OCSP Response Stapling

The OCSP Response Stapling feature allows you to check the validity of a peer's user or device credentials contained in a digital certificate using Online Certificate Status Protocol (OCSP).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Information About OCSP Response Stapling

Overview of OCSP Response Stapling

Online Certificate Status Protocol (OCSP) is a method to check certificate revocation when a peer has to retrieve this revocation information and then validate it to check the certificate revocation status. In this method, the certification revocation status is limited by the peer's ability to reach an OCSP responder through the cloud or by the certificate sender's performance in retrieving the certificate revocation-information.

OCSP response stapling supports a new method to fetch the OCSP response for a device’s own certificates. This feature allows the device to obtain its own certificate revocation information by contacting the OCSP server and then sending this result along with its certificates directly to the peer. As a result, the peer does not require to contact the OCSP responder.

How to Configure OCSP Response Stapling

Configuring PKI Client to Request EKU Attribute

Perform this task to configure OCSP (Online Certificate Status Protocol) response stapling.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **ocsp url** *url*
5. **eku request** *attribute*
6. **match eku** *attribute*
7. **revocation-check** *method1* [*method2* [*method3*]]
8. **exit**
9. **exit**
10. **show cry pki counters**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. **a.** Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpoint** *name* **Example:** `Device(config)# crypto pki trustpoint msca`	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.

Step 4	**ocsp url** *url*
	Example:
	`Device(ca-trustpoint)# ocsp url http://ocsp-server`
	Example:
	`Device(ca-trustpoint)# ocsp url http://10.10.10.1:80`
	Example:
		The *url* argument specifies the URL of an OCSP server so that the trustpoint can check the certificate status. This URL overrides the URL of the OCSP server (if one exists) in the Authority Info Access (AIA) extension of the certificate. All certificates associated with a configured trustpoint are checked by the OCSP server. The URL can be a hostname, IPv4 address, or an IPv6 address.
		Note Make sure that the OCSP request url is configured with the **ocsp url** *url* command and not with an http-proxy server.

	Command or Action	Purpose
	`Device(ca-trustpoint)# ocsp url http://[2001DB8:1:1::2]:80`	
Step 5	**eku request** *attribute* **Example:** `Device(ca-trustpoint)# eku request ssh-client`	Requests to include specified eku *attribute* in the certificate. This request, when configured on the PKI client, will be sent to the CA server during enrollment. The *attribute* argument can be one of the following: • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • time-stamping • ssh-server • ssh-client
Step 6	**match eku** *attribute* **Example:** `Device(ca-trustpoint)# match eku client-auth`	Allows PKI to validate a peer certificate only if the specified attribute is present in the certificate else validation fails. The *attribute* argument can be one of the following: • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • time-stamping • ssh-server • ssh-client

	Command or Action	Purpose
Step 7	**revocation-check** *method1* [*method2* [*method3*]] **Example:** `Device(ca-trustpoint)# revocation-check ocsp none`	(Optional) Checks the revocation status of a certificate. • crl --Certificate checking is performed by a CRL. This is the default option. • none --Certificate checking is ignored. • ocsp --Certificate checking is performed by an OCSP server. If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.
Step 8	**exit** **Example:** `Device(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 9	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 10	**show cry pki counters** **Example:** `Device# show cry pki counters`	(Optional) Displays the PKI counters of the device.

Configuring PKI Server to Include EKU Attributes

Perform this task to configure OCSP (Online Certificate Status Protocol) response stapling.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **eku request** *attribute*
6. **exit**
7. **exit**
8. **show crypto pki counters**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. **a.** Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server on your system.
Step 4	**crypto pki server** *cs-label* **Example:** `Device(config)# crypto pki server server-pki`	Defines a label for the certificate server and enters certificate server configuration mode. **Note** If you manually generated an RSA key pair, the *cs-label* argument must match the name of the key pair.
Step 5	**eku request** *attribute* **Example:** `Device(cs-server)# eku request ssh-server`	Requests to include specified eku *attribute* in the certificate. The *attribute* argument can be one of the following: • client-auth • code-signing • email-protection • ipsec-end-system • ipsec-tunnel • ipsec-user • ocsp-signing • server-auth • time-stamping • ssh-server • ssh-client
Step 6	**exit** **Example:** `Device(cs-server)# exit`	Exits cs-server configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 8	**show crypto pki counters** **Example:** `Device# show crypto pki counters`	(Optional) Displays the PKI counters of the device.

Example

The following is sample output from the **show crypto pki counters**.

```
Device# show crypto pki counters

PKI Sessions Started: 0
PKI Sessions Ended: 0
PKI Sessions Active: 0
Successful Validations: 0
Failed Validations: 0
Bypassed Validations: 0
Pending Validations: 0
CRLs checked: 0
CRL - fetch attempts: 0
CRL - failed attempts: 0
CRL - rejected busy fetching: 0
OCSP - fetch requests: 0
OCSP - received responses: 0
OCSP - failed attempts: 0
OCSP - staple requests: 0
AAA authorizations: 0
```

Additional References for OCSP Response Stapling

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z

Standards and RFCs

Standard/RFC	Title
RFC 2560	*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*
RFC 4806	*Online Certificate Status Protocol (OCSP) Extensions to IKEv2*
RFC 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
RFC 6187	*X.509v3 Certificates for Secure Shell Authentication*
RFC 6066	*Transport Layer Security (TLS) Extensions: Extension Definitions*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for OCSP Response Stapling

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for OCSP Response Stapling

Feature Name	Releases	Feature Information
OCSP Response Stapling		This feature allows you to check the validity of a peer's user or device credentials contained in a digital certificate using Online Certificate Status Protocol (OCSP).