DB7000100001671</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 XE 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, page 5
- What Is OCSP, page 6

**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, page 5**

When a CDP server does not respond to a request, the Cisco IOS XE 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 XE 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.
Although the Cisco IOS XE 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 XE memory and may reduce resources available to other processes.
- CRLs expire frequently, causing the CDP to handle a larger load of CRLs.
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, page 7

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 XE Release 2.1 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 XE 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.

PKI High Availability Support

High Availability (HA) support is provided for the client-side PKI only. There is no CA server support. Route processor to route processor redundancy and Stateful Switchover (SSO) are supported. In Service Software Upgrade (ISSU) and box-to-box HA are not supported.

How to Configure Authorization and Revocation of Certificates for Your PKI

• Configuring PKI Integration with a AAA Server, page 9
• Configuring a Revocation Mechanism for PKI Certificate Status Checking, page 14
• Configuring Certificate Authorization and Revocation Settings, page 17
• Configuring Certificate Chain Validation, page 25

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.
How to Configure Authorization and Revocation of Certificates for Your PKI

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authorization network listname [method]
5. crypto pki trustpoint name
6. enrollment url url
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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| 2    | configure terminal | Enters global configuration mode. |
| 3    | aaa new-model     | Enables the AAA access control model. |
| 4    | aaa authorization network listname [method] | Sets the parameters that restrict user access to a network.  
  - *method* --Can be group radius, group tacacs+, or group group-name. |
| 5    | crypto pki trustpoint name | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode. |
| 6    | enrollment url url | Specifies the enrollment parameters of your CA.  
  - The *url* argument is the URL of the CA to which your router should send certificate requests. |
| 7    | revocation-check method | (Optional) Checks the revocation status of a certificate. |
### Configuring PKI Integration with a AAA Server

**How to Configure Authorization and Revocation of Certificates for Your PKI**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits ca-trustpoint configuration mode and returns to global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

Router (ca-trustpoint)# exit

<table>
<thead>
<tr>
<th><strong>Step 9</strong> authorization username subjectname subjectname</th>
<th>Sets parameters for the different certificate fields that are used to build the AAA username.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router (config)# authorization username subjectname</td>
<td></td>
</tr>
<tr>
<td>subjectname serialnumber</td>
<td></td>
</tr>
</tbody>
</table>

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.
- `ipaddress` -- Certificate IP address.
- `locality` -- Certificate locality.
- `organization` -- Certificate organization.
- `organizationalunit` -- Certificate organizational unit.
- `postalcode` -- Certificate postal code.
- `serialnumber` -- Certificate serial number.
- `state` -- Certificate state field.
- `streetaddress` -- Certificate street address.
- `title` -- Certificate title.
- `unstructuredname` -- Certificate unstructured name.

<table>
<thead>
<tr>
<th><strong>Step 10</strong> authorization list listname</th>
<th>Specifies the AAA authorization list.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router (config)# authorization list</td>
<td></td>
</tr>
<tr>
<td>maxaaa</td>
<td></td>
</tr>
</tbody>
</table>
Command or Action | Purpose
---|---
**Step 11** tacacs-server host *hostname* [key *string*]  
Example:  
or  
Example:  
radius-server host *hostname* [key *string*]  
Example:  
or  
Example:  

- **Troubleshooting Tips, page 13**

**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_aalist, 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")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "15DE")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: authorization passed
Apr 22 23:12:30.327: CRYPTO_PKI: Found a issuer match
```
Failed Exchange

Router# debug crypto pki transactions
Apr 22 23:11:13.703: CRYPTO_PKI_AAA: checking AAA authorization -
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: reply attribute ("cert-serial" = "233D")
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, page 14
- Nonces and Peer Communications with OCSP Servers, page 14

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 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.
• 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. `ocsp url url`
5. `revocation-check method1 [method2 method3]`
6. `ocsp 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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto pki trustpoint name</td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
## Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th><strong>ocsp url&lt;html&gt;$url&lt;/html&gt;</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# ocsp url <a href="http://ocsp-server">http://ocsp-server</a></td>
</tr>
</tbody>
</table>

(Optional) Specifies the URL of an OCSP server so that the trustpoint can check the certificate status. This URL will override the URL of the OCSP server (if one exists) in the Authority Info Access (AIA) extension of the certificate.

<table>
<thead>
<tr>
<th>Step 5</th>
<th><strong>revocation-check method1 [method2 method3]</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# revocation-check ocsp none</td>
</tr>
</tbody>
</table>

Checks the revocation status of a certificate.
- **crl** --Certificate checking is performed by a CRL. This is the default option.
- **none** --Certificate checking is ignored.
- **ocsp** --Certificate checking is performed by an OCSP server.

If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.

<table>
<thead>
<tr>
<th>Step 6</th>
<th><strong>ocsp disable-nonce</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# ocsp disable-nonce</td>
</tr>
</tbody>
</table>

(Optional) Specifies that a nonce, or an OCSP request unique identifier, will not be sent during peer communications with the OCSP server.

<table>
<thead>
<tr>
<th>Step 7</th>
<th><strong>exit</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# exit</td>
</tr>
</tbody>
</table>

Returns to global configuration mode.

<table>
<thead>
<tr>
<th>Step 8</th>
<th><strong>exit</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>

Returns to privileged EXEC mode.

<table>
<thead>
<tr>
<th>Step 9</th>
<th><strong>show crypto pki certificates</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router# show crypto pki certificates</td>
</tr>
</tbody>
</table>

(Optional) Displays information about your certificates.
### 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, page 17
- Manually Overriding CDPs in a Certificate, page 17
- Manually Overriding the OCSP Server Setting in a Certificate, page 18
- Configuring CRL Cache Control, page 18
- Configuring Certificate Serial Number Session Control, page 18
- Examples, page 24
- Troubleshooting Tips, page 25

### 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 `ocsp-url` command. One or more OCSP servers may be manually specified, either per client certificate or per group of client certificates by the `match certificate override ocsp` command. The `match certificate override ocsp` command overrides the client certificate AIA field or the `ocsp-url` command setting if a client certificate is successfully matched to a certificate map during the revocation check.

Note

Only one OCSP server can be specified per client certificate.

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 `crl-cache delete-after` command or disable CRL caching by issuing the `crl-cache none` command. Only the `crl-cache delete-after` command or the `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 `crl-cache none` command nor the `crl-cache delete-after` command affects the currently cached CRL. If you configure the `crl-cache none` command, all CRLs downloaded after this command is issued will not be cached. If you configure the `crl-cache delete-after` command, the configured lifetime will only affect CRLs downloaded after this command is issued.

This functionality is useful is 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 `serial-number` field or an AAA attribute, with the `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.

• The trustpoint should be defined and authenticated before attaching certificate maps to the trustpoint.
• 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, page 3.”
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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>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:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</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></td>
<td></td>
</tr>
<tr>
<td>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></td>
<td></td>
</tr>
<tr>
<td>Router(ca-certificate-map)# subject-name co MyExample</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The field-name is one of the following case-insensitive name strings or a date:</td>
</tr>
<tr>
<td></td>
<td>• alt-subject-name</td>
</tr>
<tr>
<td></td>
<td>• expires-on</td>
</tr>
<tr>
<td></td>
<td>• issuer-name</td>
</tr>
<tr>
<td></td>
<td>• name</td>
</tr>
<tr>
<td></td>
<td>• serial-number</td>
</tr>
<tr>
<td></td>
<td>• subject-name</td>
</tr>
<tr>
<td></td>
<td>• unstructured-subject-name</td>
</tr>
<tr>
<td></td>
<td>• valid-start</td>
</tr>
<tr>
<td><strong>Note</strong> Date field format is dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The match-criteria is one of the following logical operators:</td>
</tr>
<tr>
<td></td>
<td>• co --contains (valid only for name fields and serial number field)</td>
</tr>
<tr>
<td></td>
<td>• eq --equal (valid for name, serial number, and date fields)</td>
</tr>
<tr>
<td></td>
<td>• ge --greater than or equal (valid only for date fields)</td>
</tr>
<tr>
<td></td>
<td>• lt --less than (valid only for date fields)</td>
</tr>
<tr>
<td></td>
<td>• nc --does not contain (valid only for name fields and serial number field)</td>
</tr>
<tr>
<td></td>
<td>• ne --not equal (valid for name, serial number, and date fields)</td>
</tr>
<tr>
<td></td>
<td>The match-value is the name or date to test with the logical operator assigned by match-criteria.</td>
</tr>
<tr>
<td><strong>Note</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(ca-certificate-map)# exit</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 6**  
**crypto pki trustpoint name**

**Example:**

Router(config)# crypto pki trustpoint Access2

**Purpose:** Declares the trustpoint, given name and enters ca-trustpoint configuration mode.

**Step 7**  
Do one of the following:

- **crl-cache none**
- **crl-cache delete-after time**

**Example:**

Router(config)# crypto pki trustpoint Access2

**Purpose:** (Optional) Disables CRL caching completely for all CRLs associated with the trustpoint.

The **crl-cache none** command does not affect any currently cached CRLs. All CRLs downloaded after this command is configured will not be cached.

(Optional) Specifies the maximum time CRLs will remain in the cache for all CRLs associated with the trustpoint.

- **time** -- The amount of time in minutes before the CRL is deleted.

The **crl-cache delete-after** command does not affect any currently cached CRLs. The configured lifetime will only affect CRLs downloaded after this command is configured.

**Step 8**

**match certificate certificate-map-label**

[allow expired-certificate] | [skip revocation-check] | [skip authorization-check]

**Example:**

Router(config)# match certificate certificate-map-label allow expired-certificate

**Purpose:** (Optional) Associates the certificate-based ACL (that was defined via the **crypto pki certificate map** command) to a trustpoint.

- **certificate-map-label** -- Must match the label argument specified via the **crypto pki certificate map** command.
- **allow expired-certificate** -- Ignores expired certificates.
- **skip revocation-check** -- Allows a trustpoint to enforce CRLs except for specific certificates.
- **skip authorization-check** -- Skips the AAA check of a certificate when PKI integration with an AAA server is configured.
### Command or Action

**Step 9**
```plaintext
match certificate certificate-map-label override cdp url | directory string
```

**Example:**
```plaintext
Router(ca-trustpoint)# match certificate Group1 override cdp url http://server.cisco.com
```

**Purpose**
(Optional) Manually overrides the existing CDP entries for a certificate with a URL or directory specification.
- `certificate-map-label` -- A user-specified label that must match the `label` argument specified in a previously defined `crypto pki certificate map` command.
- `url` -- Specifies that the certificate’s CDPs will be overridden with an HTTP or LDAP URL.
- `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 XE software will continue attempting to retrieve a CRL until all CDPs have been tried.

**Step 10**
```plaintext
match certificate certificate-map-label override ocs p [trustpoint trustpoint-label] sequence-number url ocs p-url
```

**Example:**
```plaintext
Router(ca-trustpoint)# match certificate mycertmapname override ocs p trustpoint mytp 15 url http:// 192.0.2.2
```

**Purpose**
(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.
- `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 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 `ocsp 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 `ocsp url` configuration exists, the `ocsp url` configuration settings will continue to apply to the client certificates.

**Step 11**
```plaintext
exit
```

**Example:**
```plaintext
Router(ca-trustpoint)# exit
```

Returns to global configuration mode.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 12</strong> aaa new-model</td>
<td>(Optional) Enables the AAA access control model.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> aaa attribute list list-name</td>
<td>(Optional) Defines an AAA attribute list locally on a router and enters config-attr-list configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# aaa attribute list crl</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> attribute type name value</td>
<td>(Optional) Defines an AAA attribute type that is to be added to an AAA attribute list locally on a router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-attr-list)# attribute type cert-serial-not 6C4A</td>
<td>To configure certificate serial number session control, an administrator may specify a specific certificate in the value field to be accepted or rejected based on its serial number where name is set to cert-serial-not. If the serial number of the certificate matches the serial number specified by the attribute type setting, the certificate will be rejected. For a full list of available AAA attribute types, execute the show aaa attributes command.</td>
</tr>
<tr>
<td><strong>Step 15</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-attr-list)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> exit</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong> show crypto pki certificates</td>
<td>(Optional) Displays the components of the certificates installed on the router if the CA certificate has been authenticated.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show crypto pki certificates</td>
<td></td>
</tr>
</tbody>
</table>
Examples

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

Certificate:
Data:
   Version: v3
   Serial Number: 0x14
   Signature Algorithm: MD5withRSA - 1.2.840.113549.1.1.4
   Issuer: CN=CA server, OU=PKI, O=Cisco Systems
   Validity:
      Not Before: Thursday, August 8, 2002 4:38:05 PM PST
      Not After: Tuesday, August 7, 2003 4:38:05 PM PST
   Subject: CN=OCSP server, OU=PKI, O=Cisco Systems
   Subject Public Key Info:
      Algorithm: RSA - 1.2.840.113549.1.1.1
      Public Key:
         Exponent: 65537
         Public Key Modulus: (1024 bits): <snip>
   Extensions:
      Identifier: Subject Key Identifier - 2.5.29.14
      Critical: no
      Key Identifier: <snip>
      Identifier: Authority Key Identifier - 2.5.29.35
      Critical: no
      Key Identifier: <snip>
      Identifier: OCSP NoCheck: - 1.3.6.1.5.5.7.48.1.5
      Critical: no
      Identifier: Extended Key Usage: - 2.5.29.37
      Critical: no
      Extended Key Usage:
         OCSPSigning
      !
      Identifier: CRL Distribution Points - 2.5.29.31
      Critical: no
      Number of Points: 1
      Distribution Point:
         [URIName: ldap:// CA-server/ CN= CA server, OU= PKI, O= Cisco Systems]
      Signature:
         Algorithm: MD5withRSA - 1.2.840.113549.1.1.4
         Signature: <snip>

The following example shows an excerpt of the running configuration output when adding a **match certificate override ocs p** command to the beginning of an existing sequence:

```
match certificate map3 override ocs p 5 url http://192.0.2.3/
show running-configuration
```

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

```
match certificate map4 override ocs p trustpoint tp4 10 url http://192.0.2.4/newvalue
show running-configuration
```
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.

- 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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

**Example:**

Router> enable
### Configuration Examples for Setting Up Authorization and Revocation of Certificates

#### Examples Configuring and Verifying PKI AAA Authorization

**Example Router Configuration**

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
```
Examples Configuring and Verifying PKI AAA Authorization

Example Router Configuration

hostname router7200

!  aa 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 1024
    auto-enroll
    authorization list ACSLab
!
  crypto pki certificate chain EM-CERT-SERV
    certificate 04
    30820207 03020107 A030201D A020101D 02020104 00000000 2A864886 F70D0101 04050030
    17311530 13060355 0403130C 454204D3 4552542D 53455256 3001170D 30340301
    31393232 30323535 5A170D30 35303131 38322330 3235355A 3033032E 300E0603
    55040513 07311443 45424434 30010609 2A864886 F70D0109 01260F37 3230320D
    312E6772 696CE63 6F6D0301 9F30DD06 092A6648 86F70D01 01010500 03318D00
    30018901 25400001 3F8837AA D92F510A 9C2F890F 324D86A8
    7D2357A6 BCC5596F A8EB9108 4743562E D9A8F2A 123195BB 3E3E7A4E 1B18AA20
    5C4A62FF 83CA4AF 3B3E9F27 B031642D 681AEB18 40F2E3B4 F96B6EF 382C7823
    3792A369 236F8561 874BA33F BC41F012 B559D9C4 DB4F756E 3CE2E829 704BD68F
    FD904043 05F55702 03010001 A3573505 30250003 551D1F04 1E301C80 1AA80A80
    16861468 7474703A 225F6333 2E323437 3E133037 2E393300 08603550 1DF04040
    02005A0 301F0603 551D2304 18301680 1420FC4B CF0B1C4F D784F516 DA6B50C4 7B3C3BC9
    589223AB 9F9A0D1C 04F74E2F A2EE8E8F 5E3F8A97 2F8090F7 3889E6A1 2C7266C9
    54A29870 7E7636FF 3C0F1D90 1F5A73C7 FF3F0D30 9E486C44 2A3E5495 CD0738BB
    E99DE981 E7338B68 A01B6C80 A04860D7 D34B38C0 64BC101 161FC103 130C6500
    22D6E757 76D181C3 7F15151F 32830203 010011A3 63306130 0F060355 1D3C1001
    FF040503 030110FF 030E0603 551D0F01 0F1F0400 30021016 3201D053 551D0D04
    16041420 F044BFCF 1C565F5B 40C06DAD 4E6736A1 E6121D30 1F060355 120D3014
    3016B01A 20FC4B8F 01BC565F 05D4606A 046E6734 1AE612D1 30060609 2A864886
    F70D0109 01050003 81801005 2E3886F5 107116B6 AD3AC990 CBE84603 5FB2A65B
    BD572026 52E992ED 02F3AA0E 18032F02 AA40EDE2 D559F180 7B50264F 304F2C41
    0A9F9C4E 70BD3C8B 00000000 8E9363BD B44100DF 062DACF 67DAE658 3879A3E3
    12AFB9C3 2E27C627 EC74E1FC AEE2F5CA AA8B4349 615A98D5 6D6ED6C3 7F92C797
    3963E363 F2989FB9 795B8A
    quit
!
!  crypto isakmp policy 10
  encr 3des
  group 2
!
!  crypto ipsec transform-set ISC_TS_1 esp-3des esp-sha-hmac
!  crypto ipsec profile ISC_IPSECPROFILE_2
Example Debug of a Successful PKI AAA Authorization

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
```
Example Debugs of a Failed PKI AAA Authorization

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 crypto isakmp sa
<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.22</td>
<td>192.0.2.102</td>
<td>QM_IDLE</td>
<td>84</td>
<td>0</td>
</tr>
</tbody>
</table>

Example Debugs of a Failed PKI AAA Authorization

May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:36:12.813: TPLUS: Would block while reading pak header
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: Processing the reply packet
May 28 19:36:12.817: TPLUS: Processed AV cert-application=all
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

Router# show crypto isakmp sa
<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.22</td>
<td>192.0.2.102</td>
<td>QM_IDLE</td>
<td>84</td>
<td>0</td>
</tr>
</tbody>
</table>

Example Debugs of a Failed PKI AAA Authorization

Router# show crypto isakmp sa
<table>
<thead>
<tr>
<th>dst</th>
<th>src</th>
<th>state</th>
<th>conn-id</th>
<th>slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.22</td>
<td>192.0.2.102</td>
<td>QM_IDLE</td>
<td>84</td>
<td>0</td>
</tr>
</tbody>
</table>
Examples Configuring a Revocation Mechanism

Example Configuring an OCSP Server

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

Example Specifying a CRL and Then an OCSP Server

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

Example Specifying an OCSP Server

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
Example Disabling Nonces in Communications with the OCSP Server

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(config)# ocsp url http://myocspserver:81
Router(config)# revocation-check ocsp none
Router(config)# ocsp disable-nonce

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

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:
  cn=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
  end   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
  end   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(ca-certificate-map)#

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.

cn=Central VPN Gateway
o=Home Office Inc

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
!Many lines left out
.
.
.
crypto pki trustpoint home-office
Example Configuring a Hub Router at a Central Site for Certificate Revocation Checks

Example Disabling Nonces in Communications with the OCSP Server

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.

match 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: 2F62BE14000000000CA0
 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
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 co 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=Brahcn 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.

Examples Configuring Certificate Authorization and Revocation Settings

Example 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=name Cert 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

Example 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
  enrollment url http://CA1
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
  revocation-check crl
  aaa new-model
  aaa attribute list crl
    attribute-type aaa-cert-serial-not 4ACA
```

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

```
Dec 3 04:24:39.051: CRYPTO_PKI: Trust-Point CA1 picked up
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.051: CRYPTO_PKI: unlocked trustpoint CA1, refcount is 0
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.135: CRYPTO_PKI: validation path has 1 certs
Dec 3 04:24:39.135: CRYPTO_PKI: Found a issuer match
Dec 3 04:24:39.135: CRYPTO_PKI: Using CA1 to validate certificate
Dec 3 04:24:39.135: CRYPTO_PKI: Selected AAA username: "PKIAAA"
Dec 3 04:24:39.135: CRYPTO_PKI: Anticipate checking AAA list: "CRL"
Dec 3 04:24:39.135: CRYPTO_PKI: AAA: checking AAA authorization (CRL, PKIAAA-L1, <all>)
Dec 3 04:24:39.135: CRYPTO_PKI: AAA: pre-authorization chain validation status (0x4)
Dec 3 04:24:39.135: AAA/AUTHOR (0x21): Pick method list 'CRL'

Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-serial-not" = "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: cert-serial doesn't match ("4ACA" != "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: post-authorization chain validation status (0x7)
Dec 3 04:24:39.175: CRYPTO_PKI: chain cert was anchored to trustpoint CA1, and chain validation result was: CRYPTO_PKI_CERT_NOT_AUTHORIZED
```
Examples Configuring Certificate Chain Validation

Example 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
  revocation-check none
  rsakeypair RootCA

crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
  rsakeypair SubCA1

crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
  rsakeypair SubCA11

Example 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.

crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
  rsakeypair RootCA

crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
  rsakeypair SubCA1

crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
  rsakeypair SubCA11

Example Configuring Certificate Chain Validation Through a Gap

In the following configuration example, SubCA1 is not in the configured Cisco IOS XE 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, SubCA11, and SubCA1 certificates.
If the peer does not supply the SubCA1 certificate in the presented certificate chain, the chain validation will fail.

```plaintext
crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
  rsakeypair RootCA

crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
  rsakeypair SubCA1
```

### 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 XE PKI Overview: Understanding and Planning a PKI” module in the <em>Cisco IOS XE Security Configuration Guide: Secure Connectivity</em></td>
</tr>
<tr>
<td>RSA key generation and deployment</td>
<td>“Deploying RSA Keys Within a PKI” module in the <em>Cisco IOS XE Security Configuration Guide: Secure Connectivity</em></td>
</tr>
<tr>
<td>Certificate enrollment: supported methods, enrollment profiles, configuration tasks</td>
<td>“Configuring Certificate Enrollment for a PKI” module in the <em>Cisco IOS XE Security Configuration Guide: Secure Connectivity</em></td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</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>Software Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Control Enhancements for Certification Revocation Lists</td>
<td>Cisco IOS XE Release 2.4</td>
<td>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 • Configuring Certificate Authorization and Revocation Settings • Examples: Configuring Certificate Authorization and Revocation Settings The following commands were introduced or modified by this feature: <code>crl-cache delete-after, crl-cache none, crypto pki certificate map</code></td>
</tr>
<tr>
<td>Certificate-Complete Chain Validation</td>
<td>Cisco IOS XE Release 2.4</td>
<td>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 • Configuring Certificate Chain Validation • Examples: Configuring Certificate Chain Validation The following command was introduced by this feature: <code>chain-validation</code></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Software Releases</td>
<td>Feature Configuration Information</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OCSP - Server Certification from Alternate Hierarchy</td>
<td></td>
<td>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 - Configuring Certificate Authorization and Revocation Settings The following command was introduced by this feature: <code>match certificate override ocs</code></td>
</tr>
<tr>
<td>Optional OCSP Nonce</td>
<td>Cisco IOS XE Release 2.1</td>
<td>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 - Configuring a Revocation Mechanism for PKI Certificate Status Checking - Example: Disabling Nonces in Communications with the OCSP Server</td>
</tr>
</tbody>
</table>
Certificate Security Attribute-Based Access Control

Cisco IOS XE Release 2.1

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
• Configuring Certificate Authorization and Revocation Settings

The following commands were introduced or modified by this feature: `crypto pki certificate map`, `crypto pki trustpoint match certificate`
### Feature Information for Certificate Authorization and Revocation

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Software Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
</table>
| Online Certificate Status Protocol (OCSP)         | Cisco IOS XE Release 2.1   | 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  
  - Configuring a Revocation Mechanism for PKI Certificate Status Checking  
  The following commands were introduced by this feature: `ocsp url`, `revocation-check` |
| PKI AAA Authorization Using the Entire Subject Name | Cisco IOS XE Release 2.1   | 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  
  - Configuring PKI Integration with a AAA Server  
  The following command was modified by this feature: `authorization username` |
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Software Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
</table>
| PKI Integration with AAA Server | Cisco IOS XE Release 2.1  | 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  
- Configuring PKI Integration with a AAA Server  
The following commands were introduced by this feature:  
authorization list, authorization username |
PKI: Query Multiple Servers During Certificate Revocation Check

Cisco IOS XE Release 2.1

This feature introduces the ability for Cisco IOS XE 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
- Manually Overriding CDPs in a Certificate

The following command was introduced by this feature: `match certificate override cdp`
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Software Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
</table>
| Using Certificate ACLs to Ignore Revocation Check and Expired Certificates | Cisco IOS XE Release 2.1 | 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  
  - Configuring Certificate-Based ACLs to Ignore Revocation Checks  
  The following command was modified by this feature: `match certificate` |
| Query Mode Definition Per Trustpoint             | Cisco IOS XE Release 2.1 | This feature was integrated into Cisco IOS XE Release 2.1.                                                                                                         |
| PKI High Availability                            | Cisco IOS XE Release 3.2S | Public Key Infrastructure (PKI) High Availability refers to the technology and system-design approach that supports the operation of a certificate-based public key cryptographic system that is available at all times. This feature was integrated into Cisco IOS XE Release 3.2S. The following sections provide information about this feature:  
  - PKI High Availability Support |
Examples Configuring Certificate Chain Validation

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.