



Source Interface Selection for Outgoing Traffic with Certificate Authority

The Source Interface Selection for Outgoing Traffic with Certificate Authority feature allows you to specify that the address of an interface be used as the source address for all outgoing TCP connections associated with that trustpoint when a designated trustpoint has been configured.

Feature Specifications for Source Interface Selection for Outgoing Traffic with Certificate Authority

Feature History

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

Supported Platforms

Cisco 1600, Cisco 1600R, Cisco 1710, Cisco 1720, Cisco 1750, Cisco 1751, Cisco 1760, Cisco 2400, Cisco 2610–2613, Cisco 2610XM–2611XM, Cisco 2620–2621, Cisco 2620XM–2621XM, Cisco 2650–2651, Cisco 2650XM–2651XM, Cisco 2691, Cisco 3620, Cisco 3631, Cisco 3640, Cisco 3660, Cisco 3725, Cisco 3745, Cisco 7100, Cisco 7200, Cisco 7400, Cisco 7500, Cisco 801–Cisco 806, Cisco 811, Cisco 813, Cisco 828, Cisco 8850-RPM, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco MC3810, Cisco ubr7200, Cisco ubr905, Cisco ubr925

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

- [Information About Source Interface Selection for Outgoing Traffic with Certificate Authority, page 2](#)
- [How to Configure Source Interface Selection for Outgoing Traffic with Certificate Authority, page 2](#)
- [Configuration Examples for Source Interface Selection for Outgoing Traffic with Certificate Authority, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)

- [Glossary, page 10](#)

Information About Source Interface Selection for Outgoing Traffic with Certificate Authority

To configure the Source Interface Selection for Outgoing Traffic with Certificate Authority feature, you must understand the following concepts:

- [Certificates That Identify an Entity, page 2](#)
- [Source Interface for Outgoing TCP Connections Associated with a Trustpoint, page 2](#)

Certificates That Identify an Entity

Certificates can be used to identify an entity. A trusted server, known as the certification authority (CA), issues the certificate to the entity after determining the identity of the entity. A router that is running Cisco IOS software obtains its certificate by making a network connection to the CA. Using the Simple Certificate Enrollment Protocol (SCEP), the router transmits its certificate request to the CA and receives the granted certificate. The router obtains the certificate of the CA in the same manner using SCEP. When validating a certificate from a remote device, the router may again contact the CA or a Lightweight Directory Access Protocol (LDAP) or HTTP server to determine whether the certificate of the remote device has been revoked. (This process is known as checking the certificate revocation list [CRL].)

In some configurations, the router may make the outgoing TCP connection using an interface that does not have a valid or routable IP address. The user must specify that the address of a different interface be used as the source IP address for the outgoing connection. Cable modems are a specific example of this requirement because the outgoing cable interface (the RF interface) usually does not have a routable address. However, the user interface (usually Ethernet) does have a valid IP address.

Source Interface for Outgoing TCP Connections Associated with a Trustpoint

The **crypto ca trustpoint** command is used to specify a trustpoint. The **source interface** command is used along with the **crypto ca trustpoint** command to specify the address of the interface that is to be used as the source address for all outgoing TCP connections associated with that trustpoint.



Note

If the interface address is not specified using the **source interface** command, the address of the outgoing interface is used.

How to Configure Source Interface Selection for Outgoing Traffic with Certificate Authority

This section includes the following procedure:

- [Configuring the Interface for All Outgoing TCP Connections Associated with a Trustpoint, page 3](#)

Configuring the Interface for All Outgoing TCP Connections Associated with a Trustpoint

Perform this task to configure the interface that you want to use as the source address for all outgoing TCP connections associated with a trustpoint.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ca trustpoint** *name*
4. **enrollment url** *url*
5. **source interface** *interface-address*
6. **interface** *type slot/port*
7. **description** *string*
8. **ip address** *ip-address mask*
9. **interface** *type slot/port*
10. **description** *string*
11. **ip address** *ip-address mask*
12. **crypto map** *map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ca trustpoint <i>name</i> Example: Router (config)# crypto ca trustpoint ms-ca	Declares the Certificate Authority (CA) that your router should use and enters ca-trustpoint configuration mode.
Step 4	enrollment url <i>url</i> Example: Router (ca-trustpoint)# enrollment url http://yourname:80/certsrv/mscep/mscep.dll	Specifies the enrollment parameters of your CA.

	Command or Action	Purpose
Step 5	source interface <i>interface-address</i> Example: Router (ca-trustpoint)# interface ethernet 0	Interface to be used as the source address for all outgoing TCP connections associated with that trustpoint.
Step 6	interface <i>type slot/port</i> Example: Router (ca-trustpoint)# interface ethernet 1	Configures an interface type and enters interface configuration mode.
Step 7	description <i>string</i> Example: Router (config-if)# description inside interface	Adds a description to an interface configuration.
Step 8	ip address <i>ip-address mask</i> Example: Router (config-if)# ip address 10.1.1.1 255.255.255.0	Sets a primary or secondary IP address for an interface.
Step 9	interface <i>type slot/port</i> Example: Router (config-if)# interface ethernet1/0	Configures an interface type.
Step 10	description <i>string</i> Example: Router (config-if)# description outside interface 10.1.1.205 255.255.255.0	Adds a description to an interface configuration.
Step 11	ip address <i>ip-address mask</i> Example: Router (config-if)# ip address 10.2.2.205 255.255.255.0	Sets a primary or secondary IP address for an interface.
Step 12	crypto map <i>map-name</i> Example: Router (config-if)# crypto map mymap	Applies a previously defined crypto map set to an interface.

Troubleshooting Tips

Ensure that the interface specified in the command has a valid address. Attempt to ping the router using the address of the specified interface from another device (possibly the HTTP or LDAP server that is serving the CRL). You can do the same thing by using a traceroute to the router from the external device.

You can also test connectivity between the router and the CA or LDAP server by using Cisco IOS command-line interface (CLI). Enter the **ping ip** command and respond to the prompts. If you answer “yes” to the “Extended commands [n]:” prompt, you will be able to specify the source address or interface.

In addition, you can use Cisco IOS CLI to input a traceroute command. If you enter the **traceroute ip** command (in EXEC mode), you will be prompted for the destination and source address. You should specify the CA or LDAP server as the destination and the address of the interface that you specified in the “source interface” as the source address.

Configuration Examples for Source Interface Selection for Outgoing Traffic with Certificate Authority

This section includes the following example:

- [Source Interface Selection for Outgoing Traffic with Certificate Authority Example, page 5](#)

Source Interface Selection for Outgoing Traffic with Certificate Authority Example

In the following example, the router is located in a branch office. The router uses IP Security (IPSec) to communicate with the main office. Ethernet 1 is the “outside” interface that connects to the Internet Service Provider (ISP). Ethernet 0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office, the router must send its IP datagrams out interface Ethernet 1 (address 10.2.2.205) using the IPSec tunnel. Address 10.2.2.205 is assigned by the ISP. Address 10.2.2.205 is not a part of the branch office or main office.

The CA cannot access any address outside the company because of a firewall. The CA sees a message coming from 10.2.2.205 and cannot respond (that is, the CA does not know that the router is located in a branch office at address 10.1.1.1, which it is able to reach).

Adding the **source interface** command tells the router to use address 10.1.1.1 as the source address of the IP datagram that it sends to the CA. The CA is able to respond to 10.1.1.1.

This scenario is configured using the **source interface** command and the interface addresses as described above.

```
crypto ca trustpoint ms-ca
  enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
  source interface ethernet0
!
interface ethernet 0
  description inside interface
  ip address 10.1.1.1 255.255.255.0
!
interface ethernet 1
  description outside interface
  ip address 10.2.2.205 255.255.255.0
  crypto map main-office
```

Additional References

For additional information related to Source Interface Selection for Outgoing Traffic with Certificate Authority, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring IPsec and certification authority	Cisco IOS Security Configuration Guide , Release 12.2
IPsec and certification authority commands	Cisco IOS Security Command Reference , Release 12.2 T

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	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: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

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. 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
No new or modified RFCs are supported by this feature.	—

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.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

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

- [source interface](#)

source interface

To specify the address of an interface to be used as the source address for all outgoing TCP connections associated with a trustpoint, use the **source interface** command in ca-trustpoint configuration mode. To disable the interface that was specified, use the **no** form of this command.

source interface *interface-name*

no source interface *interface-name*

Syntax Description

<i>interface-name</i>	Interface address to be used as the source address for all outgoing TCP connections associated with a trustpoint.
-----------------------	---

Defaults

If this command is not specified, the address of the outgoing interface is used.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

This command must be used following the **crypto ca trustpoint** command. If this command is used and the address of the outgoing interface is specified, the router uses the specified address (or address of the specified interface) as the source address for any datagrams that are sent to the certification authority (CA) server or Lightweight Directory Access Protocol (LDAP) server during authentication, enrollment, and if appropriate, when obtaining certificate revocation lists (CRLs).

In the following example, the router is located in a branch office. The router uses IP Security (IPSec) to communicate with the main office. Ethernet 1 is the “outside” interface that connects to the Internet Service Provider (ISP). Ethernet 0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office the router needs to send its IP datagrams out interface Ethernet 1 (address 10.2.2.205) using the IPSec tunnel. Address 10.2.2.205 is assigned by the ISP. Address 10.2.2.205 is not a part of the branch office or main office.

The CA cannot access any address outside the company because of a firewall. The CA sees a message coming from 10.2.2.205 and cannot respond (that is, it does not know that the router is located in a branch office at address 10.1.1.1, which it is able to reach).

Adding the **source interface** command tells the router to use address 10.1.1.1 as the source address of the IP datagram that it sends to the CA. The CA is able to respond to 10.1.1.1.

This scenario is configured using the **source interface** command and the interface addresses as described above.

```
crypto ca trustpoint ms-ca
  enrollment url http://yourname:80/certsrv/mscep/mscep.dll
  source interface ethernet0
!
interface ethernet 0
```

```
description inside interface
ip address 10.1.1.1 255.255.255.0
!
interface ethernet 1
description outside interface
ip address 10.2.2.205 255.255.255.0
crypto map main-office
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

Glossary

authenticate—To prove the identity of an entity using the certificate of an identity and a secret that the identity poses (usually the private key corresponding to the public key in the certificate).

CA—Certificate Authority. A CA is an entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

CA authentication—The user manually approves a certificate from a root CA. Usually a fingerprint of the certificate is presented to the user, and the user is asked to accept the certificate based on the fingerprint. The certificate of a root CA is signed by itself (self-signed) so that it cannot be automatically authenticated using the normal certificate verification process.

CRL—certificate revocation list. A CRL is a data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire.

enrollment—A router receives its certificate via the enrollment process. The router generates a request for a certificate in a specific format (known as PKCS #10). The request is transmitted to a CA, which grants the request and generates a certificate encoded in the same format as the request. The router receives the granted certificate and stores it in an internal database for use during normal operations.

certificate—A data structure defined in International Organization for Standardization (ISO) standard X.509 to associate an entity (machine or human) with the public key of that entity. The certificate contains specific fields, including the name of the entity. The certificate is normally issued by a CA on behalf of the entity. In this case the router will act as its own CA. Common fields within a certificate include the distinguished name (DN) of the entity, the DN of the authority issuing the certificate, and the public key of the entity.

LDAP—Lightweight Directory Access Protocol. A LDAP is a protocol that provides access for management and browser applications that provide read-and-write interactive access to the X.500 directory.



Note

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.
