



Certificate to ISAKMP Profile Mapping

First Published: May 17, 2004

Last Updated: June 22, 2009

The Certificate to ISAKMP Profile Mapping feature enables you to assign an Internet Security Association and Key Management Protocol (ISAKMP) profile to a peer on the basis of the contents of arbitrary fields in the certificate. In addition, this feature allows you to assign a group name to those peers that are assigned an ISAKMP profile.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for Certificate to ISAKMP Profile Mapping”](#) section on page 10.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Certificate to ISAKMP Profile Mapping, page 2](#)
- [Restrictions for Certificate to ISAKMP Profile Mapping, page 2](#)
- [Information About Certificate to ISAKMP Profile Mapping, page 2](#)
- [How to Configure Certificate to ISAKMP Profile Mapping, page 3](#)
- [Configuration Examples for Certificate to ISAKMP Profile Mapping, page 6](#)
- [Additional References, page 9](#)
- [Feature Information for Certificate to ISAKMP Profile Mapping, page 10](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Certificate to ISAKMP Profile Mapping

- You should be familiar with configuring certificate maps.
- You should be familiar with configuring ISAKMP profiles.

Restrictions for Certificate to ISAKMP Profile Mapping

This feature is not applicable if you use Rivest, Shamir, and Adelman (RSA)-signature or RSA-encryption authentication without certificate exchange. ISAKMP peers must be configured for RSA-signature or RSA-encryption authentication using certificates.

IPsec with two trustpoints enrolled in the same Certificate Authority (CA) server is not supported. When there are two or more ISAKMP profiles, each having a different trustpoint enrolled in the same CA server, the responder selects the last global trustpoint. (Trustpoints are selected in the reverse order in which they are defined globally). For the IPsec tunnel establishment to be successful for peers, the trustpoint selected by the initiator should match the trustpoint selected by the responder. All other IPsec tunnels will fail to establish connection if the trustpoints do not match.

Information About Certificate to ISAKMP Profile Mapping

- [Certificate to ISAKMP Profile Mapping Overview, page 2](#)
- [How Certificate to ISAKMP Profile Mapping Works, page 3](#)
- [Assigning an ISAKMP Profile and Group Name to a Peer, page 3](#)

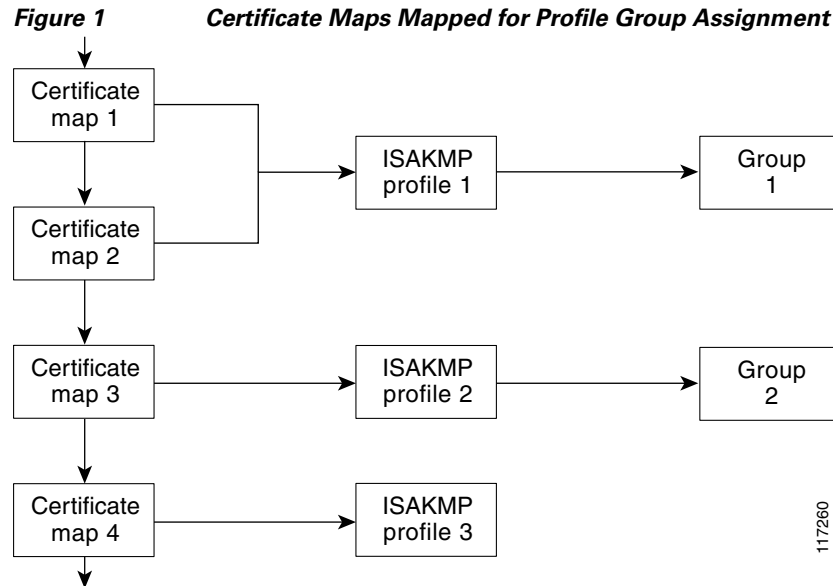
Certificate to ISAKMP Profile Mapping Overview

Prior to Cisco IOS Release 12.3(8)T, the only way to map a peer to an ISAKMP profile was as follows. The ISAKMP identity field in the ISAKMP exchange was used for mapping a peer to an ISAKMP profile. When certificates were used for authentication, the ISAKMP identity payload contained the subject name from the certificate. If a CA did not provide the required group value in the first Organizational Unit (OU) field of a certificate, an ISAKMP profile could not be assigned to a peer.

Effective with Cisco IOS Release 12.3(8)T, a peer can still be mapped as explained above. However, the Certificate to ISAKMP Profile Mapping feature enables you to assign an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate. You are no longer limited to assigning an ISAKMP profile on the basis of the subject name of the certificate. In addition, this feature allows you to assign a group to a peer to which an ISAKMP profile has been assigned.

How Certificate to ISAKMP Profile Mapping Works

Figure 1 illustrates how certificate maps may be attached to ISAKMP profiles and assigned group names.



A certificate map can be attached to only one ISAKMP profile although an ISAKMP profile can have several certificate maps attached to it.

Certificate maps provide the ability for a certificate to be matched with a given set of criteria. ISAKMP profiles can bind themselves to certificate maps, and if the presented certificate matches the certificate map present in an ISAKMP profile, the peer will be assigned the ISAKMP profile. If the ISAKMP profile contains a client configuration group name, the same group name will be assigned to the peer. This ISAKMP profile information will override the information in the ID_KEY_ID identity or in the first OU field of the certificate.

Assigning an ISAKMP Profile and Group Name to a Peer

To assign an ISAKMP profile to a peer on the basis of arbitrary fields in the certificate, use the **match certificate** command after the ISAKMP profile has been defined.

To associate a group name with an ISAKMP profile that will be assigned to a peer, use the **client configuration group** command, also after the ISAKMP profile has been defined.

How to Configure Certificate to ISAKMP Profile Mapping

- [Mapping the Certificate to the ISAKMP Profile, page 4](#) (required)
- [Verifying That the Certificate Has Been Mapped, page 4](#) (optional)
- [Assigning the Group Name to the Peer, page 5](#) (required)
- [Monitoring and Maintaining Your Certificate to ISAKMP Profile Mapping, page 6](#) (optional)

Mapping the Certificate to the ISAKMP Profile

To map the certificate to the ISAKMP profile, perform the following steps. This configuration will enable you to assign the ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **match certificate** *certificate-map*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp profile <i>profile-name</i> Example: Router (config)# crypto isakmp profile vpnprofile	Defines an ISAKMP profile and enters into crypto ISAKMP profile configuration mode.
Step 4	match certificate <i>certificate-map</i> Example: Router (conf-isa-prof)# match certificate map1	Accepts the name of a certificate map.

Verifying That the Certificate Has Been Mapped

The following **show** command may be used to verify that the subject name of the certificate map has been properly configured.

SUMMARY STEPS

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

DETAILED STEPS

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

Assigning the Group Name to the Peer

To associate a group name with a peer when the peer is mapped to an ISAKMP profile, perform the following steps.

SUMMARY STEPS

- enable**
- configure terminal**
- crypto isakmp profile** *profile-name*
- client configuration group** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp profile <i>profile-name</i> Example: Router (config)# crypto isakmp profile vpnprofile	Defines an ISAKMP profile and enters into isakmp profile configuration mode.
Step 4	client configuration group <i>group-name</i> Example: Router (conf-isa-prof)# client configuration group group1	Accepts the name of a group that will be assigned to a peer when the peer is assigned this crypto ISAKMP profile.

Monitoring and Maintaining Your Certificate to ISAKMP Profile Mapping

To monitor and maintain your certificate to ISAKMP profile mapping, you may use the following **debug** command.

SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug crypto isakmp Example: Router# debug crypto isakmp	Displays output showing that the certificate has gone through certificate map matching and that the certificate matches the ISAKMP profile. The command may also be used to verify that the peer has been assigned a group.

Configuration Examples for Certificate to ISAKMP Profile Mapping

This section contains the following configuration examples:

- [Certificates Mapped to the ISAKMP Profile on the Basis of Arbitrary Fields: Example, page 6](#)
- [Group Name Assigned to a Peer That Is Associated with an ISAKMP Profile: Example, page 7](#)
- [Mapping a Certificate to an ISAKMP Profile Verification: Example, page 7](#)
- [Group Name Assigned to a Peer Verification: Example, page 8](#)

Certificates Mapped to the ISAKMP Profile on the Basis of Arbitrary Fields: Example

The following configuration example shows that whenever a certificate contains “ou = green,” the ISAKMP profile “cert_pro” will be assigned to the peer:

```
crypto pki certificate map cert_map 10
  subject-name co ou = green
  !
  !
crypto isakmp identity dn
crypto isakmp profile cert_pro
  ca trust-point 2315
  ca trust-point LaBcA
```

```
initiate mode aggressive
match certificate cert_map
```

Group Name Assigned to a Peer That Is Associated with an ISAKMP Profile: Example

The following example shows that the group “some_group” is to be associated with a peer that has been assigned an ISAKMP profile:

```
crypto isakmp profile id_profile
ca trust-point 2315
match identity host domain cisco.com
client configuration group some_group
```

Mapping a Certificate to an ISAKMP Profile Verification: Example

The following examples show that a certificate has been mapped to an ISAKMP profile. The examples include the configurations for the responder and initiator, **show command** output verifying that the subject name of the certificate map has been configured, and **debug** command output showing that the certificate has gone through certificate map matching and been matched to the ISAKMP profile.

Responder Configuration

```
crypto pki certificate map cert_map 10
! The above line is the certificate map definition.
subject-name co ou = green
! The above line shows that the subject name must have "ou = green."
!
crypto isakmp profile certpro
! The above line shows that this is the ISAKMP profile that will match if the certificate
of the peer matches cert_map (shown on third line below).
ca trust-point 2315
ca trust-point LaBcA
match certificate cert_map
initiate mode aggressive
```

Initiator Configuration

```
crypto ca trustpoint LaBcA
enrollment url http://10.76.82.20:80/cgi-bin/openscep
subject-name ou=green,c=IN
! The above line ensures that the subject name "ou = green" is set.
revocation-check none
```

show crypto ca certificates Command Output for the Initiator

```
Router# show crypto ca certificates
```

```
Certificate
Status: Available
Certificate Serial Number: 21
Certificate Usage: General Purpose
Issuer:
cn=blue-lab CA
o=CISCO
c=IN
Subject:
Name: Router1.cisco.com
c=IN
```

```

ou=green
! The above line is a double check that "ou = green" has been set as the subject name.
hostname=Router1.cisco.com
Validity Date:
  start date: 14:34:30 UTC Mar 31 2004
  end   date: 14:34:30 UTC Apr 1 2009
  renew date: 00:00:00 UTC Jan 1 1970
Associated Trustpoints: LaBCA

```

debug crypto isakmp Command Output for the Responder

```

Router# debug crypto isakmp

6d23h: ISAKMP (0:268435460): received packet from 192.0.0.2 dport 500 sport 500 Global (R)
MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:      ID payload
6d23h:      FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:      CERT payload
6d23h:      SIG payload
6d23h:      KEEPALIVE payload
6d23h:      NOTIFY payload
6d23h: ISAKMP:(0:4:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:4:HW:2):Old State = IKE_R_MM4  New State = IKE_R_MM5

6d23h: ISAKMP:(0:4:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435460): ID payload
      next-payload : 6
      type         : 2
      FQDN name    : Router1.cisco.com
      protocol     : 17
      port        : 500
      length      : 28

6d23h: ISAKMP:(0:4:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:4:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:4:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:4:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:4:HW:2): OU = green
6d23h: ISAKMP:(0:4:HW:2): certificate map matches certpro profile
! The above line shows that the certificate has gone through certificate map matching and
that it matches the "certpro" profile.
6d23h: ISAKMP:(0:4:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:4:HW:2): Creating CERT validation list: 2315, LaBCA,
6d23h: ISAKMP:(0:4:HW:2): CERT validity confirmed.

```

Group Name Assigned to a Peer Verification: Example

The following configuration and debug output show that a group has been assigned to a peer.

Initiator Configuration

```

crypto isakmp profile certpro
  ca trust-point 2315
  ca trust-point LaBCA
  match certificate cert_map
  client configuration group new_group
! The statement on the above line will assign the group "new_group" to any peer that
matches the ISAKMP profile "certpro."
  initiate mode aggressive
!

```


debug crypto isakmp profile Command Output for the Responder

The following debug output example shows that the peer has been matched to the ISAKMP profile named “certpro” and that it has been assigned a group named “new_group.”

```

Router# debug crypto isakmp profile
6d23h: ISAKMP (0:268435461): received packet from 192.0.0.2 dport 500 sport 500 Global (R)
MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:         ID payload
6d23h:         FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:         CERT payload
6d23h:         SIG payload
6d23h:         KEEPALIVE payload
6d23h:         NOTIFY payload
6d23h: ISAKMP:(0:5:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:5:HW:2):Old State = IKE_R_MM4 New State = IKE_R_MM5

6d23h: ISAKMP:(0:5:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435461): ID payload
        next-payload : 6
        type          : 2
        FQDN name     : Router1.cisco.com
        protocol      : 17
        port          : 500
        length        : 28
6d23h: ISAKMP:(0:5:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:5:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:5:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:5:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:5:HW:2): OU = green
6d23h: ISAKMP:(0:5:HW:2): certificate map matches certpro profile
6d23h: ISAKMP:(0:5:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:5:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:5:HW:2): CERT validity confirmed.
6d23h: ISAKMP:(0:5:HW:2):Profile has no keyring, aborting key search
6d23h: ISAKMP:(0:5:HW:2): Profile certpro assigned peer the group named new_group

```

Additional References

Related Documents

Related Topic	Document Title
Configuring ISAKMP profiles	VRF-Aware IPsec
Security commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Certificate to ISAKMP Profile Mapping

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 **Feature Information for Certificate to ISAKMP Profile Mapping**

Feature Name	Releases	Feature Information
Certificate to ISAKMP Profile Mapping	12.3(8)T 12.2(33)SRA 12.2(33)SXH	<p>The Certificate to ISAKMP Profile Mapping feature enables you to assign an Internet Security Association and Key Management Protocol (ISAKMP) profile to a peer on the basis of the contents of arbitrary fields in the certificate. In addition, this feature allows you to assign a group name to those peers that are assigned an ISAKMP profile.</p> <p>This feature was introduced in the Cisco IOS Release 12.3(8)T</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRA.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SXH.</p>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

© 2004–2009 Cisco Systems, Inc. All rights reserved.

