



Online Certificate Status Protocol (OCSP)

The Online Certificate Status Protocol (OCSP) feature allows users to enable OCSP instead of certificate revocation lists (CRLs) to check certificate status. Unlike CRLs, which provide only periodic certificate status, OCSP can provide timely information regarding the status of a certificate.

Feature History for Online Certificate Status Protocol (OCSP)

Feature History

Release	Modification
12.3(2)T	This feature was introduced.

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

- [Restrictions for Online Certificate Status Protocol \(OCSP\), page 2](#)
- [Information About Online Certificate Status Protocol \(OCSP\), page 2](#)
- [How to Use OCSP, page 2](#)
- [Configuration Examples for OCSP Server, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Restrictions for Online Certificate Status Protocol (OCSP)

- OCSP transports messages over HTTP, so there may be a time delay when you access the OCSP server. If the OCSP server is unavailable, certificate verification will fail.
- The increased certificate size may cause a problem for low-end routers when certificates are stored on NVRAM. Thus, before you add the Authority Info Access (AIA) extension to a certificate, make ensure that the increased size will not cause deployment problems.

Information About Online Certificate Status Protocol (OCSP)

To configure an OCSP server to check certificate status, you should understand the following concept:

- [OCSP Benefits, page 2](#)

OCSP Benefits

- OCSP provides revocation status information more frequently than CRLs, which provide only periodic updates.
- OCSP allows a network administrator to configure a central OCSP server to collect and update CRLs from different certification authority (CA) servers; thus, the devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every device.

How to Use OCSP

This section contains the following procedures:

- [Configuring an OCSP Server, page 2](#)
- [Verifying Certificate Information, page 5](#)

Configuring an OCSP Server

Use this task to configure your router for OCSP to check certificate status.

OCSP Server: Pushing and Polling Revocation Consideration

An OCSP server usually operates in either push or poll mode. You can configure a CA server to push revocation information to an OCSP server or configure an OCSP server to periodically download (poll) a CRL from the CA server. To ensure that timely certificate revocation status is obtained, you should carefully consider the “push and poll” interval.

Prerequisites

When configuring an OCSP server to return the revocation status for a CA server, the OCSP server must be configured with an OCSP response signing certificate that is issued by that CA server. Ensure that the signing certificate is in the correct format, or the router will not accept the OCSP response. Refer to your OCSP manual for additional information.

The following is a sample OCSP response certificate signing. Note that the extensions are in bold.

```
Certificate:
  Data:
    Version: v3
    Serial Number:0x14
    Signature Algorithm:MD5withRSA - 1.2.840.113549.1.1.4
    Issuer:CN=CA server,OU=PKI,O=Cisco Systems
    Validity:
      Not Before:Thursday, August 8, 2002 4:38:05 PM PST
      Not After:Tuesday, August 7, 2003 4:38:05 PM PST
    Subject:CN=OCSP server,OU=PKI,O=Cisco Systems
    Subject Public Key Info:
      Algorithm:RSA - 1.2.840.113549.1.1.1
      Public Key:
        Exponent:65537
        Public Key Modulus:(1024 bits) :
          <snip>

    Extensions:
      Identifier:Subject Key Identifier - 2.5.29.14
      Critical:no
      Key Identifier:
        <snip>

      Identifier:Authority Key Identifier - 2.5.29.35
      Critical:no
      Key Identifier:
        <snip>

      Identifier:OCSP NoCheck:- 1.3.6.1.5.5.7.48.1.5
      Critical:no
      Identifier:Extended Key Usage:- 2.5.29.37
      Critical:no
      Extended Key Usage:
      OCSPSigning
      Identifier:CRL Distribution Points - 2.5.29.31
      Critical:no
      Number of Points:1
      Point 0
        Distribution Point:
          [URIName:ldap://CA-server/CN=CA server,OU=PKI,O=Cisco Systems]
    Signature:
      Algorithm:MD5withRSA - 1.2.840.113549.1.1.4
      Signature:
        <snip>
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint *name***
4. **ocsp url *url***
5. **revocation-check *method1* [*method2* [*method3*]]**

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 pki trustpoint <i>name</i> Example: Router(config)# crypto pki trustpoint strawberry	Declares the CA that your router should use and puts you in ca-trustpoint configuration mode.
Step 4	ocsp url <i>url</i> Router(ca-trustpoint)# ocsp url http://ocspserver.cisco.com:81	(Optional) Specifies the URL of an OCSP server so that the trustpoint can check the certificate status. This URL will override the URL of the OCSP server (if one exists) in Authority Info Access (AIA) extension of the certificate.
Step 5	revocation-check <i>method1</i> [<i>method2</i> [<i>method3</i>]] Router(ca-trustpoint)# revocation-check ocsp none	Checks the revocation status of a certificate. <ul style="list-style-type: none"> • cr1—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.

Verifying Certificate Information

To verify certificate and trustpoint information, perform the following optional steps.

SUMMARY STEPS

1. `enable`
2. `show crypto pki certificates`
3. `show crypto pki trustpoints`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>show crypto pki certificates</code> Example: Router# <code>show crypto pki certificates</code>	Displays information about your certificate and the CA certificate.
Step 3	<code>show crypto pki trustpoints</code> Example: Router# <code>show crypto pki trustpoints</code>	Displays the trustpoints and configured trustpoint subcommands that are configured in the router.

Configuration Examples for OCSP Server

The following section provides configuration examples that show alternate ways to configure your router for certificate checking:

- [OCSP Server Configuration Example, page 5](#)
- [CRL Then OCSP Server Configuration Example, page 6](#)
- [Specific OCSP Server Configuration Example, page 6](#)

OCSP Server Configuration Example

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp
```

CRL Then OCSP Server Configuration Example

The following example shows how to configure the router to download the CRL from the CRL distribution point (CDP); if the CRL is unavailable, the OCSP server that is specified in the AIA extension of the certificate will be used. If both options fail, certificate verification will also fail.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsf
```

Specific OCSP Server Configuration Example

The following example shows how to configure your router to use the OCSP server at the HTTP URL “http://myocspserver:81.” If the server is down, revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsf url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsf none
```

Additional References

The following sections provide references related to OCSP.

Related Documents

Related Topic	Document Title
Additional CA configuration tasks	The chapter “Configuring Certification Authority Interoperability” in the <i>Cisco IOS Security Configuration Guide</i>
Additional CA commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	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

RFCs

RFCs	Title
RFC 2560	<i>X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP</i>

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 new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 T command reference publications.

- [ocsp url](#)
- [revocation-check](#)

ocsp url

To specify the URL of an online certificate status protocol (OCSP) server to override the OCSP server URL (if one exists) in Authority Info Access (AIA) extension of the certificate, use the **ocsp url** command in ca-trustpoint configuration mode. To disable the OCSP server, use the **no** form of this command.

ocsp url *url*

no ocsp url *url*

Syntax Description

<i>url</i>	All certificates associated with a configured trustpoint will be checked by the OCSP server at the specified HTTP URL.
------------	--

Defaults

Uses the OCSP server URL in AIA extension of the certificate. If a URL does not exist, revocation check will fail.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

A central OCSP server can be configured to collect and update certificate revocation lists (CRLs) from different certification authority (CA) servers. Thus, the devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every device.

If the *url* option is not enabled, the certificate will be checked by the OCSP server in the Authority Info Access (AIA) extension of the certificate.

Examples

The following example shows how to configure your router to use the OCSP server at the HTTP URL "http://myocspserver:81." If the server is down, revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

revocation-check

To check the revocation status of a certificate, use the **revocation-check** command in ca-trustpoint configuration mode. To disable this functionality, use the **no** form of this command.

```
revocation-check method1 [method2[method3]]
```

```
no revocation-check method1 [method2[method3]]
```

Syntax Description

<i>method1</i> [<i>method2[method3]</i>]	Method used by the router to check the revocation status of the certificate. Available methods are as follows: <ul style="list-style-type: none"> • cr1—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • none—Certificate checking is not required. • ocsp—Certificate checking is performed by an online certificate status protocol (OCSP) server. <p>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.</p>
---	--

Defaults

After a trustpoint is enabled, the default is set to **revocation-check cr1**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced. This command replaced the cr1 best-effort and cr1 optional commands.

Usage Guidelines

Use the **revocation-check** command to ensure that the certificate of a peer has not been revoked.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the certificate of the peer—unless you include the **none** keyword in your configuration. If you use the **none** keyword, your router will check the CRL if it is cached in the router memory, but it will not download the CRL from the CRL distribution point (CDP). If the **none** keyword is configured and a CRL is not available, the certificate will always be accepted. If the **revocation-check none** command is configured, you cannot manually download the CRL via the **crypto pki cr1 request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL can cause all certificate verifications to be denied.

**Note**

If you enter the **crl optional** command, it will be written back as the **revocation-check none** command.

Also, the **crl** and **none** keywords issued together replace the **crl best-effort** command. If you enter the **crl best-effort** command, it will be written back as the **revocation-check crl none** command.

Examples

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsf
```

The following example shows how to configure the router to download the CRL from the CDP; if the CRL is unavailable, the OCSP server that is specified in the Authority Info Access (AIA) extension of the certificate will be used. If both options fail, certificate verification will also fail.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsf
```

The following example shows how to configure your router to use the OCSP server at the HTTP URL “http://myocspserver:81.” If the server is down, revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsf none
```

Related Commands

Command	Description
crl query	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki trustpoint	Declares the CA that your router should use.
ocsp url	Enables an OCSP server.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

