



PKI Integration with AAA Server

The PKI Integration with AAA Server feature provides additional scalability for authorization by generating an authentication, authorization, and accounting (AAA) username from the certificate presented by the peer. An AAA server is queried to determine whether the certificate is authorized for use by the internal component. The authorization is indicated by a component-specified label that must be present in the attribute-value (AV) pair for the user.

Feature Specifications for the PKI Integration with AAA Server Feature

Feature History

Release	Modification
12.3(1)	This feature was introduced.

Supported Platforms

Cisco 801–806, Cisco 811, Cisco 813, Cisco 820, Cisco 827–828, Cisco 1600, Cisco 1600R, Cisco 1710, Cisco 1720–1721, Cisco 1750–1751, Cisco 1760, Cisco 2610–2613, Cisco 2610XM–2611XM, Cisco 2620–2621, Cisco 2620XM–2621XM, Cisco 2650–2651, Cisco 2650XM–2651XM, Cisco 2691, Cisco 3620, Cisco 3631, Cisco 3640, Cisco 3660, Cisco 3725, Cisco 3745, Cisco 4500, Cisco 7100, Cisco 7200, Cisco 7400, Cisco 7500, Cisco AS5300, Cisco AS5350, Cisco AS5800, Cisco ubr7200, Cisco ubr905, Cisco ubr920, Cisco ubr925.

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 PKI Integration with AAA Server, page 2](#)
- [Information About PKI Integration with AAA Server, page 2](#)
- [How to Configure PKI Integration with AAA Server, page 4](#)
- [Configuration Examples for PKI Integration with AAA Server, page 8](#)



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

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

- [Where to Go Next, page 8](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)
- [Glossary, page 14](#)
- [Appendix A: Adding a PKI Service to a Cisco Secure ACS 3.2 AAA Server, page 15](#)
- [Appendix B: Additional PKI AAA Integration with AAA Server Examples, page 24](#)

Prerequisites for PKI Integration with AAA Server

- AAA integration is part of the public key infrastructure (PKI) subsystem. The PKI system requires the crypto subsystem. For information about configuring a PKI, refer to the following document:
 - *Certification Authority Interoperability Commands*
- You must understand how to configure AAA authorization lists. For information about configuring an AAA authorization list, refer to the following chapters:
 - The chapters “AAA Overview” and “Configuring Authorization” in the Cisco IOS Security Configuration Guide

Information About PKI Integration with AAA Server

To configure the PKI Integration with AAA Server feature, you must understand the following concepts:

- [PKI Authorization, page 2](#)
- [PKI Integration with AAA Server Overview, page 3](#)
- [New Attribute-Value Pairs, page 3](#)
- [PKI Integration with AAA Server Using RADIUS or TACACS+, page 4](#)

PKI Authorization

PKI authentication does not provide authorization. Current solutions for authorization are specific to the router that is being configured although a centrally managed solution is often required.

There is not a clean mechanism by which certificates are defined as authorized for particular tasks and not for others. This authorization information can be captured in the certificate itself if the application is aware of the certificate-based authorization information. But this solution does not provide a simple mechanism for real-time updates to the authorization information and forces each application to be aware of the specific authorization information embedded in the certificate.

When the access control list (ACL) mechanism is implemented as part of the trustpoint authentication, the application is no longer responsible for determining this authorization information, and it is no longer possible to specify for which application the certificate is authorized. In some cases, the ACL on the router gets so large that it cannot be managed. Additionally, it is beneficial to retrieve ACL indications from an external server.

Current solutions to the real-time authentication problem involve specifying a new protocol and building a new server (with associated tasks, such as management and data distribution).

PKI Integration with AAA Server Overview

The PKI Integration with AAA Server feature provides an alternative online certificate status solution that leverages the existing AAA infrastructure. Certificates can be listed in the AAA database with appropriate levels of authorization. For components that do not explicitly support PKI-AAA, a default label of “all” from the AAA server provides authorization. Likewise, a label of “none” from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent, but “none” is included for completeness and clarity). If the application component does support PKI-AAA, the component may be specified directly; for example, the application component could be “ipsec,” “ssl,” or “osp.” (ipsec=IP Security, ssl=Secure Sockets Layer, and osp=Open Settlement Protocol.)



Note

- Currently, no application component supports specification of the application label.
- There may be a time delay when accessing the AAA server. If the AAA server is not available, the authorization fails.

New Attribute-Value Pairs

The following AV pairs have been added (values shown are possible values). The AV pairs in the peer certificate must exactly match the AV pairs that are in the AAA database. If they do not match, the peer certificate is not authorized.

Table 1 AV Pairs That Must Match

AV Pair	Value
cisco-avpair=pki:cert-application=all	Valid values are “all” and “none.”
cisco-avpair=pki:cert-trustpoint=msca	The value is a Cisco IOS command-line interface (CLI) configuration trustpoint label. Note The cert-trustpoint AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.

Table 1 AV Pairs That Must Match

AV Pair	Value
cisco-avpair=pki:cert-serial=16318DB7000100001671	<p>The value is a certificate serial number.</p> <p>Note The cert-serial AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.</p>
cisco-avpair=pki:cert-lifetime-end=1:00jan 1, 2003	<p>The value must match the following form: hours:minutes month day, year.</p> <p>Note Only the first three characters of a month are used: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. If more than three characters are entered for the month, the remaining characters are ignored (for example Janxxxx).</p> <p>Note The cert-lifetime-end AV pair is available to artificially extend a certificate lifetime beyond the time period that is indicated in the certificate itself. If the cert-lifetime-end AV pair is used, the cert-trustpoint and cert-serial AV pairs must also be specified.</p>

PKI Integration with AAA Server Using RADIUS or TACACS+

The PKI Integration with AAA Server feature works with either the RADIUS or TACACS+ protocol.

If the RADIUS protocol is used, the password that is configured for the username in the AAA server should be set to “cisco.” When the TACACS protocol is used, the password that is configured for the username in the AAA server is irrelevant because TACACS supports authorization without requiring authentication (the password is used for authentication).

When you are configuring the AAA server for the PKI integration, you must set the RADIUS or TACACS attributes that are required for authentication.

In addition, if you are using TACACS, you must add a PKI service to the AAA server. The custom attribute “cert-application=all” is added under the PKI service for the particular user or usergroup to authorize the specific username. (See the section [Appendix A: Adding a PKI Service to a Cisco Secure ACS 3.2 AAA Server](#).)

How to Configure PKI Integration with AAA Server

This section contains the following procedures:

- [Configuring PKI Integration with an AAA Server, page 5](#)
- [Troubleshooting PKI Integration with AAA Server, page 6](#)

Configuring PKI Integration with an AAA Server

Perform this task to specify which fields within a certificate should be used to build the AAA database username.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization {network} {listname}**
4. **aaa new-model**
5. **crypto ca trustpoint name**
6. **enrollment url url**
7. **authorization list {listname}**
8. **authorization username {subjectname subjectname}**

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	aaa authorization {network} {listname} Example: Router (config)# aaa authorization network maxaaa group tacacs+	Sets the parameters that restrict user access to a network.
Step 4	aaa new-model Example: Router (config)# aaa new-model	Enables the AAA access control model
Step 5	crypto ca trustpoint name Example: Route (config)# crypto ca trustpoint msca	Declares the certification authority (CA) that your router should use.

	Command or Action	Purpose
Step 6	<pre>enrollment url url</pre> <p>Example: Router (config)# enrollment url http://caserver.mycompany.com </p>	<p>Specifies the enrollment parameters of your CA.</p> <ul style="list-style-type: none"> The <i>url</i> argument is the URL of the CA to which your router should send certificate requests.
Step 7	<pre>authorization list {listname}</pre> <p>Example: Route (config)# authorization list maxaaa </p>	<p>Specifies the AAA authorization list.</p>
Step 8	<pre>authorization username {subjectname subjectname}</pre> <p>Example: Router (config)# authorization username subjectname serialnumber </p>	<p>Sets parameters for the different certificate fields that are used to build the AAA username.</p> <p>The <i>subjectname</i> argument can be any of the following:</p> <ul style="list-style-type: none"> commonname—Certification 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.

Troubleshooting PKI Integration with AAA Server

Perform this task to verify your PKI integration with an AAA server.

SUMMARY STEPS

- enable
- debug crypto pki transactions

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	debug crypto pki transactions Example: Router# debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the certification authority (CA) and the router.

Examples

The following sample outputs for the **debug crypto pki transactions** command show a successful PKI integration with AAA server exchange and a failed PKI integration with AAA server exchange:

Successful Exchange

```
Router# debug crypto pki transactions
```

```
Apr 22 23:15:03.695: CRYPTO_PKI: Found a issuer match
Apr 22 23:15:03.955: CRYPTO_PKI: cert revocation status unknown.
Apr 22 23:15:03.955: CRYPTO_PKI: Certificate validated without
revocation check
```

Each line that shows “CRYPTO_PKI_AAA” indicates the state of the AAA authorization checks. Each of the AAA AV pairs is indicated, and then the results of the authorization check are shown.

```
Apr 22 23:15:04.019: CRYPTO_PKI_AAA: checking AAA authorization
(ipsecca_script_aalist, PKIAAA-L, <all>)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-application"
= "all")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint"
= "yni-u10")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-serial" =
"15DE")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: authorization passed
Apr 22 23:12:30.327: CRYPTO_PKI: Found a issuer match
```

Failed Exchange

```
Router# debug crypto pki transactions
```

```
Apr 22 23:11:13.703: CRYPTO_PKI_AAA: checking AAA authorization =
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-application"
=
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint"
=
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-serial" =3D
=
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute =
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: parsed cert-lifetime-end as: 21:30
=
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: timezone specific extended =
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end is expired
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end check failed.
```

Apr 22 23:11:14.203: CRYPTO_PKI_AAA: authorization failed

In the above failed exchange, the certificate has expired.

Configuration Examples for PKI Integration with AAA Server

This section includes the following example:

- [Configuring PKI Integration with an AAA Server Example, page 8](#)

Configuring PKI Integration with an AAA Server Example

The following example shows that the AAA authorization list “maxaaa” is specified:

```
Router (config)# 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
```

Where to Go Next

You may want to configure solutions that use PKI as the authentication or authorization mechanism, such as IP security (IPSec) Virtual Private Network (VPN) accounting, Open Settlements Protocol (OSP), and Secure Sockets Layer (SSL).

For more information about configuring IPSec VPN accounting, refer to the following document or to [Cisco.com](#) for more documents about IPSec VPN accounting:

- *IPSec VPN Accounting*

For more information about Open Settlement Protocol (OSP) and Secure Sockets Layer (SSL), refer to the following documents, respectively, and to [Cisco.com](#):

- *Open Settlements Protocol (OSP) Clearinghouse Solution*
- *SSL: Introduction to Secure Sockets Layer*

Additional References

For additional information related to the PKI Integration with AAA Server feature, refer to the following references:

Related Documents

Related Topic	Document Title
AAA authorization lists	The chapter “Configuring Authorization” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3
Cisco IOS security configurations	<i>Cisco IOS Security Configuration Guide</i> , Release 12.3

Related Topic	Document Title
Cisco IOS security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3
Diagnosing and troubleshooting AAA	<i>Diagnosing and Troubleshooting AAA Operations</i>
IPSec VPN accounting	<i>IPSec VPN Accounting</i>
PKI	<i>Deploying Cisco IOS Security with a Public-Key Infrastructure</i>
OSP	<i>Open Settlements Protocol (OSP) Clearinghouse Solution</i>
SSL	<i>SSL: Introduction to Secure Sockets Layer</i>

Standards

Standards	Title
None	—

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
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 Release 12.3 command reference publications.

- **authorization list**
- **authorization username**

authorization list

To specify the authentication, authorization, and accounting (AAA) authorization list, use the **authorization list** command in global configuration mode. To disable the authorization list, use the **no** form of this command.

```
authorization list {listname}
```

```
no authorization list {listname}
```

Syntax Description

<i>listname</i>	Name of the aaa authorization list.
-----------------	-------------------------------------

Defaults

If the **authorization list** command is not configured, an authorization list is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Use the **authorization list** command to specify an AAA authorization list. For components that do not support specifying the application label, a default label of “any” from the AAA server will provide authorization. Likewise, a label of “none” from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent to a label of “none,” but “none” is included for completeness and clarity.)

Examples

The following example shows that the AAA authorization list “maxaaa” is specified:

```
Router (config)# 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 username	Specifies the parameters for the different certificate fields that are used to build the AAA username.

authorization username

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 global 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 are options that may be used as the AAA username: <ul style="list-style-type: none"> • 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 (equivalent to the Fully Qualified Domain Name (FQDN) of the device). This option is the default.

Defaults

If this command is not specified, the default username is **unstructuredname**.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example shows that the serialnumber field is to be used as the authorization username:

```
Router (config)# 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.

Glossary

attribute—Characteristics that an entity possesses. Within this document attributes are usually fields within the certificate, and the values for those attributes are obtained from the certificate after the entity has been authenticated.

authenticate—To prove the identity of an entity using the certificate of that identity and a secret the identity possesses (usually the private key corresponding to the public key in the certificate).

authorize—To determine whether an authenticated entity is allowed to perform a requested action.

certificate—Data structure defined in ISO standard X.509 to associate an entity (machine or human) with the public key of that entity. The certificate contains specific fields, including the name of the entity. The certificate is issued by a Certificate Authority (CA) on behalf of the entity. Common fields within a certificate include the distinguished name (DN) of the entity, the distinguished name of the authority issuing the certificate, and the public key of the entity.

DN—distinguished name. Name based on the ISO X.500 standard. The DN includes subfields that identify (or distinguish) the entity possessing the DN. Common subfields include the country in which the entity resides, the company and organization where the entity works, and the common name of the entity.



Note

Refer to the [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 © 2003–2004 Cisco Systems, Inc. All rights reserved.

Appendix A: Adding a PKI Service to a Cisco Secure ACS 3.2 AAA Server

If you are using TACACS, you must add a PKI service to the Cisco Secure ACS 3.2 AAA server. The following sections explain the process.

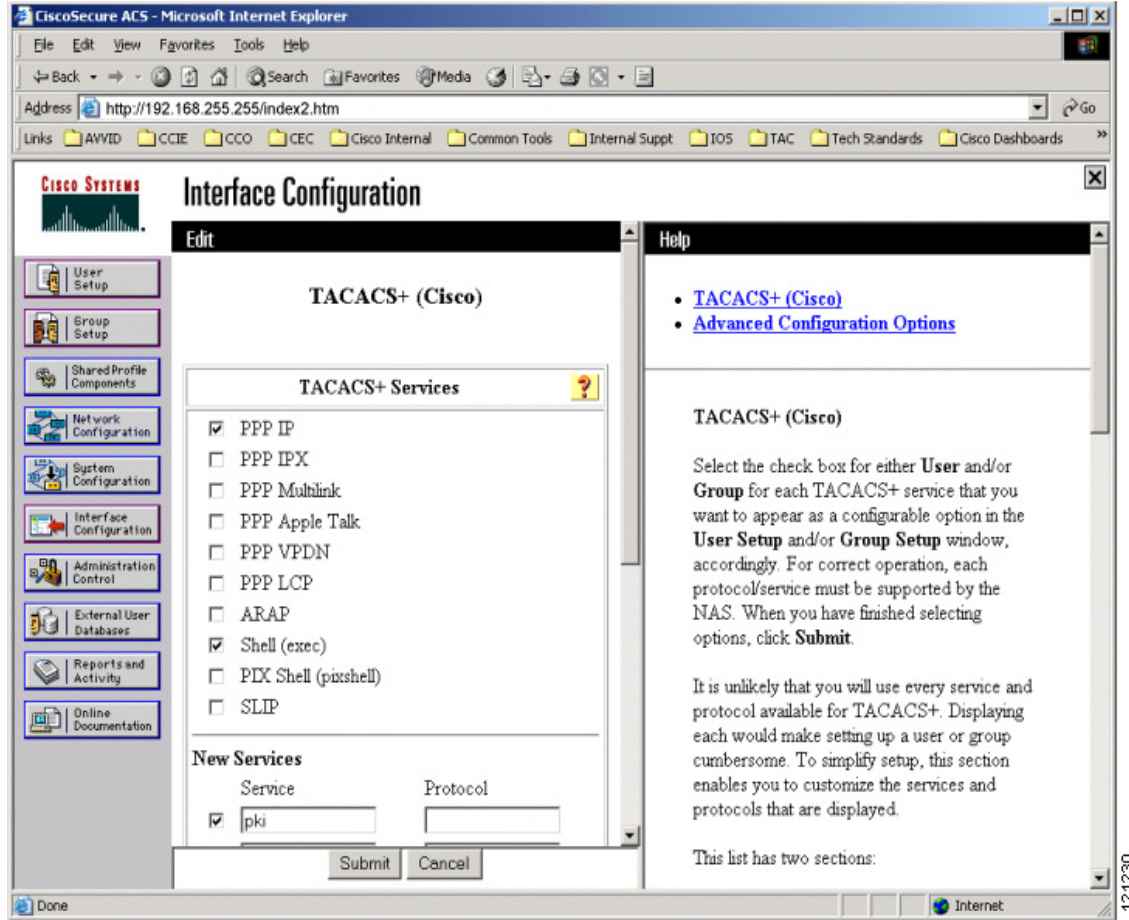
- [Adding the PKI Service As a New TACACS Service, page 15](#) (Required)
- [Creating a Device Group for Authorized VPN Routers, page 16](#) (Required)
- [Creating a Username to Match the FQDN of the Router, page 20](#) (Required)
- [Disabling Authorization for an IPSec Peer, page 23](#) (Optional)

Adding the PKI Service As a New TACACS Service

To configure Cisco Secure ACS to authorize a router to establish an IPSec VPN with another router, perform the following steps.

-
- Step 1** Click on the Interface Configuration button in the left-hand column of the Cisco Secure ACS screen to obtain the screen.
 - Step 2** Click on TACACS+ (Cisco IOS) to obtain the screen shown in [Figure 1](#).
 - Step 3** Click the New Services (Service) check box and enter “pki” as shown in [Figure 1](#). Click the Submit button.

Figure 1 Interface Configuration



Creating a Device Group for Authorized VPN Routers

To create a device group for authorized VPN routers, perform the following steps.

- Step 1** Click the Group Setup button on the left pane to get the screen that is shown in [Figure 2](#).
- Step 2** Choose a group from the list. If you want to rename the group, click the rename button. (This button is hidden under the pull-down screen in [Figure 2](#).)
- Step 3** Select the group to obtain the screen shown in [Figure 3](#)
- Step 4** In the Jump To: pull-down menu, choose TACACS+ to display the screen shown in [Figure 4](#).
- Step 5** Scroll down and select the check boxes for “pki” and “Custom Attributes” that are shown in [Figure 5](#). Add the value “cert-application=all” for the Custom Attribute. Click Submit + Restart. Ensure that you wait for the hourglass to disappear before continuing.

Figure 2 Group Setup – Choose Group

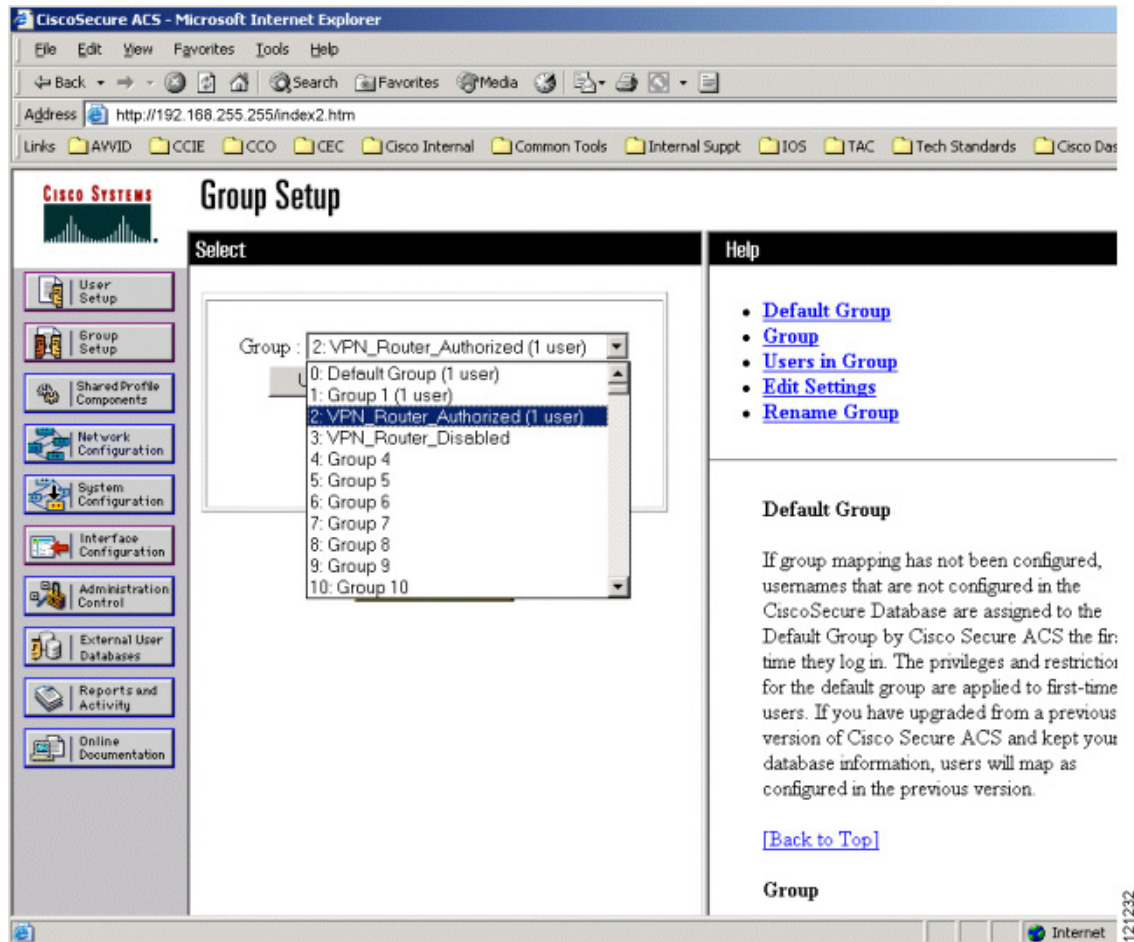


Figure 3 Group Setup – Choose Jump To TACACS+

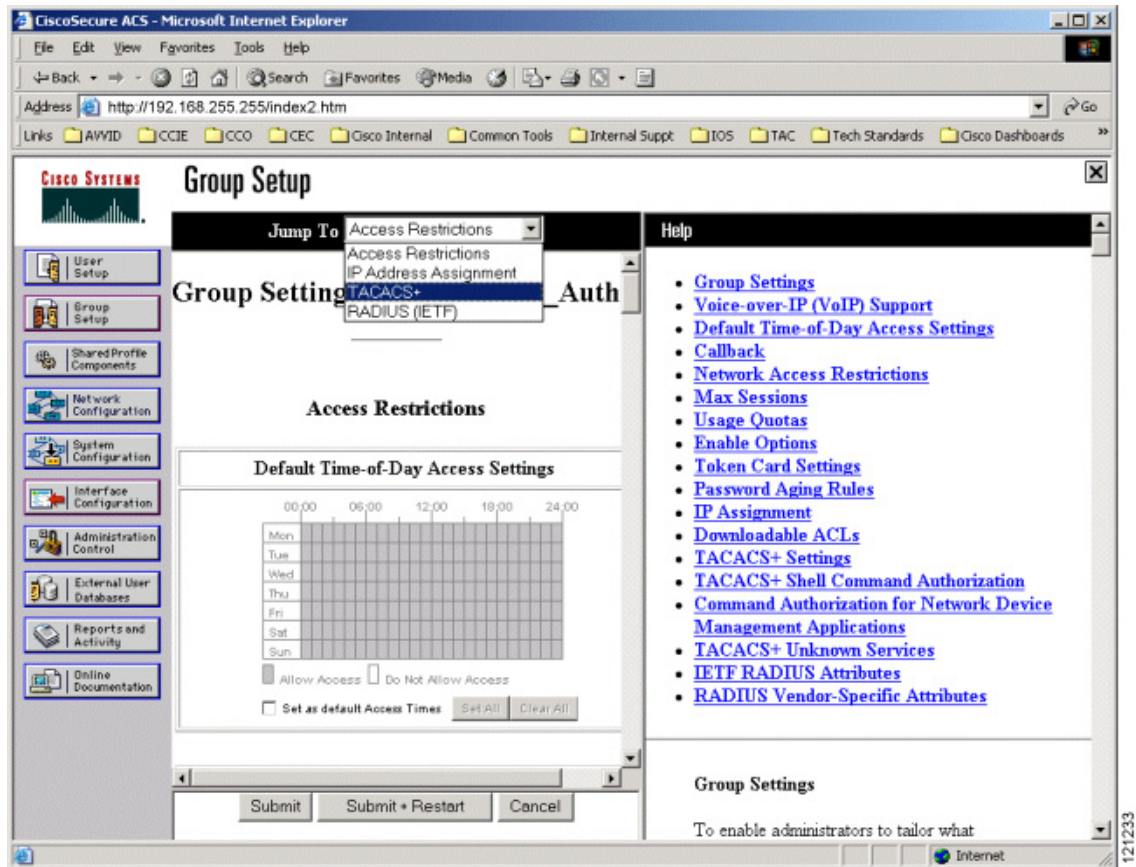


Figure 4 Group Setup – TACACS+ Settings

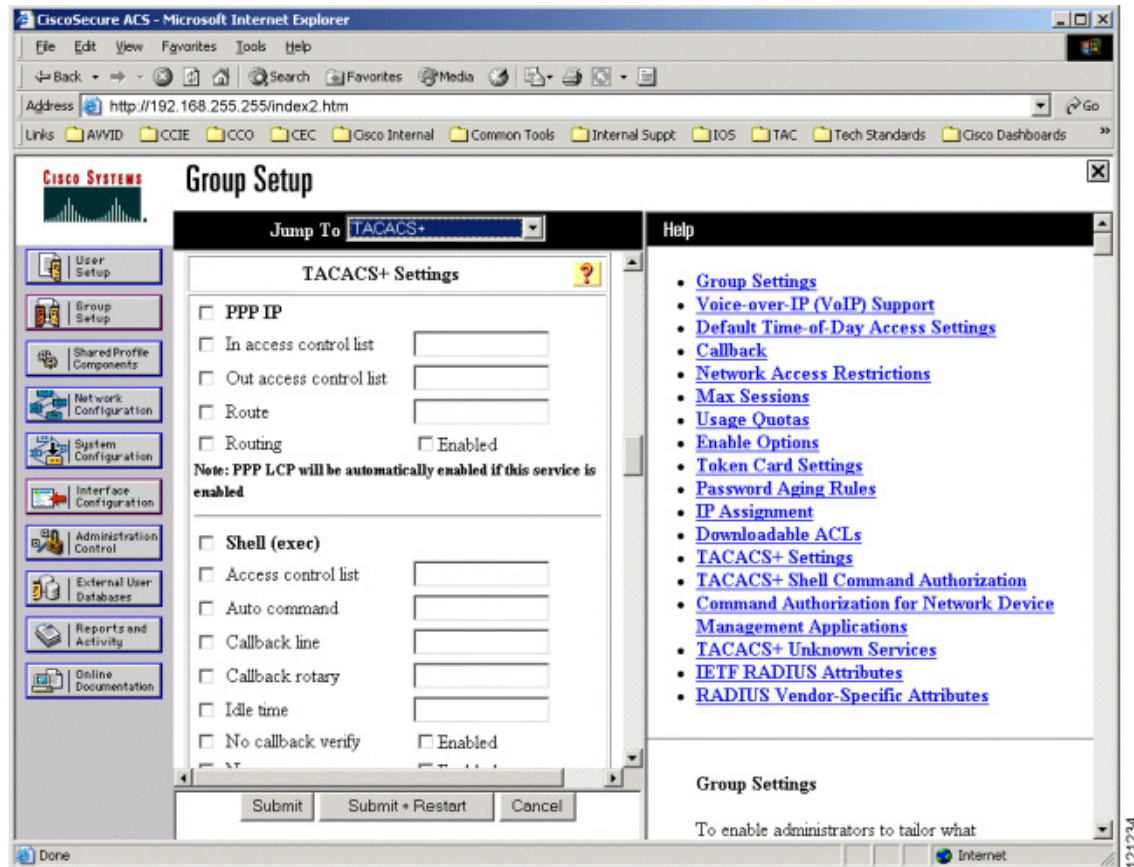
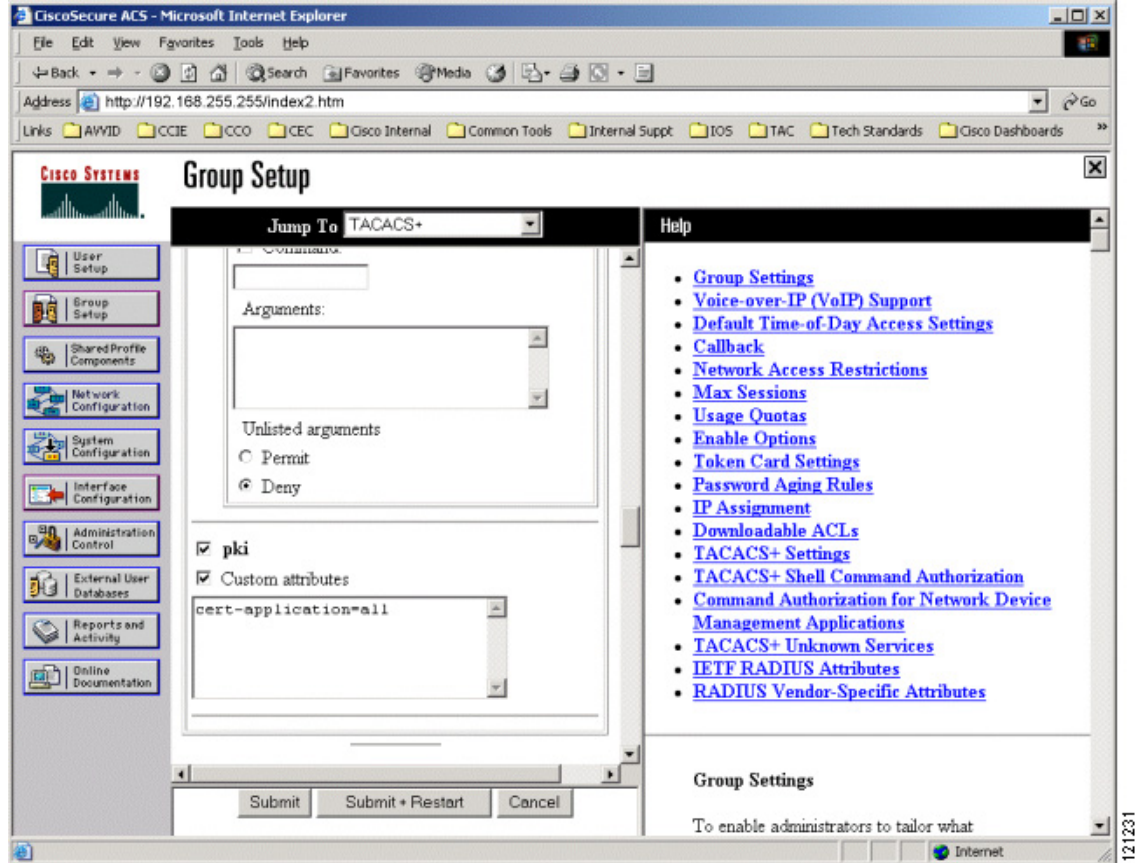


Figure 5 Group Setup – TACACS+ Window



Creating a Username to Match the FQDN of the Router

To create a username to match the fully qualified domain name (FQDN) of the router, perform the following steps.

- Step 1** Click the User Setup button in the left pane to see the screen in [Figure 6](#).
- Step 2** Enter the username that corresponds to the FQDN of the router. Then click the Add/Edit button to obtain the screen that is shown in [Figure 7](#). (In the example, POD-5.gril.com was entered as the username.)
- Step 3** Under User Setup, enter a password in the Password box and confirm that password in the Confirm Password box.

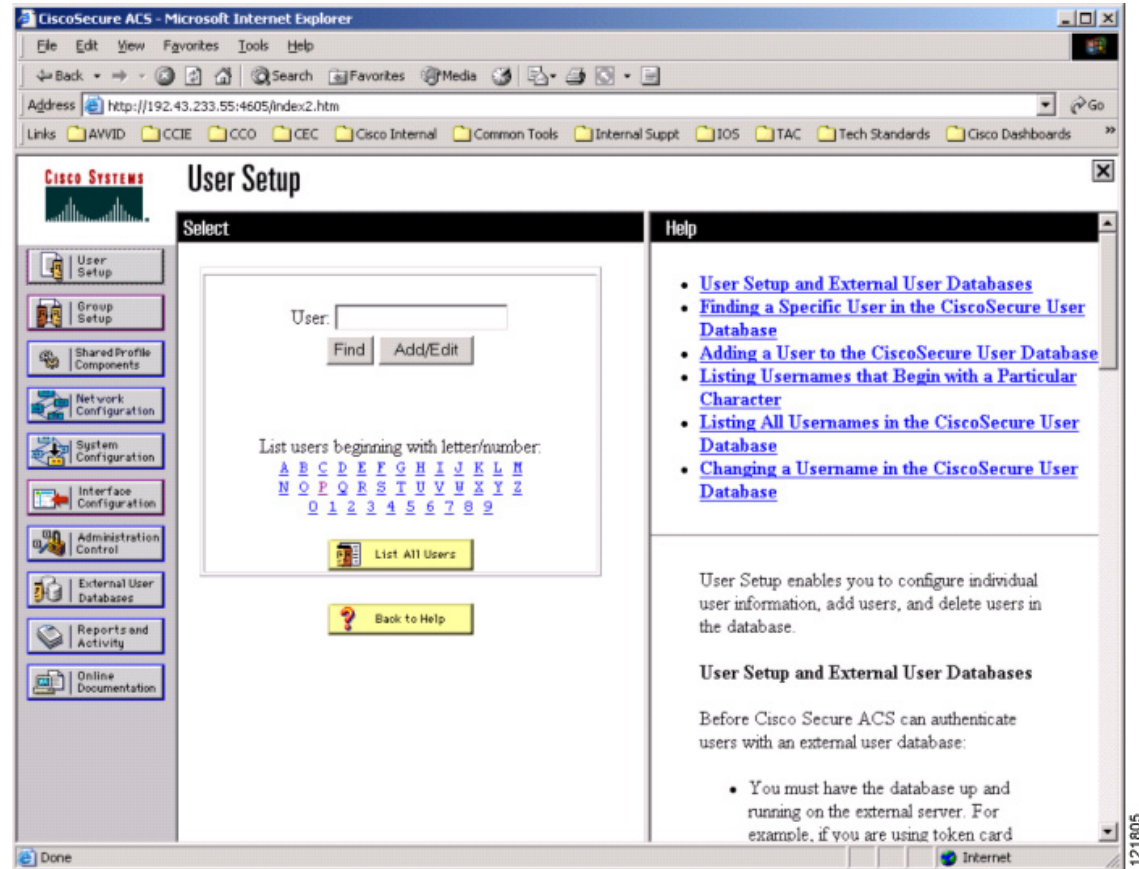


Note When using TACACS, the above password is not used during PKI authentication, but it is necessary to create the username for Cisco Secure ACS.

- Step 4** Scroll down to see the pull-down menu for the Group to which the user is assigned: box, as shown in [Figure 8](#). Choose the group that you edited in Step 2 of the section “[Creating a Device Group for Authorized VPN Routers.](#)” Click the Submit button.

The router named POD-5.gril.com will now be authorized to establish an IPsec VPN connection to 7200-1.gril.com.

Figure 6 User Setup



121805

Figure 7 User Setup – Username and Password

CiscoSecure ACS - Microsoft Internet Explorer

Address <http://192.43.233.55:4605/index2.htm>

CISCO SYSTEMS **User Setup**

User: **POD-5.gril.com**

Account Disabled

Supplementary User Info ?

Real Name

Description

User Setup ?

Password Authentication:

 CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

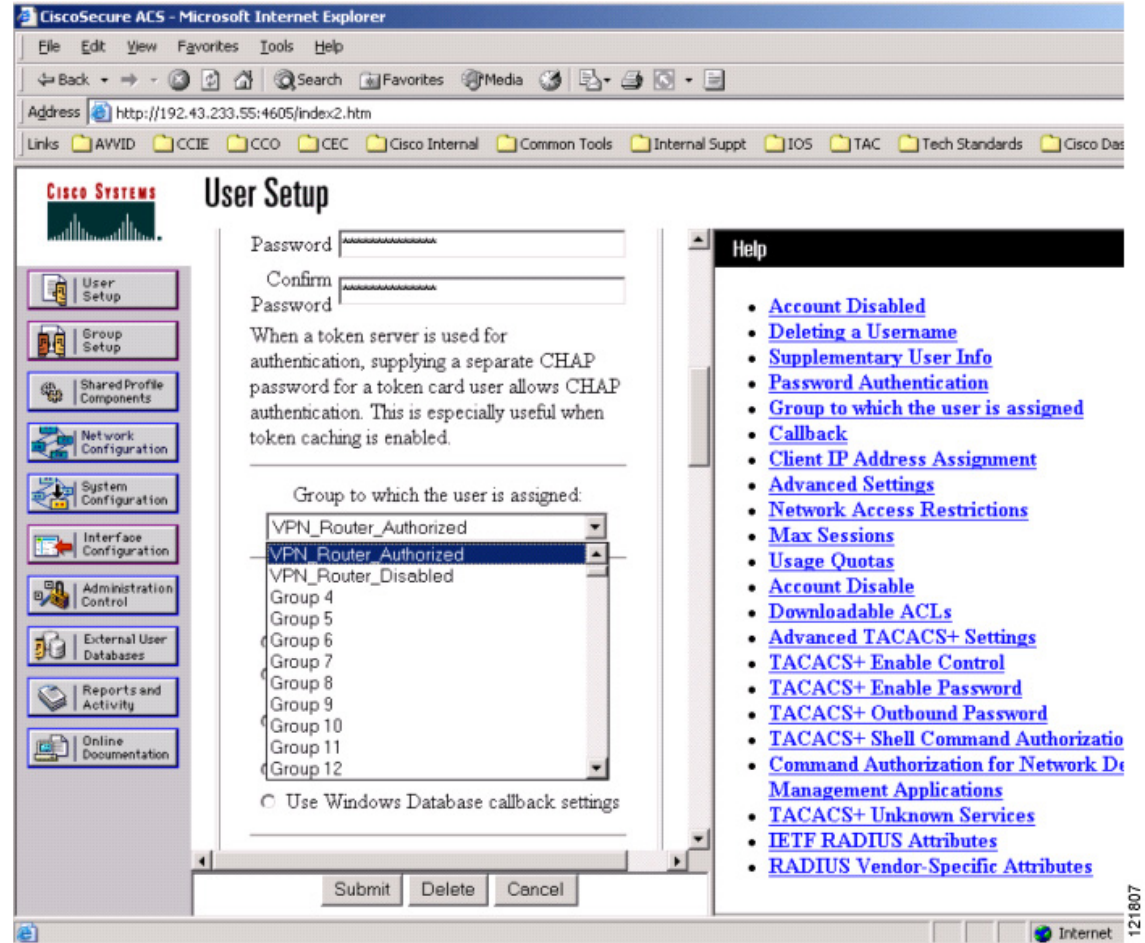
Submit Delete Cancel

Help

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Done Internet 121806

Figure 8 User Setup – Group



Disabling Authorization for an IPSec Peer



Note This task is optional. It is not required for enabling authorization.

To deny an IPSec peer from being authorized, move the username to a group that does not contain the TACACS value “cert-application=all.” To move the username to another group, use the Cisco Secure ACS User Setup screen.



Note Disabling the account using the Account Disabled check box in the User Setup screen does not affect authorization. The Account Disabled check box is used only to disable authentication and has no effect on authorization. Because authentication is not invoked during TACACS authorization, the Account Disabled check box will not affect PKI integration with an AAA server.

Appendix B: Additional PKI AAA Integration with AAA Server Examples

This appendix provides configuration examples of PKI AAA authorizations:

- [Router Configuration: Example, page 24](#)
- [Debug of a Successful PKI AAA Authorization: Example, page 26](#)
- [Debugs of a Failed PKI AAA Authorization: Example, page 27](#)

Router Configuration: Example

The following **show running configuration** command output shows the working configuration of a router that is set up to authorize VPN connections using the PKI Integration with AAA Server feature.

Router# **show running configuration**

```
Building configuration...
!
version 12.3
!
hostname 7200-1
!
aaa new-model
!
!
aaa authentication login default group tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default group tacacs+
aaa authorization exec ACSHouLab group tacacs+
aaa authorization network ACSHouLab group tacacs+
aaa accounting exec ACSHouLab start-stop group tacacs+
aaa accounting network default start-stop group ACSHouLab
aaa session-id common
!
ip domain name gril.com
!
crypto ca trustpoint EM-CERT-SERV
  enrollment url http://10.3.3.3:80
  serial-number
  crl optional
  rsakeypair STOREVPN 1024
  auto-enroll
  authorization list ACSHouLab
!
crypto ca certificate chain EM-CERT-SERV
  certificate 04
    30820214 3082017D A0030201 02020104 300D0609 2A864886 F70D0101 04050030
    17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30343031
    31393232 30323535 5A170D30 35303131 38323230 3235355A 3030312E 300E0603
    55040513 07314437 45424434 301C0609 2A864886 F70D0109 02160F37 3230302D
    312E6772 696C2E63 6F6D3081 9F300D06 092A8648 86F70D01 01010500 03818D00
    30818902 818100BD F3B837AA D925F391 2B64DA14 9C2EA031 5A7203C4 92F8D6A8
    7D2357A6 BCC8596F A38A9B10 47435626 D59A8F2A 123195BB BE5A1E74 B1AA5AE0
    5CA162FF 8C3ACA4F B3EE9F27 8B031642 B618AE1B 40F2E3B4 F996BEFE 382C7283
    3792A369 236F8561 8748AA3F BC41F012 B859BD9C DB4F75EE 3CEE2829 704BD68F
    FD904043 0F555702 03010001 A3573055 30250603 551D1F04 1E301C30 1AA018A0
    16861468 7474703A 2F2F3633 2E323437 2E313037 2E393330 0B060355 1D0F0404
    030205A0 301F0603 551D2304 18301680 1420FC4B CF0B1C56 F5BD4C06 0AFD4E67
```

```

341AE612 D1300D06 092A8648 86F70D01 01040500 03818100 79E97018 FB955108
12F42A56 2A6384BC AC8E22FE F1D6187F DA5D6737 C0E241AC AAAEC75D 3C743F59
08DEEFF2 0E813A73 D79E0FA9 D62DC20D 8E2798CD 2C1DC3EC 3B2505A1 3897330C
15A60D5A 8A13F06D 51043D37 E56E45DF A65F43D7 4E836093 9689784D C45FD61D
EC1F160C 1ABC8D03 49FB11B1 DA0BED6C 463E1090 F34C59E4
quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30333132
31363231 34373432 5A170D30 36313231 35323134 3734325A 30173115 30130603
55040313 0C454D2D 43455254 2D534552 5630819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C14D 833641CF D784F516 DA6B50C0 7B3CB3C9
589223AB 99A7DC14 04F74EF2 AAEEE8F5 E3BFAE97 F2F980F7 D889E6A1 2C726C69
54A29870 7E7363FF 3CD1F991 F5A37CFF 3FFDD3D0 9E486C44 A2E34595 C2D078BB
E9DE981E B733B868 AA8916C0 A8048607 D34B83C0 64BDC101 161FC103 13C06500
22D6EE75 7D6CF133 7F1B515F 32830203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
16041420 FC4BCF0B 1C56F5BD 4C060AFD 4E67341A E612D130 1F060355 1D230418
30168014 20FC4BCF 0B1C56F5 BD4C060A FD4E6734 1AE612D1 300D0609 2A864886
F70D0101 04050003 81810085 D2E386F5 4107116B AD3AC990 CBE84063 5FB2A6B5
BD572026 528E92ED 02F3A0AE 1803F2AE AA4C0ED2 0F59F18D 7B50264F 30442C41
0AF19C4E 70BD3CB5 0ADD8DE8 8EF636BD 24410DF4 DB62DAFC 67DA6E58 3879AA3E
12AFB1C3 2E27CB27 EC74E1FC AEE2F5CF AA80B439 615AA8D5 6D6DEDC3 7F9C2C79
3963E363 F2989FB9 795BA8
quit
!
!
crypto isakmp policy 10
  encr 3des
  group 2
!
!
crypto ipsec transform-set ISC_TS_1 esp-3des esp-sha-hmac
!
crypto ipsec profile ISC_IPSEC_PROFILE_2
  set security-association lifetime kilobytes 530000000
  set security-association lifetime seconds 14400
  set transform-set ISC_TS_1
!
!
controller ISA 1/1
!
!
interface Tunnel0
  description MGRE Interface provisioned by ISC
  bandwidth 10000
  ip address 10.17.17.2 255.255.255.0
  no ip redirects
  ip mtu 1408
  ip nhrp map multicast dynamic
  ip nhrp network-id 101
  ip nhrp holdtime 500
  ip nhrp server-only
  no ip split-horizon eigrp 101
  tunnel source FastEthernet2/1
  tunnel mode gre multipoint
  tunnel key 101
  tunnel protection ipsec profile ISC_IPSEC_PROFILE_2
!
interface FastEthernet2/0
  ip address 10.1.1.1 255.255.255.0
  duplex auto
  speed auto
!

```

```

interface FastEthernet2/1
 ip address 10.2.2.2 255.255.255.0
 duplex auto
 speed auto
 !
 !
 tacacs-server host 192.43.233.55 single-connection
 tacacs-server directed-request
 tacacs-server key gril lab
 !
 ntp master 1
 !
 end

```

Debug of a Successful PKI AAA Authorization: Example

The following **show debugging** command output shows a successful authorization using the PKI Integration with AAA Server feature.

```
Router# show debugging
```

```
General OS:
```

```

TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on

```

```
Cryptographic Subsystem:
```

```
Crypto PKI Trans debugging is on
```

```
Router#
```

```

May 28 19:36:11.117: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:36:12.789: CRYPTO_PKI: Found a issuer match
May 28 19:36:12.805: CRYPTO_PKI: cert revocation status unknown.
May 28 19:36:12.805: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:36:12.813: CRYPTO_PKI_AAA: checking AAA authorization (ACSHouLab,
POD-5.gril.com, <all>)
May 28 19:36:12.813: AAA/BIND(00000042): Bind i/f
May 28 19:36:12.813: AAA/AUTHOR (0x42): Pick method list 'ACSHouLab'
May 28 19:36:12.813: TPLUS: Queuing AAA Authorization request 66 for processing
May 28 19:36:12.813: TPLUS: processing authorization request id 66
May 28 19:36:12.813: TPLUS: Protocol set to None .....Skipping
May 28 19:36:12.813: TPLUS: Sending AV service=pmi
May 28 19:36:12.813: TPLUS: Authorization request created for 66(POD-5.gril.com)
May 28 19:36:12.813: TPLUS: Using server 198.43.233.55
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT/203A4628: Started 5 sec timeout
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:36:12.813: TPLUS: Would block while reading pak header
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27 bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS(00000042)/0/203A4628: Processing the reply packet
May 28 19:36:12.817: TPLUS: Processed AV cert-application=all
May 28 19:36:12.817: TPLUS: received authorization response for 66: PASS
May 28 19:36:12.817: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
May 28 19:36:12.817: CRYPTO_PKI_AAA: authorization passed
Router#
Router#
May 28 19:36:18.681: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 101: Neighbor 17.17.17.1 (Tunnel0) is
up: new adjacency
Router#

```

```
Router# show crypto isakmp sa
```

```
dst          src          state          conn-id slot
00.2.2.2    10.247.102.20  QM_IDLE       84      0
```

Debugs of a Failed PKI AAA Authorization: Example

The following **show debugging** command output shows that the router is not authorized to connect using VPN. The messages are typical of those that you might see in such a situation.

In this example, the peer username was configured as not authorized. This was done by moving the username to a Cisco Secure ACS group called VPN_Router_Disabled in Cisco Secure ACS. The router 7200-1.gril.com has been configured to check with a Cisco Secure ACS AAA server prior to establishing a VPN connection to any peer. (For information on how to create a group such as VPN_Router_Disabled, see the section [“Disabling Authorization for an IPsec Peer.”](#))

```
Router# show debugging
```

```
General OS:
```

```
TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on
```

```
Cryptographic Subsystem:
```

```
Crypto PKI Trans debugging is on
```

```
Router#
```

```
May 28 19:48:29.837: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:31.509: CRYPTO_PKI: Found a issuer match
May 28 19:48:31.525: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:31.525: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:31.533: CRYPTO_PKI_AAA: checking AAA authorization (ACSHouLab,
POD-5.gril.com, <all>)
May 28 19:48:31.533: AAA/BIND(00000044): Bind i/f
May 28 19:48:31.533: AAA/AUTHOR (0x44): Pick method list 'ACSHouLab'
May 28 19:48:31.533: TPLUS: Queuing AAA Authorization request 68 for processing
May 28 19:48:31.533: TPLUS: processing authorization request id 68
May 28 19:48:31.533: TPLUS: Protocol set to None .....Skipping
May 28 19:48:31.533: TPLUS: Sending AV service=pki
May 28 19:48:31.533: TPLUS: Authorization request created for 68(POD-5.gril.com)
May 28 19:48:31.533: TPLUS: Using server 198.43.233.55
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT/203A4C50: Started 5 sec timeout
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:48:31.533: TPLUS: Would block while reading pak header
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 18 bytes response
May 28 19:48:31.537: TPLUS(00000044)/0/203A4C50: Processing the reply packet
May 28 19:48:31.537: TPLUS: received authorization response for 68: FAIL
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:31.537: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:31.537: CRYPTO_PKI: AAA authorization for list 'ACSHouLab', and user
'POD-5.gril.com' failed.
May 28 19:48:31.537: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 63.247.102.20
is bad: certificate invalid
May 28 19:48:39.821: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:41.481: CRYPTO_PKI: Found a issuer match
May 28 19:48:41.501: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:41.501: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:41.505: CRYPTO_PKI_AAA: checking AAA authorization (ACSHouLab,
POD-5.gril.com, <all>)
```

```

May 28 19:48:41.505: AAA/BIND(00000045): Bind i/f
May 28 19:48:41.505: AAA/AUTHOR (0x45): Pick method list 'ACSHouLab'
May 28 19:48:41.505: TPLUS: Queuing AAA Authorization request 69 for processing
May 28 19:48:41.505: TPLUS: processing authorization request id 69
May 28 19:48:41.505: TPLUS: Protocol set to None .....Skipping
May 28 19:48:41.505: TPLUS: Sending AV service=pki
May 28 19:48:41.505: TPLUS: Authorization request created for 69(POD-5.gril.com)
May 28 19:48:41.505: TPLUS: Using server 192.43.233.55
May 28 19:48:41.509: TPLUS(00000045)/0/IDLE/63B22834: got immediate connect on new 0
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE/63B22834: Started 5 sec timeout
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE: wrote entire 46 bytes request
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 18 bytes response
May 28 19:48:41.509: TPLUS(00000045)/0/63B22834: Processing the reply packet
May 28 19:48:41.509: TPLUS: received authorization response for 69: FAIL
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:41.509: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:41.509: CRYPTO_PKI: AAA authorization for list 'ACSHouLab', and user
'POD-5.gril.com' failed.
May 28 19:48:41.509: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 63.247.102.20
is bad: certificate invalid
Router#

Router# show crypto iskmp sa

dst          src          state          conn-id slot
10.2.2.2     10.247.102.20 MM_KEY_EXCH    95      0

```