client through crl

client

To specify a RADIUS client from which a device can accept Change of Authorization (CoA) and disconnect requests, use the **client** command in dynamic authorization local server configuration mode. To remove this specification, use the **no** form of this command.

client {*hostname* | *ip-address*} [**server-key** {**0** *string* | **6** *string* | **7** *string* | *string*} | **vrf** *vrf-id*]

no client {*hostname* | *ip-address*} [**server-key** {**0** *string* | **6** *string* | **7** *string* | *string*} | **vrf** *vrf-id*]

Syntax Description

hostname	Hostname of the RADIUS client.
ip-address	IP address of the RADIUS client.
server-key	(Optional) Configures the RADIUS key to be shared between a device and a RADIUS client.
0 *string*	Specifies that an unencrypted key follows. • *string*—The unencrypted (clear text) shared key.
6 *string*	Specifies that an encrypted key follows. • *string*—The advanced encryption scheme [AES] encrypted key.
7 *string*	Specifies that a hidden key follows. • *string*—The hidden shared key.
string	The unencrypted (clear text) shared key.
vrf *vrf-id*	(Optional) Virtual routing and forwarding (VRF) ID of the client.

Command Default

CoA and disconnect requests are dropped.

Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.

Release	Modification
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T. The **6** keyword was added.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **client** command to specify the RADIUS clients for which the router can act as server.

Examples

The following example shows how to configure the router to accept requests from the RADIUS client at IP address 10.0.0.1:

```
aaa server radius dynamic-author
 client 10.0.0.1 key cisco
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures an ISG as a AAA server to facilitate interaction with an external policy server.

crl

To specify the certificate revocation list (CRL) query and CRL cache options for the public key infrastructure (PKI) trustpool, use the **crl** command in ca-trustpool configuration mode. To return to the default behavior in which the router checks the URL that is embedded in the certificate, use the **no** form of this command.

crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

no crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

Syntax Description

cache	Specifies CRL cache options.
delete-after	Removes the CRL from cache after a timeout.
minutes	The number of minutes from 1 to 43200 to wait before deleting CRL from cache.
none	Specifies that CRLs are not cached.
query *url*	Specifies the URL published by the certification authority (CA) server to query the CRL.

Command Default

The CRL is not queried and no CRL cache parameters are configured.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

The **crl query** command is used if the CDP is in Lightweight Directory Access Protocol (LDAP) form, which means that the CDP location in the certificate indicates only where the CRL distribution point (CDP) is located in the directory; that is, the CDP does not indicate the actual query location for the directory.

The Cisco IOS software queries the CRL to ensure that the certificate has not been revoked in order to verify a peer certificate (for example, during Internet Key Exchange (IKE) or Secure Sockets Layer (SSL) handshake). The query looks for the CDP extension in the certificate, which is used to download the CRL. If this query is

unsuccessful, then the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports the following CDP entries:

- HTTP URL with a hostname. For example: http://myurlname/myca.crl
- HTTP URL with an IPv4 address. For example: http://10.10.10.10:81/myca.crl
- LDAP URL with a hostname. For example: ldap://CN=myca, O=cisco
- LDAP URL with an IPv4 address. For example: ldap://10.10.10.10:3899/CN=myca, O=cisco
- LDAP/X.500 DN. For example: CN=myca, O=cisco

The Cisco IOS needs a complete URL in order to locate the CDP.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# crl query http://www.cisco.com/security/pki/crl/crca2048.crl
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.

Command	Description
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.