



Secure Device Provisioning Certificate-Based Authorization

The Secure Device Provisioning (SDP) Certificate-Based Authorization feature allows certificates issued by other certificate authority (CA) servers to be used for SDP introductions.

Feature History for SDP Certificate-Based Authorization

Release	Modification
12.3(14)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

- [Prerequisites for SDP Certificate-Based Authorization, page 2](#)
- [Restrictions for SDP Certificate-Based Authorization, page 2](#)
- [Information About SDP Certificate-Based Authorization, page 2](#)
- [How to Configure SDP Certificate-Based Authorization, page 4](#)
- [Configuration Examples for SDP Certificate-Based Authorization, page 8](#)
- [Additional References, page 11](#)
- [Command Reference, page 13](#)
- [Glossary, page 22](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Prerequisites for SDP Certificate-Based Authorization

- SDP must be configured and operational.
- Your SDP petitioner device must have an existing manufacturer's or a third-party certificate.
- You must understand how to use SDP, formerly called Easy Secure Device Deployment (EzSDD). (See the *Easy Secure Device Deployment* feature module for more information.)

Restrictions for SDP Certificate-Based Authorization

Since remote authentication dial-in user service (RADIUS) does not differentiate between authentication and authorization, you need to use the default password, cisco, for certificate authorization.

Information About SDP Certificate-Based Authorization

To use the SDP Certificate-Based Authorization feature, you need to understand the following concepts:

- [Feature Overview of SDP Certificate-Based Authorization, page 2](#)
- [Benefits of SDP Certificate-Based Authorization, page 3](#)

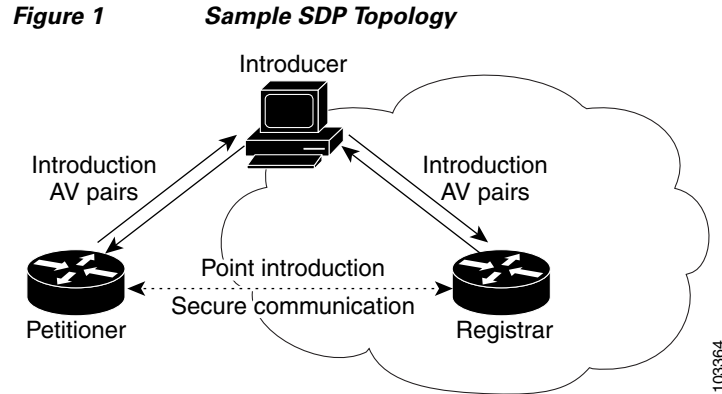
Feature Overview of SDP Certificate-Based Authorization

When the registrar receives an introduction request via the secure HTTP server, the registrar does an authentication, authorization, and accounting (AAA) lookup based on the introducer's username and password to authorize the request. The registrar checks the integrity of the request by verifying the request signature using the petitioner-signing certificate.

Because the petitioner certificate is self-signed, it is just used to convey the public key of the petitioner. No verification or authorization check is done on the certificate. This basically means authorization is per-user based and no per-device information is used.

There are some scenarios when per-device authorization is preferred. Therefore, if the petitioner is able to use certificates issued by other CA servers for SDP transactions, the existing PKI infrastructure can be used and authorization can be achieved over the certificate attributes.

[Figure 1](#) shows a sample SDP topology with an introducer, a petitioner (with an existing certificate), and a registrar.



Benefits of SDP Certificate-Based Authorization

Enhanced Security Through Improved Authorization

The SDP Certificate-Based Authorization feature provides authorization of the specific device being deployed. Previously, introducer-to-petitioner device communication was secured only using physical security between the introducer and the petitioner device. SDP certificate-based authorization gives the registrar an opportunity to validate the current device identity before accepting the introduction.

How to Configure SDP Certificate-Based Authorization

This section contains the following procedures:

- [Configuring the Petitioner, page 4](#) (required)
- [Configuring the Registrar, page 5](#) (required)
- [Verifying the Configuration, page 6](#) (optional)

Configuring the Petitioner

Perform the following task to configure the petitioner to use a certificate and the Rivest, Shamir, and Adelman (RSA) keys associated with a specific trustpoint.



Note

By default, the SDP petitioner device uses an existing certificate. If multiple certificates and one specific certificate exist, use the following commands to make a choice. However, these commands are not necessary to enable the default behavior.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto provisioning petitioner**
4. **trustpoint signing *trustpoint-label***
5. **end**



Note

For other SDP parameters that you can configure, see the [Easy Secure Device Deployment](#) feature module.

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 provisioning petitioner Example: Router(config)# crypto provisioning petitioner	Allows SDP petitioner device behavior to be modified and enters tti-petitioner configuration mode. Note Effective with Cisco IOS Release 12.3(14)T, the crypto provisioning petitioner command replaced the crypto wui tti petitioner command.

	Command or Action	Purpose
Step 4	trustpoint signing <i>trustpoint-label</i> Example: Router(tti-petitioner)# trustpoint signing mytrust	Specifies the trustpoint and associated certificate to be used when signing all introduction data during the SDP exchange.
Step 5	end Example: Router(tti-petitioner)# end	(Optional) Exits tti-petitioner configuration mode.

Configuring the Registrar

Perform the following tasks to configure the registrar:

- Verify the petitioner-signing certificate using a specified trustpoint or any configured trustpoint.
- Initiate authorization lookups using the introducer username and the certificate name field.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto provisioning registrar**
4. **authentication trustpoint** {*trustpoint-label* | **use-any**}
5. **authorization** {**login**} | {**certificate**} | {**login certificate**}
6. **authorization username** {**subjectname** *subjectname*}
7. **end**

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 provisioning registrar Example: Router(config)# crypto provisioning registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode. Note Effective with Cisco IOS Release 12.3(14)T, the crypto provisioning registrar command replaced the crypto wui tti registrar command.

Command or Action	Purpose
<p>Step 4</p> <pre>authentication trustpoint {trustpoint-label use-any}</pre> <p>Example: Router(tti-registrar)# authentication trustpoint mytrust</p>	<p>(Optional) Specifies the trustpoint used to authenticate the SDP petitioner device’s existing certificate.</p> <ul style="list-style-type: none"> Use the <i>trustpoint-label</i> argument to specify a specific trustpoint or the use-any keyword to specify any configured trustpoint. <p>Note If you do not use this command to specify a trustpoint, then the existing petitioner certificate is not validated. (This provides compatibility with self-signed petitioner certificates.)</p>
<p>Step 5</p> <pre>authorization {login} {certificate} {login certificate}</pre> <p>Example: Router(tti-registrar)# authorization login certificate</p>	<p>(Optional) Enables AAA authorization for an introducer or a certificate.</p> <ul style="list-style-type: none"> Use the login keyword for authorization based on the introducer’s username. Use the certificate keyword for authorization based on the petitioner’s certificate. Use both the login and certificate keywords for authorization based on the introducer’s username and the petitioner’s certificate.
<p>Step 6</p> <pre>authorization username {subjectname subjectname}</pre> <p>Example: Router(tti-registrar)# authorization username subjectname all</p>	<p>Sets parameters for the different certificate fields that are used to build the AAA username.</p> <ul style="list-style-type: none"> The all keyword specifies that the entire subject name of the certificate is used as the authorization username. <p>Note See the PKI AAA Authorization Using the Entire Subject Name feature module for more information about AAA usernames.</p>
<p>Step 7</p> <pre>end</pre> <p>Example: Router(tti-registrar)# end</p>	<p>(Optional) Exits tti-registrar configuration mode.</p>

Verifying the Configuration

Perform the following task to verify that the SDP parameters have been configured.

SUMMARY STEPS

- enable
- show running-config [system | mod_num] [all]
- end

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>show running-config [system <i>mod_num</i>] [all]</p> <p>Example: Router# show running-config</p>	<p>(Optional) Displays the configuration information currently running on the router.</p> <ul style="list-style-type: none"> • Enter the optional system keyword to display the system configuration. • Enter the optional <i>mod_num</i> argument for the number of the module. • Enter the optional all keyword to specify all modules and system configuration information, including the IP address.
Step 3	<p>end</p> <p>Example: Router# end</p>	<p>(Optional) Exits privileged EXEC mode.</p>

Configuration Examples for SDP Certificate-Based Authorization

This section contains the following configuration examples:

- [Configuring the Petitioner: Example, page 8](#)
- [Configuring the Registrar: Example, page 8](#)
- [Verifying the Configuration: Example, page 8](#)

Configuring the Petitioner: Example

In the following example, a petitioner is configured to use the certificate issued by the trustpoint named mytrust:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# crypto provisioning petitioner

Router(tti-petitioner)# trustpoint signing mytrust

Router(tti-petitioner)# end
```

Configuring the Registrar: Example

In the following example, a registrar is configured to verify the petitioner-signing certificate and to perform authorization lookups:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# crypto provisioning registrar

Router(tti-registrar)# authentication trustpoint mytrust

Router(tti-registrar)# authorization login certificate

Router(tti-registrar)# authorization username subjectname all

Router(tti-registrar)# end
```

Verifying the Configuration: Example

The following example from the **show running-config** command verifies that the petitioner, the registrar, and related parameters have been configured:

```
Router# show running-config

Building configuration...

Current configuration : 2700 bytes
!
```

```
! Last configuration change at 01:22:26 GMT Fri Feb 4 2005
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
enable secret 5 $1$tpBS$PXnBDTIDXfX5pWa//1JX20
enable password lab
!
aaa new-model
!
aaa authentication login user_aalist group tacacs+
aaa authorization network user_aalist group tacacs+
aaa authentication login admin_aalist group radius
aaa authorization network admin_aalist group radius
!
!
aaa session-id common
!
resource manager
!
clock timezone GMT 0
ip subnet-zero
no ip routing
!
!
no ip dhcp use vrf connected
!
!
no ip cef
no ip domain lookup
ip domain name cisco.com
ip host router 10.3.0.6
ip host router.cisco.com 10.3.0.6
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
crypto pki server mycs
!
crypto pki trustpoint mycs
  revocation-check crl
  rsakeypair mycs
!
crypto pki trustpoint tti
  revocation-check crl
  rsakeypair tti
!
crypto pki trustpoint mic
  enrollment url http://router:80
  revocation-check crl
!
crypto pki trustpoint foo
  revocation-check crl
!
!
```

```

!
crypto pki certificate map foo 10
!
crypto pki certificate chain mycs
  certificate ca 01
crypto pki certificate chain tti
crypto pki certificate chain mic
  certificate 02
  certificate ca 01
crypto pki certificate chain foo
!
crypto provisioning registrar <----- !SDP registrar device parameters!
pki-server mycs
authentication list user_aalist
authentication trustpoint mytrust
authorization list existingcerts_aalist
authorization login certificate
authorization username subjectname all
!
no crypto engine onboard 0
username qa privilege 15 password 0 lab
!
!
!

```

Additional References

The following sections provide references related to the SDP Certificate-Based Authorization feature.

Related Documents

Related Topic	Document Title
PKI AAA functionality	<i>PKI AAA Authorization Using the Entire Subject Name</i> feature module, Release 12.3(11)T
SDP, including the SDP web page	<i>Easy Secure Device Deployment</i> feature module, Release 12.3(7)T
Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T
Security features including trustpoints, certificate enrollment, and authentication	<i>Cisco IOS Security Configuration Guide</i> , Release 12.3

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of 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/techsupport

Command Reference

This section documents new commands.

- [authentication trustpoint](#)
- [authorization \(tti-registrar\)](#)
- [authorization username \(tti-registrar\)](#)
- [trustpoint signing](#)

authentication trustpoint

To specify the trustpoint used to authenticate the Secure Device Provisioning (SDP) petitioner device's existing certificate, use the **authentication trustpoint** command in tti-registrar configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

authentication trustpoint {*trustpoint-label* | **use-any**}

no authentication trustpoint {*trustpoint-label* | **use-any**}

Syntax Description

<i>trustpoint-label</i>	Name of trustpoint.
use-any	Use any configured trustpoint.

Defaults

If this command is not specified, the petitioner-signing certificate is not verified.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Issue the **authentication trustpoint** command in tti-registrar configuration mode to validate the signing certificate that the petitioner used.

Examples

The following example shows how to specify the trustpoint mytrust for the petitioner-signing certificate:

```
crypto provisioning registrar
 authentication trustpoint mytrust
```

After the SDP exchange is complete, the petitioner automatically enrolls with the registrar and obtains a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration with the default trustpoint tti:

```
crypto pki trustpoint tti
 enrollment url http://pkil-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
crypto provisioning petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.
trustpoint signing	Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar for signing the SDP data including the certificate.

authorization (tti-registrar)

To enable authentication, authorization, and accounting (AAA) authorization for an introducer or a certificate, use the **authorization** command in tti-registrar configuration mode. To disable authorization, use the **no** form of this command.

authorization {login} | {certificate} | {login certificate}

no authorization {login} | {certificate} | {login certificate}

Syntax Description

login	Use the username of the introducer for AAA authorization.
certificate	Use the certificate of the petitioner for AAA authorization.
login certificate	Use the username of the introducer and the certificate of the petitioner for AAA authorization.

Defaults

If an authorization list is configured, then authorization is enabled by default.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command controls the authorization of the introduction. Authorization can be based on the following:

- The login of the petitioner (username and password) to the registrar
- The current certificate of the petitioner
- Both the login of the introducer and the current certificate of the petitioner

If you issue the **authorization login** command, the introducer logs in with a username and password such as ttiuser and mypassword, which are used against the configured authorization list to contact the AAA server and determine the appropriate authorization.

If you issue the **authorization certificate** command, the certificate of the petitioner is used to build an AAA username, which is used to obtain authorization information.

If you issue the **authorization login certificate** command, authorization for the introducer combines with authorization for the petitioner’s current certificate. This means that two AAA authorization lookups occur. In the first lookup, the introducer username is used to retrieve any AAA attributes associated with the introducer. The second lookup is done using the configured certificate name field. If an AAA attribute appears in both lookups, the second one prevails.

Examples

The following example shows how to specify authorization for both the introducer and the current certificate of the petitioner:

```
crypto provisioning registrar
authorization login certificate
```

Related Commands

Command	Description
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner for a user introducer in an SDP transaction.

authorization username (tti-registrar)

To specify the parameters for the different certificate fields that are used to build the authentication, authorization, and accounting (AAA) username, use the **authorization username** command in tti-registrar configuration mode. To disable the parameters, use the **no** form of this command.

authorization username {*subjectname* *subjectname*}

no authorization username {*subjectname* *subjectname*}

Syntax Description

subjectname	AAA username that is generated from the certificate subject name.
<i>subjectname</i>	Builds the username. The following options can be used as the AAA username: <ul style="list-style-type: none"> • all—Entire distinguished name (subject name) of the certificate • commonname—Certificate common name • country—Certificate country • email—Certificate e-mail • ipaddress—Certificate IP address • locality—Certificate locality • organization—Certificate organization • organizationalunit—Certificate organizational unit • postalcode—Certificate postal code • serialnumber—Certificate serial number • state—Certificate state field • streetaddress—Certificate street address • title—Certificate title • unstructuredname—Certificate unstructured name

Defaults

Parameters for the certificate fields are not specified.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows that the **serialnumber** option is used as the authorization username:

```
aaa authorization network maxaaa group tacac+
aaa new-model
```

```
crypto ca trustpoint msca
enrollment url http://caserver.mycompany.com
authorization list maxaaa
authorization username subjectname serialnumber
```

Related Commands

Command	Description
authorization list	Specifies the AAA authorization list.

trustpoint signing

To specify the trustpoint and associated certificate to be used when signing all introduction data during the Secure Device Provisioning (SDP) exchange, use the **trustpoint signing** command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint signing *trustpoint-label*

no trustpoint signing *trustpoint-label*

Syntax Description

<i>trustpoint-label</i>	Name of trustpoint.
-------------------------	---------------------

Defaults

If a trustpoint is not specified, any existing device certificate is used. If none is available, a self-signed certificate is generated.

Command Modes

tti-petitioner configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **trustpoint signing** command in tti-petitioner configuration mode to associate a specific trustpoint with the petitioner for signing its certificate.

Examples

The following example shows how to specify the trustpoint mytrust:

```
crypto provisioning petitioner
 trustpoint signing mytrust
```

After the SDP exchange is complete, the petitioner automatically enrolls with the registrar and obtains a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration with the default trustpoint tti:

```
crypto pki trustpoint tti
 enrollment url http://pk11-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
crypto provisioning petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.
trustpoint (tti-petitioner)	Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar.

Glossary

authentication, authorization, and accounting (AAA)—An architectural framework for configuring a set of independent security functions in a consistent manner.

certificate—A digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

certificate authority (CA)—A service responsible for managing certificate requests and issuing certificates to participating IPSec network devices. This service provides centralized key management for the participating devices and is explicitly entrusted by the receiver to validate identities and to create digital certificates.

enrollment—The process of obtaining a new certificate from a CA.

petitioner—A new device that is joined to the secure domain. The petitioner can be a certificate server.

public key infrastructure (PKI)—A system of certificates and authorities that provide trusted and efficient key and certificate management to support security protocols such as IPSec.

registrar—A server that authorizes the petitioner.

RADIUS (remote authentication dial-in user service)—A distributed client/server system that secures networks against unauthorized access by providing detailed accounting information and flexible administrative control over authentication and authorization processes.

trustpoint—One or more identities that are considered trustworthy and can be used to validate other identities.

user introducer—An end user using SDP to deploy a VPN device associated with itself.

VPN—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

**Note**

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

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 © 2005 Cisco Systems, Inc. All rights reserved.