



# Certificate Security Attribute-Based Access Control

---

Under the IP Security (IPSec) protocol, certification authority (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. The Certificate Security Attribute-Based Access Control feature adds fields to the certificate that allow specifying an access control list (ACL), to create a certificate-based ACL.

## Feature Specifications for Certificate Security Attribute-Based Access Control

---

### Feature History

Release	Modification
12.2(15)T	This feature was introduced.

---

### Supported Platforms

Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco MC3810, Cisco ubr7200, Cisco ubr905, Cisco ubr925, Cisco 800 series, Cisco 1600, Cisco 1600R, Cisco 1700 series, Cisco 2400, Cisco 2600 series, Cisco 3620, Cisco 3631, Cisco 3640, Cisco 3660, Cisco 3725, Cisco 3745, Cisco 7100, Cisco 7200, Cisco 7400, Cisco 7500, Cisco 8850-RPM

---

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

# Contents

- [Prerequisites for Certificate Security Attribute-Based Access Control, page 2](#)
- [Information About Certificate Security Attribute-Based Access Control, page 2](#)
- [How to Configure Certificate-Based ACLs, page 3](#)
- [Configuration Examples for Certificate Security Attribute-Based Access Control, page 7](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)

## Prerequisites for Certificate Security Attribute-Based Access Control

- You must be familiar with International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendation X.509, *Public-Key and Attribute Certificate Frameworks*.
- You must have a CA available to your network that supports the Cisco Public-Key Infrastructure (PKI) protocol and Simple Certificate Enrollment Protocol (SCEP), or you are able to use the cut and paste method of enrollment. Refer to the [“Manual Certificate Enrollment \(TFTP and Cut-and-Paste\)”](#) feature module, which describes this functionality.
- Certificate ACL support is part of the PKI subsystem, and this subsystem requires the crypto subsystem.

## Information About Certificate Security Attribute-Based Access Control

To create a certificate-based ACL, you need to understand the following concepts:

- [Certificate-Based ACLs, page 2](#)
- [Memory Requirements for Certificate-Based ACLs, page 3](#)

## Certificate-Based ACLs

Certificates are used to identify an entity (a user or device) and, using fields within the certificate, to associate attributes with that entity. The certificate includes several fields that determine whether the entity is authorized to perform a specified action. The Certificate Security Attribute-Based Access Control feature adds a new command, **crypto ca certificate map**, and new fields to the certificate that create the certificate-based ACL.

The certificate-based ACL specifies 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. Each ACL will be processed in turn until a match is found or all of the ACLs have been processed.

The **crypto ca trustpoint** command has been enhanced to support certificate-based ACLs, which allows any application using the Cisco IOS software to take advantage of certificate-based ACLs.

## Memory Requirements for Certificate-Based ACLs

Memory is required to hold the ACLs as they are created and as they are loaded from the configuration file. The amount of memory depends on which fields within the certificate are being checked and how many ACLs have been defined. Certificate-based ACL support requires one or more compare operations when the fields in a certificate are being checked. Only the fields specified by the ACL are checked. The compare operations are a small part of certificate validation and will not have a noticeable effect on router performance when validating certificates.

## How to Configure Certificate-Based ACLs

This section contains the following procedures:

- [Configuring Certificate-Based ACLs, page 3](#) (required)
- [Verifying Certificate-Based ACLs Example, page 7](#) (optional)

## Configuring Certificate-Based ACLs


The IPSec protocol and CA interoperability permit Cisco IOS devices and a CA to communicate so that the Cisco IOS device can obtain and use digital certificates from the CA. The certificate includes several fields that determine whether an entity is authorized to perform a specified action. The Certificate Security Attribute-Based Access Control feature adds fields to specify a certificate-based ACL. In this task, you use the **crypto ca certificate map** command and the **match certificate** subcommand of the **crypto ca trustpoint** command, to map the name of an ACL.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **crypto ca certificate map** *label sequence-number*
4. *field-name match-criteria match-value*
5. **exit**
6. **crypto ca trustpoint** *name*
7. **match certificate** *certificate-map-label*
8. **exit**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>crypto ca certificate map</b> <i>label sequence-number</i>  <b>Example:</b> Router(config)# crypto ca certificate map Group 10	Starts ca-certificate-map mode and defines certificate-based ACLs by assigning a label for the ACL that will also be referenced within the <b>crypto ca trustpoint</b> command. A sequence number orders ACLs with the same label.

Command or Action	Purpose
<p><b>Step 4</b> <code>field-name match-criteria match-value</code></p> <p><b>Example:</b>  Router(ca-certificate-map)# subject-name co  Cisco</p>	<p>In ca-certificate-map mode, you specify one or more certificate fields together with their matching criteria and the value to match.</p> <ul style="list-style-type: none"> <li>The <i>field-name</i> is one of the following case-insensitive name strings or a date: <ul style="list-style-type: none"> <li><b>subject-name</b></li> <li><b>issuer-name</b></li> <li><b>unstructured-subject-name</b></li> <li><b>alt-subject-name</b></li> <li><b>name</b></li> <li><b>valid-start</b></li> <li><b>expires-on</b></li> </ul> </li> </ul> <p> <b>Note</b> Date field format is dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.</p> <ul style="list-style-type: none"> <li>The <i>match-criteria</i> is one of the following logical operators: <ul style="list-style-type: none"> <li><b>eq</b>—equal (valid for name and date fields)</li> <li><b>ne</b>—not equal (valid for name and date fields)</li> <li><b>co</b>—contains (valid only for name fields)</li> <li><b>nc</b>—does not contain (valid only for name fields)</li> <li><b>lt</b>—less than (valid only for date fields)</li> <li><b>ge</b>—greater than or equal (valid only for date fields)</li> </ul> </li> </ul> <p>The <i>match-value</i> is the name or date to test with the logical operator assigned by <i>match-criteria</i>.</p>
<p><b>Step 5</b> <code>exit</code></p> <p><b>Example:</b>  Router(config-cert-map)# exit</p>	<p>Exits ca-certificate-map mode.</p>
<p><b>Step 6</b> <code>crypto ca trustpoint name</code></p> <p><b>Example:</b>  Router(config)# crypto ca trustpoint Access</p>	<p>Starts ca-trustpoint configuration mode and creates a name for the CA.</p>

	Command or Action	Purpose
Step 7	<b>match certificate</b> <i>certificate-map-label</i>  <b>Example:</b> Router(ca-trustpoint)# match certificate Group	Associates the certificate-based ACL defined with the <b>crypto ca certificate map</b> command to the trustpoint. <ul style="list-style-type: none"> <li>The <i>certificate-map-label</i> argument must match the <i>label</i> argument specified in the previously defined <b>crypto ca certificate map</b> command.</li> </ul>
Step 8	<b>exit</b>  <b>Example:</b> Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.

## What to Do Next

See the examples in the [“Configuration Examples for Certificate Security Attribute-Based Access Control” section on page 7](#) to understand how to configure certificate-based ACLs. The [“Verifying Certificate-Based ACLs”](#) section describes how to display certificate components.

## Verifying Certificate-Based ACLs

If the router has authenticated, or authenticated and enrolled with any trustpoint, you can use the **show crypto ca certificates** command to show the components of the certificates installed on the router; that is, CA certificate if authenticated, and CA and router certificate if the router has both authenticated and enrolled.

### SUMMARY STEPS

1. **enable**
2. **show crypto ca certificates**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>show crypto ca certificates</b>  <b>Example:</b> Router# show crypto ca certificates	Displays information about your certificate.

## What to Do Next

Review the verification example in the [“Verifying Certificate-Based ACLs Example”](#) section to see the certificate components that can be displayed.

# Configuration Examples for Certificate Security Attribute-Based Access Control

This section provides the following examples for the Certificate Security Attribute-Based Access Control feature.

- [Certificate-Based ACL Example, page 7](#)
- [Certificate-Based ACL with Sequence Numbers Example, page 7](#)
- [Verifying Certificate-Based ACLs Example, page 7](#)

## Certificate-Based ACL Example

The following example shows a certificate-based ACL with the label Group defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca trustpoint** command:

```
crypto ca certificate map Group 10
  subject-name co WAN
  subject-name co Cisco
!
crypto ca trustpoint Access1
  match certificate Group
```

## Certificate-Based ACL with Sequence Numbers Example

The following example accepts any certificate issued by Cisco Systems for an entity with the subject name DIAL or WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first.

```
crypto ca certificate map Group 10
  issuer-name co Cisco Systems
  subject-name co DIAL
crypto ca certificate map Group 20
  issuer-name co Cisco Systems
  subject-name co WAN
!
crypto ca trustpoint Access2
  match certificate Group
```

Case is ignored in string comparisons, therefore DIAL in this example will match dial, DIAL, Dial, and so on.

## Verifying Certificate-Based ACLs Example

The following example shows the components of the certificates—CA and router certificate—installed on the router when the router has both authenticated and enrolled with a trustpoint:

```
router# show crypto ca certificate

CA Certificate
  Status: Available
  Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
  Certificate Usage: Signature
```

```

Issuer:
  CN = new-user
  OU = pki new-user
  O = cisco
  L = santa cruz2
  ST = CA
  C = US
  EA = user@cisco.net
Subject:
  CN = new-user
  OU = pki new-user
  O = cisco
  L = santa cruz2
  ST = CA
  C = US
  EA = user@cisco.net
CRL Distribution Point:
  http://new-user.cisco.net/CertEnroll/new-user.crl
Validity Date:
  start date: 14:19:29 PST Oct 31 2002
  end date: 14:27:27 PST Oct 31 2017
Associated Trustpoints: MS

```

```

Certificate
Status: Available
Certificate Serial Number: 193E28D20000000009F7
Certificate Usage: Signature
Issuer:
  CN = new-user
  OU = pki new-user
  O = cisco
  L = santa cruz2
  ST = CA
  C = US
  EA = user@cisco.net
Subject:
  Name: User1.Cisco.Net
  OID.1.2.840.113549.1.9.2 = User1.Cisco.Net
CRL Distribution Point:
  http://new-user.cisco.net/CertEnroll/new-user.crl
Validity Date:
  start date: 12:40:14 PST Feb 26 2003
  end date: 12:50:14 PST Mar 5 2003
  renew date: 16:00:00 PST Dec 31 1969
Associated Trustpoints: MS

```

## Additional References

For additional information related to the Certificate Security Attribute-Based Access Control feature, refer to the following sections:

- [Related Documents, page 9](#)
- [Standards, page 9](#)
- [MIBs, page 9](#)
- [RFCs, page 9](#)
- [Technical Assistance, page 10](#)

## Related Documents

Related Topic	Document Title
CA interoperability	<i>Cisco IOS Security Configuration Guide</i> , Release 12.2. Refer to the chapter “Configuring Certification Authority Interoperability.”
IPSec and encryption commands.	<i>Cisco IOS Security Command Reference</i> , Release 12.2 T. Refer to the parts “IP Security and Encryption” and “Certification Authority Interoperability Commands.”

## Standards

Standards	Title
ITU-T Recommendation X.509	<i>Public-Key and Attribute Certificate Frameworks</i>

## MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:  <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

RFCs	Title
None	—

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

### New

- [crypto ca certificate map](#)
- [match certificate](#)

### Modified

- [crypto ca trustpoint](#)

# crypto ca certificate map

To define certificate-based access control lists (ACLs), use the **crypto ca certificate map** command in CA certificate map mode. To remove the certificate-based ACLs, use the **no** form of this command.

**crypto ca certificate map** *label sequence-number*

**no crypto ca certificate map** *label sequence-number*

## Syntax Description

<i>label</i>	A user-specified label that is referenced within the <b>crypto ca trustpoint</b> command.
<i>sequence-number</i>	A number that orders the ACLs with the same label. ACLs with the same label are processed from lowest to highest sequence number. When an ACL is matched, processing stops with a successful result.

## Defaults

No default behavior or value.

## Command Modes

Ca-certificate- map

## Command History

Release	Modification
12.2(15)T	This command was introduced.

## Usage Guidelines

Issuing this command places the router in ca-certificate-map mode where you can specify several certificate fields together with their matching criteria. The general form of these fields is as follows:

*field-name match-criteria match-value*

The *field-name* is one of the certificate fields. Field names are similar to the names used in the ITU-T X.509 standard. The **name** field is a special field that matches any subject name or related name field in the certificate, such as the **subject-name**, **unstructured-subject-name**, and **alt-subject-name** fields.

- **subject-name**—Case-insensitive string.
- **issuer-name**—Case-insensitive string.
- **unstructured-subject-name**—Case-insensitive string.
- **alt-subject-name**—Case-insensitive string.
- **name**—Case-insensitive string.
- **valid-start**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.
- **expires-on**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

**Note**

The time portion is optional in both the **valid-start** and **expires-on** date fields, and defaults to 00:00:00 if not specified. The time is interpreted according to the time zone offset configured for the router. The string **utc** can be appended to the date and time when they are configured as Universal Time, Coordinated (UTC) rather than local time.

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

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

The *match-value* is a case-insensitive string or a date.

**Examples**

The following example shows how to configure a certificate-based ACL that will allow any certificate issued by Cisco Systems to an entity within the cisco.com domain. The label is Cisco and the sequence is 10.

```
crypto ca certificate map Cisco 10
 issuer-name co Cisco Systems
 unstructured-subject-name co cisco.com
```

The following example accepts any certificate issued by Cisco Systems for an entity with DIAL or organizationUnit component ou=WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first. Note that the string “DIAL” can occur anywhere in the subjectName field of the certificate, but the string WAN must be in the organizationUnit component.

```
crypto ca certificate map Group 10
 issuer-name co Cisco Systems
 subject-name co DIAL
crypto ca certificate map Group 20
 issuer-name co Cisco Systems
 subject-name co ou=WAN
```

Case is ignored in string comparisons, therefore DIAL in the previous example will match dial, DIAL, Dial, and so on. Also note that the component identifiers (o=, ou=, cn=, and so on) are not required unless it is desirable that the string to be matched occurs in a specific component of the name. (Refer to the ITU-T security standards for more information about certificate fields and components such as ou=.)

If a component identifier is specified in the match string, the exact string, including the component identifier, must appear in the certificate. This requirement can present a problem if more than one component identifier is included in the match string. For example, “ou=WAN,o=Cisco Systems” will not match a certificate with the string “ou=WAN,ou=Engineering,o=Cisco Systems” because the “ou=Engineering” string separates the two desired component identifiers.

To match both “ou=WAN” and “o=Cisco Systems” in a certificate while ignoring other component identifiers, you could use this certificate map:

```
crypto ca certificate map Group 10
  subject-name co ou=WAN
  subject-name co o=Cisco
```

Any space character proceeding or following the “=” character in component identifiers is ignored. Therefore “o=Cisco” in the proceeding example will match “o = Cisco,” “o= Cisco,” “o=Cisco,” and so on.

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">crypto ca trustpoint</a>	Declares the CA that your router should use.

---

# crypto ca trustpoint

To declare the certification authority (CA) that your router should use, use the **crypto ca trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the CA, use the **no** form of this command.

**crypto ca trustpoint** *name*

**no crypto ca trustpoint** *name*

## Syntax Description

<i>name</i>	A name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.)
-------------	--

## Defaults

Your router does not know about any CAs until you declare one using this command.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The <b>match certificate</b> subcommand was introduced.

## Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA, which can be a root CA and have a self-signed certificate that contains its own public key. Issuing this command places the router in ca-trustpoint configuration mode.

In ca-trustpoint configuration mode, you can specify characteristics for the trustpoint CA using the following subcommands:

- **crl**—Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **default (ca-trustpoint)**—Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment**—Specifies enrollment parameters (optional).
- **enrollment http-proxy**—Accesses the CA by HTTP through the proxy server.
- **match certificate**—Associates the certificate-based access control list (ACL) defined with the **crypto ca certificate map** command.
- **primary**—Assigns a specified trustpoint as the primary trustpoint of the router.
- **root**—Defines the TFTP protocol to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

**Note**

The **crypto ca trustpoint** command unifies the functionality of the **crypto ca identity** and **crypto ca trusted-root** commands, thereby replacing these commands. Although you can still enter the **crypto ca identity** and **crypto ca trusted-root** commands, the configuration mode and command will be written back as ca-trustpoint.

**Examples**

The following example shows how to declare the CA named ka and specify enrollment and CRL parameters:

```
crypto ca trustpoint ka
  enrollment url http://kahului:80
```

The following example shows a certificate-based ACL with the label Group defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca trustpoint** command:

```
crypto ca certificate map Group 10
  subject-name co ou=WAN
  subject-name co o=Cisco
!
crypto ca trustpoint pki
  match certificate Group
```

**Related Commands**

Command	Description
<a href="#">crl</a>	Queries the CRL to ensure that the certificate of the peer has not been revoked.
<a href="#">default (ca-trustpoint)</a>	Resets the value of a ca-trustpoint configuration subcommand to its default.
<a href="#">enrollment</a>	Specifies the enrollment parameters of your CA.
<a href="#">enrollment http-proxy</a>	Accesses the CA by HTTP through the proxy server.
<a href="#">match certificate</a>	Associates a certificate-based ACL defined with the <b>crypto ca certificate map</b> command.
<a href="#">primary</a>	Assigns a specified trustpoint as the primary trustpoint of the router.
<a href="#">root</a>	Obtains the CA certificate via TFTP.

# match certificate

To associate a certificate-based access control list (ACL) defined with the **crypto ca certificate map** command, use the **match certificate** subcommand in ca-trustpoint configuration mode. To remove the association, use the **no** form of this subcommand.

**match certificate** *certificate-map-label*

**no match certificate** *certificate-map-label*

## Syntax Description

*certificate-map-label* Matches the *label* argument specified in a previously defined **crypto ca certificate map** command.

## Defaults

No default match certificate is configured.

## Command Modes

Ca-trustpoint configuration

## Command History

Release	Modification
12.2(15)T	This subcommand was introduced.

## Usage Guidelines

The **match certificate** subcommand associates the certificate-based ACL defined with the **crypto ca certificate map** command to the trustpoint. The *certificate-map-label* argument in the **match certificate** subcommand must match the *label* argument specified in a previously defined **crypto ca certificate map** command.

The certificate map with the label *certificate-map-label* must be defined before it can be used with the **match certificate** subcommand.

A certificate referenced in a **match certificate** subcommand may not be deleted until all references to the certificate map are removed from configured trustpoints (that is, no **match certificate** subcommands can reference the certificate map being deleted).

When a peer's certificate has been verified, the certificate-based ACL as specified by the certificate map is checked. If the peer's certificate matches the certificate ACL, or a certificate map is not associated with the trustpoint used to verify the peer's certificate, the peer's certificate is considered valid.

If the certificate map does not have any attributes defined, the certificate is rejected.

## Examples

The following example shows a certificate-based ACL with the label Group defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca trustpoint** command:

```
crypto ca certificate map Group 10
  subject-name co ou=WAN
  subject-name co o=Cisco
```

```
!  
crypto ca trustpoint pki  
match certificate Group
```

**Related Commands**

Command	Description
<b>crypto ca certificate map</b>	Defines certificate-based ACLs.
<b>crypto ca trustpoint</b>	Declares the CA that your router should use.

■ match certificate