



# Administrative Secure Device Provisioning Introducer

---

The Administrative Secure Device Provisioning (SDP) Introducer feature allows you to act as an administrative introducer to introduce a device into a public key infrastructure (PKI) network and then provide a username as the device name for the record locator in the authentication, authorization, and accounting (AAA) database.

## Feature History for Administrative SDP Introducer

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 Administrative SDP Introducer, page 2](#)
- [Restrictions for Administrative SDP Introducer, page 2](#)
- [Information About Administrative SDP Introducer, page 2](#)
- [How to Configure Administrative SDP Introducer, page 4](#)
- [Configuration Examples for Administrative SDP Introducer, page 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)
- [administrator authentication list, page 11](#)



---

**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 Administrative SDP Introducer

- Both the client device and the server must have IP connectivity between each other.
- The administrator must have a web browser that supports JavaScript.
- The administrative introducer must have enable privileges on the client device and administrator privileges on the server.
- SDP must be configured and operational.
- 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 Administrative SDP Introducer

When using RADIUS, a user/device that needs to be introduced by the administrative introducer must always use cisco as its own password. TACACS+ does not have this limitation; a user/device can have any password and be introduced by the administrative introducer.

## Information About Administrative SDP Introducer

To use the Administrative SDP Introducer feature, you need to understand the following concepts:

- [Feature Overview of Administrative SDP Introducer, page 2](#)
- [Benefits of Administrative SDP Introducer, page 3](#)

## Feature Overview of Administrative SDP Introducer

SDP simplifies deployment of Virtual Private Network (VPN) devices by allowing users to introduce their VPN device to the PKI network. The SDP mechanisms assume a permanent relationship between the introducer and the device. As a result, the introducer username is used to define the device name.

In some deployment scenarios, the introducer is an administrator doing the introduction for many devices. However, using the introducer (the administrator) name to define the device name results in multiple devices being incorrectly deployed with the same device name. Instead this feature allows the administrator to specify the correct device name during the introduction.

More generally stated, the introducer username is used as the database record locator to determine all other information about the device including the Cisco IOS configuration template, various template variables (pulled from an AAA database and expanded into the template), and the appropriate subject name for PKI certificates issued to the device. For simplicity, this database record locator is called the user/device name.

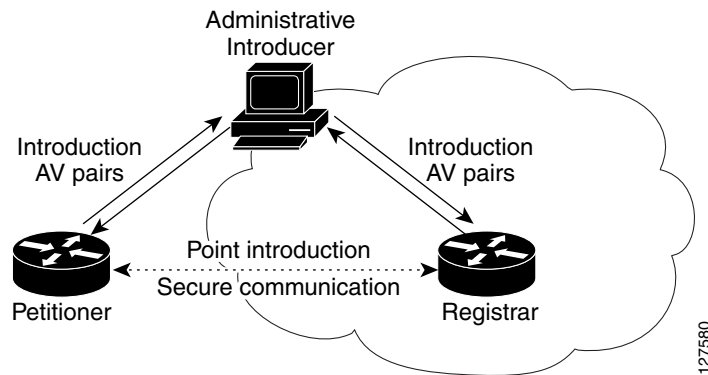
The administrative introducer provides a device name. In that way, an administrator can provide the appropriate record locator when doing an introduction. For example, if an administrator is trying to introduce a device for username rover, then the administrator introduces the device into the PKI network and provides rover as the record locator after logging into the registrar using the administrator's own

credentials. The record locator, rover, becomes the device name. All other template and PKI certificate subject name information specific to the introduction is then provided by the rover username records instead of by the administrator's record.

The registrar device uses the supplied username information with a user introducer name. This allows the existing mechanisms for determining a user's authorization, template, and PKI certificate information to be supported without modification.

Figure 1 shows a sample SDP topology in which an administrative introducer is introducing the petitioner to the registrar which then authorizes the petitioner.

**Figure 1** *Sample SDP Topology*



## Benefits of Administrative SDP Introducer

### Greater Flexibility and Ease of Use

The SDP introduction phase allows an administrator performing the introduction to supply the name for the device being introduced. The supplied device name is used as if it were the name of an introducer in the normal SDP mechanisms, preserving the existing functionality of the SDP configuration.

# How to Configure Administrative SDP Introducer

This section contains the following procedures:

- [Configuring an Administrative Introducer, page 4](#) (required)
- [Verifying the Configuration, page 5](#) (optional)

## Configuring an Administrative Introducer

Perform the following task to configure an administrative introducer using administrator authentication and authorization lists.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto provisioner registrar**
4. **administrator authentication list** *list-name*
5. **administrator authorization list** *list-name*
6. **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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto provisioning registrar</b>  <b>Example:</b> Router(config)# crypto provisioning registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.
Step 4	<b>administrator authentication list</b> <i>list-name</i>  <b>Example:</b> Router(tti-registrar)# administrator authentication list authen-tac	Configures the AAA list used to authenticate an administrator during an introduction.

	Command or Action	Purpose
Step 5	<b>administrator authorization list</b> <i>list-name</i>  <b>Example:</b> Router(tti-registrar)# administrator authorization list author-tac	Configures the AAA list used to obtain authorization information, such as the certificate subject name and/or the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner, for an administrator during an introduction.
Step 6	<b>end</b>  <b>Example:</b> Router(tti-registrar)# end	(Optional) Exits tti-registrar configuration mode.

## Verifying the Configuration

Perform the following task to verify that an administrative introducer using administrator authentication and authorization lists has been created.

### SUMMARY STEPS

1. **enable**
2. **show running-config** [**system** | *mod\_num*] [**all**]
3. **end**

### DETAILED STEPS

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

# Configuration Examples for Administrative SDP Introducer

This section contains the following configuration examples:

- [Configuring an Administrative Introducer Using Authentication and Authorization Lists: Example, page 6](#)
- [Verifying the Configuration: Example, page 6](#)

## Configuring an Administrative Introducer Using Authentication and Authorization Lists: Example

The following example shows an administrative introducer with an authentication list named `authen-tac` and an authorization list named `author-tac` being configured:

```
Router# configure terminal

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

Router(config)# crypto provisioning registrar

Router(tti-registrar)# administrator authentication list authen-tac

Router(tti-registrar)# administrator authorization list author-tac

Router(tti-registrar)# end
```

## Verifying the Configuration: Example

The following example from the `show running-config` command displays information about the administrative introducer that you just created:

```
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 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!
  administrator authentication list authen-tac
  administrator authorization list author-tac
!
no crypto engine onboard 0
username qa privilege 15 password 0 lab
!
!
!

```

# Additional References

The following sections provide references related to the Administrative SDP Introducer feature.

## Related Documents

Related Topic	Document Title
SDP, including the SDP web page	<a href="#">Easy Secure Device Deployment</a> feature module, Release 12.3(7)T <b>Note</b> Secure Device Provisioning (SDP) was formerly called Easy Secure Device Deployment (EzSDD).
Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<a href="#">Cisco IOS Security Command Reference</a> , Release 12.3 T
Security features including trustpoints, certificate enrollment, and authentication	<a href="#">Cisco IOS Security Configuration Guide</a> , 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Command Reference

This section documents new commands.

- [administrator authentication list](#)
- [administrator authorization list](#)

# administrator authentication list

To authenticate an administrative introducer for a Secure Device Provisioning (SDP) transaction, use the **administrator authentication list** command in tti-registrar configuration mode. To disable administrative introducer authentication, use the **no** form of this command.

**administrator authentication list** *list-name*

**no administrator authentication list** *list-name*

<b>Syntax Description</b>	<i>list-name</i>	Name of list.
---------------------------	------------------	---------------

**Defaults** All introducers are authenticated as users; their username is used directly to build the device name.

**Command Modes** tti-registrar configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

**Usage Guidelines** When you use the **administrator authentication list** command in SDP transactions, the RADIUS or TACACS+ authentication, authorization, and accounting (AAA) server checks for a valid account by looking at the username and password.

The authentication list and the authorization list usually both point to the same AAA list. It is possible that the lists can be on different databases, but it is generally not recommended.

**Examples** The following example shows that an administrative authentication list named authen-rad and an administrative authorization list named author-rad have been configured on a RADIUS AAA server; a user authentication list named authen-tac and a user authorization list named author-tac have been configured on a TACACS+ server:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# administrator authentication list authen-rad
Router(tti-registrar)# administrator authorization list author-rad
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-tac
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

Related Commands	Command	Description
	<b>administrator authorization list</b>	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 an administrative introducer in an SDP transaction.
	<b>authentication list (tti-registrar)</b>	Authenticates an introducer in an SDP transaction.
	<b>authorization list (tti-registrar)</b>	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.

# administrator authorization list

To specify the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS command-line interface (CLI) snippet that is sent back to the petitioner for an administrative introducer in a Secure Device Provisioning (SDP) transaction, use the **administrator authorization list** command in tti-registrar configuration mode. To disable the subject name and list of template variables, use the **no** form of this command.

**administrator authorization list** *list-name*

**no administrator authorization list** *list-name*

<b>Syntax Description</b>	<i>list-name</i>	Name of list.
---------------------------	------------------	---------------

<b>Defaults</b>	There is no authorization information requested from the authentication, authorization, and accounting (AAA) server for the administrator.	
-----------------	--	--

<b>Command Modes</b>	tti-registrar configuration
----------------------	-----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

**Usage Guidelines** When you use the **administrator authorization list** command in SDP transactions, the RADIUS or TACACS+ AAA server stores the subject name and template variables. The name and variables are sent back to the petitioner in the Cisco IOS CLI snippets. This list and the authorization list are usually on the same database, but they can be on different AAA databases. (Storing lists on different databases is not recommended.)

When a petitioner makes an introducer request, multiple queries are sent to the AAA list database on the RADIUS or TACACS+ server. The queries search for entries of the following form:

```
user Password <userpassword>
  cisco-avpair="titi:subjectname=<<DN subjectname>>"
  cisco-avpair="titi:iosconfig#<<value>>"
  cisco-avpair="titi:iosconfig#<<value>>"
  cisco-avpair="titi:iosconfig#=<<value>>"
```



**Note** The existence of a valid AAA username record is enough to pass the authentication check. The cisco-avpair=tti information is necessary only for the authorization check.

If a subject name were received in the authorization response, the registrar stores it in the enrollment database, and that subject name overrides the subject name that is supplied in the subsequent certificate request (PKCS10) from the petitioner device.

The numbered tti:iosconfig values are expanded into the Cisco IOS snippet that is sent to the petitioner. The configurations replace any numbered (\$1 through \$9) template variable. Because the default Cisco IOS snippet template does not include the variables \$1 through \$9, these variables are ignored unless you configure an external Cisco IOS snippet template. To specify an external configuration, use the **template config** command.



**Note**

The template configuration location may include a variable \$n, which is expanded to the name that the administrator enters in the additional SDP dialog.

**Examples**

The following example shows that an administrative authentication list named authen-rad and an administrative authorization list named author-rad have been configured on a RADIUS AAA server; a user authentication list named authen-tac and a user authorization list named author-tac have been configured on a TACACS+ server:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# pki-server mycs
Router(tti-registrar)# administrator authentication list authen-rad
Router(tti-registrar)# administrator authorization list author-rad
Router(tti-registrar)# authentication list authen-tac
Router(tti-registrar)# authorization list author-tac
Router(tti-registrar)# template username ftpuser password ftppwd
Router(tti-registrar)# template config ftp://ftp-server/iossnippet.txt
Router(tti-registrar)# end
```

**Related Commands**

Command	Description
<b>administrator authentication list</b>	Authenticates an administrative introducer for an SDP transaction.
<b>authentication list (tti-registrar)</b>	Authenticates a user introducer for an SDP transaction.
<b>authorization list (tti-registrar)</b>	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 operation.

# Glossary

**administrative introducer**—An administrator or management system using SDP to deploy a VPN device associated with some other user or record.

**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.

**device name**—The name of a device used to locate or generate all configuration information about a device. For a user introducer, this is the username. For an administrative introducer, this is supplied; for example, hub1.

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

**petitioner**—A new device, such as a certificate server, that is joined to the secure domain.

**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.

**TACACS+ (terminal access controller access control system plus)**—A security application that provides centralized validation of users attempting to gain access to your access point.

**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.

