Source Interface Selection for Outgoing Traffic with Certificate Authority

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

- Information About Source Interface Selection for Outgoing Traffic with Certificate Authority, on page 1
- How to Configure Source Interface Selection for Outgoing Traffic with Certificate Authority, on page 2
- Configuration Examples for Source Interface Selection for Outgoing Traffic with Certificate Authority, on page 5
- Feature History for Source Interface Selection for Outgoing Traffic with Certificate Authority, on page 5

Information About Source Interface Selection for Outgoing Traffic with Certificate Authority

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 device that is running Cisco IOS XE software obtains its certificate by making a network connection to the CA. Using the Simple Certificate Enrollment Protocol (SCEP), the device transmits its certificate request to the CA and receives the granted certificate. The device obtains the certificate of the CA in the same manner using SCEP. When validating a certificate from a remote device, the device 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Directory Access Protocol (LDAP) or HTTP server to determine whether the certificate of the remote device has been revoked.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 device may make the outgoing TCP connection using an interface that does not have a valid or IP address that can be routed. 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 an IP address that can be routed. 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

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.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ca trustpoint** *name* **Example:** `Device(config)# crypto ca trustpoint ms-ca`	Declares the Certificate Authority (CA) that your device should use and enters ca-trustpoint configuration mode.
Step 4	**enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**] **Example:**	Specifies the following enrollment parameters of the CA: • (Optional) The **mode** keyword specifies the registration authority (RA) mode, if

	Command or Action	Purpose

	`Device(ca-trustpoint)# enrollment url http://caserver.myexample.com`
	- or-
	`Device(ca-trustpoint)# enrollment url http://[2001:DB8:1:1::1]:80`
		your CA system provides an RA. By default, RA mode is disabled.
		• (Optional) The **retry period** keyword and *minutes* argument specifies the period, in minutes, in which the device waits before sending the CA another certificate request. Valid values are from 1 to 60. The default is 1.
		• (Optional) The **retry count** keyword and *number* argument specifies the number of times a device will resend a certificate request when it does not receive a response from the previous request. Valid values are from 1 to 100. The default is 10.
		• The *url* argument is the URL of the CA to which your device should send certificate requests.
		• (Optional) The **pem** keyword adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Step 5	**source interface** *interface-address* **Example:** `Device(ca-trustpoint)# source interface gigabitethernet 0/1/0`	Interface to be used as the source address for all outgoing TCP connections associated with that trustpoint.
Step 6	**exit** **Example:** `Device(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 7	**interface** *type slot / port* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Configures an interface type and enters interface configuration mode.
Step 8	**description** *string* **Example:** `Device(config-if)# description inside interface`	Adds a description to an interface configuration.

	Command or Action	Purpose
Step 9	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**interface** *type slot/port* **Example:** `Device(config-if)# interface gigabitethernet 1/0/2`	Configures an interface and enters interface configuration mode.
Step 12	**description** *string* **Example:** `Device(config-if)# description outside interface 10.1.1.205 255.255.255.0`	Adds a description to an interface configuration.
Step 13	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.2.2.205 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 14	**crypto map** *map-name* **Example:** `Device(config-if)# crypto map mymap`	Applies a previously defined crypto map set to an interface and enters crypto map configuration mode.
Step 15	**end** **Example:** `Device(config-crypto-map)# end`	Exits crypto map configuration mode and returns to privileged EXEC mode.

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

Example:Source Interface Selection for Outgoing Traffic with Certificate Authority

In the following example, the device is located in a branch office. The device uses IPSec to communicate with the main office.GigabitEthernet 1/0/1 is the “outside” interface that connects to the ISP. GigabitEthernet 0/1/0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office, the device 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 device 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 device 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.

```
Device> enable
Device# configure terminal
Device(config)# crypto ca trustpoint ms-ca
Device(ca-trustpoint)# enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
Device(ca-trustpoint)# source interface gigabitethernet 0/1/0
Device(ca-trustpoint)# exit
Device(onfig)# interface gigabitethernet 0/1/0
Device(config-if)# description inside interface
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# description outside interface
Device(config-if)# ip address 10.2.2.205 255.255.255.0
Device(config-if)# crypto map main-office
Device(config-if)# end
```

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

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.8.1a	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. Support for this feature was introduced on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.