



Local AAA Server

First Published: March 28, 2005

Last Updated: February 28, 2006

The Local AAA Server feature allows you to configure your router so that user authentication and authorization attributes currently available on AAA servers are available locally on the router. The attributes can be added to existing framework, such as the local user database or subscriber profile. The local AAA server provides access to the complete dictionary of Cisco IOS supported attributes.

History for the Local AAA Server Feature

Release	Modification
12.3(14)T	This feature was introduced.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

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 Local AAA Server, page 2](#)
- [Information About Local AAA Server, page 2](#)
- [How to Configure Local AAA Server, page 3](#)
- [Configuration Examples for Local AAA Server, page 9](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)



Corporate Headquarters:

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

© 2005–2006 Cisco Systems, Inc. All rights reserved.

Prerequisites for Local AAA Server

- Before using this feature, you must have the **aaa new-model** command enabled.

Information About Local AAA Server

To configure the Local AAA Server feature, you should understand the following concepts:

- [Local Authorization Attributes: Overview, page 2](#)
- [Local AAA Attribute Support, page 2](#)
- [AAA Attribute Lists, page 3](#)
- [Validation of Attributes, page 3](#)

Local Authorization Attributes: Overview

The AAA subsystem (authentication, authorization, and accounting) is responsible for managing all supported attributes that are available to the various services within the Cisco IOS software. As such, it maintains its own local dictionary of all supported attributes. However, prior to Cisco IOS Release 12.3(14)T, most of these authorization options were not available for local (on-box) authorizations.

Local AAA Attribute Support

Effective with Cisco IOS Release 12.3(14)T, you can configure your router so that AAA authentication and authorization attributes currently available on AAA servers are made available on existing Cisco IOS devices. The attributes can be added to existing framework, such as the local user database or subscriber profile. For example, an attribute list can now be added to an existing username, providing the ability for the local user database to act as a local AAA server. For situations in which the local username list is relatively small, this flexibility allows you to provide complete user authentication or authorization locally within the Cisco IOS software without having a AAA server. This ability can allow you to maintain your user database locally or provide a failover local mechanism without having to sacrifice policy options when defining local users.

A subscriber profile allows domain-based clients to have policy applied at the end-user service level. This flexibility allows common policy to be set for all users under a domain in one place and applied there whether or not user authorization is done locally. Effective with Cisco IOS Release 12.3(14)T, an attribute list can be added to the subscriber profile, allowing the profile to apply all attributes that can be applied to services using AAA servers. Attributes that are configured under the AAA attribute list are merged with the existing attributes that are generated with the existing subscriber profile and passed to the Subscriber Server Switch (SSS) framework for application.

**Note**

Accounting is still done on a AAA server and is not supported by this feature.

AAA Attribute Lists

AAA attribute lists define user profiles that are local to the router. Every attribute that is known to the AAA subsystem is made available for configuration.

The AAA attributes that are defined in the AAA attribute list are standard RADIUS or TACACS+ attributes. However, they are in the Cisco IOS internal format for that attribute. The attributes must be converted from the RADIUS format (for a RADIUS case) to the Cisco IOS AAA interface format. TACACS+ attributes are generally identical to the Cisco IOS AAA interface format.

Converting from RADIUS Format to Cisco IOS AAA Format

You can use the **show aaa attributes protocol radius** command to get the Cisco IOS AAA format of the Internet Engineering Task Force (IETF) RADIUS attribute. The **show** command output provides a complete list of all the AAA attributes that are supported.

**Note**

The conversion from RADIUS to internal AAA is done internally within the AAA framework. RADIUS vendor-specific attributes (VSAs) are usually accurately reflected during conversion. TACACS+ attributes are also usually identical to the local attributes and do not require the conversion process. However, IETF numbered attributes and some special VSAs often require the conversion process.

Validation of Attributes

Attributes are not validated at configuration. The AAA subsystem “knows” only the format that is expected by the services when the service defines a given attribute inside a definition file. However, it cannot validate the attribute information itself. This validation is done by a service when it first uses the attribute. This validation applies whether the AAA server is RADIUS or TACACS+. Thus, if you are not familiar with configuring a AAA server, it is advisable that you test your attribute list on a test device with the service that will be using the list before configuring and using it in a production environment.

How to Configure Local AAA Server

This section contains the following procedures:

- [Defining a AAA Attribute List, page 3](#) (required)
- [Defining a Subscriber Profile, page 6](#) (required)
- [Monitoring and Troubleshooting a Local AAA Server, page 7](#) (optional)

Defining a AAA Attribute List

To define an AAA attribute list, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **aaa attribute list** *list-name*
4. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
5. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
6. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
7. **attribute type** {*name*} {*value*}
8. **attribute type** {*name*} {*value*}
9. **attribute type** {*name*} {*value*}

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>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>aaa attribute list list-name</p> <p>Example: Router (config)# aaa attribute list TEST</p>	<p>Defines a AAA attribute list.</p>
Step 4	<p>attribute type {name} {value} [service service] [protocol protocol]</p> <p>Example: Router (config)# attribute type addr-pool "pool name" service ppp protocol ip</p>	<p>Defines an IP address pool to use.</p>
Step 5	<p>attribute type {name} {value} [service service] [protocol protocol]</p> <p>Example: Router (config)# attribute type ip-unnumbered "loopback number" service ppp protocol ip</p>	<p>Defines the loopback interface to use.</p>
Step 6	<p>attribute type {name} {value} [service service] [protocol protocol]</p> <p>Example: Router (config)# attribute type vrf-id "vrf name" service ppp protocol ip</p>	<p>Defines the virtual route forwarding (VRF) to use.</p>
Step 7	<p>attribute type {name} {value}</p> <p>Example: Router (config)# attribute type ppp-authen-list "aaa list name"</p>	<p>Defines the AAA authentication list to use.</p>
Step 8	<p>attribute type {name} {value}</p> <p>Example: Router (config)# attribute type ppp-author-list "aaa list name"</p>	<p>Defines the AAA authorization list to use.</p>
Step 9	<p>attribute type {name} {value}</p> <p>Example: Router (config)# attribute type ppp-acct-list "aaa list name"</p>	<p>Defines the AAA accounting list to use.</p>

Defining a Subscriber Profile

To define a subscriber profile, perform the following steps.



Note

RADIUS users should use the **show aaa attributes** command to map the RADIUS version of the particular attribute to the Cisco IOS AAA version of the string attribute. See the example [“Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version: Example, page 10.”](#)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber authorization enable**
4. **subscriber profile** *domain-name*
5. **service local**
6. **exit**
7. **aaa attribute list** *list-name*

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	subscriber authorization enable Example: Router (config)# subscriber authorization enable	Enables subscriber authorization.
Step 4	subscriber profile <i>domain-name</i> Example: Router (config)# subscriber profile cisco1.com	Specifies the username domain that has to be matched and enters subscriber profile configuration mode.
Step 5	service local Example: Router (subscriber-profile)# service local	Specifies that local subscriber authorization should be performed.

	Command or Action	Purpose
Step 6	<pre>exit</pre> <p>Example: Router (subscriber-profile)# exit</p>	Exits subscriber profile configuration mode.
Step 7	<pre>aaa attribute list list-name</pre> <p>Example: Router (config)# aaa attribute list TEST</p>	Defines the AAA attribute list from which RADIUS attributes are retrieved.

Monitoring and Troubleshooting a Local AAA Server

The following debug commands may be helpful in monitoring and troubleshooting, especially to ensure that domain-based service authorization is being triggered and that location authorization is being called on the local AAA server, which triggers the service.

SUMMARY STEPS

1. **enable**
2. **debug aaa authentication**
3. **debug aaa authorization**
4. **debug aaa per-user**
5. **debug ppp authentication**
6. **debug ppp error**
7. **debug ppp forward**
8. **debug ppp negotiation**
9. **debug radius**
10. **debug sss error**

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 aaa authentication Example: Router# debug aaa authentication	Displays the methods of authentication being used and the results of these methods.
Step 3	debug aaa authorization Example: Router# debug aaa authorization	Displays the methods of authorization being used and the results of these methods.
Step 4	debug aaa per-user Example: Router# debug aaa per-user	Displays information about PPP session per-user activities.
Step 5	debug ppp authentication Example: Router# debug ppp authentication	Indicates whether a client is passing authentication.
Step 6	debug ppp error Example: Router (config)# debug ppp error	Displays protocol errors and error statistics that are associated with PPP connection negotiation and operation.
Step 7	debug ppp forward Example: Router# debug ppp forward	Displays who is taking control of a session.
Step 8	debug ppp negotiation Example: Router# debug ppp negotiation	Displays PPP packets sent during PPP startup, where PPP options are negotiated.
Step 9	debug radius Example: Router# debug radius	Displays information about the RADIUS server.
Step 10	debug sss error Example: Router# debug sss error	Displays diagnostic information about errors that may occur during SSS call setup.

Configuration Examples for Local AAA Server

This section contains the following configuration examples:

- [Local AAA Server: Example, page 9](#)
- [Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version: Example, page 10](#)

Local AAA Server: Example

The following example shows a Point to Point over Ethernet (PPPoE) group named “bba-group” that is configured for subscriber profile cisco.com (thus, any user with the domain name cisco.com will execute the subscriber profile cisco.com authorization policy). The cisco.com subscriber profile is configured to attach the AAA attribute list “TEST,” which has both “ip vrf forwarding” and “ip unnumbered” configured for PPP service under Link Control Protocol (LCP) negotiation. This configuration will essentially cause the named attributes to be applied on the session with the cisco.com domain under the bba-group “pppoe grp1.”

```

aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
  attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
  attribute type interface-config "ip vrf forwarding blue" service ppp protocol lcp
!
ip vrf blue
  description vrf blue template1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
subscriber authorization enable
!
subscriber profile cisco.com
  service local
  aaa attribute list TEST
!
bba-group pppoe grp1
  virtual-template 1
  service profile cisco.com
!
interface Virtual-Template1
  no ip address
  no snmp trap link-status
  no peer default ip address
  no keepalive
  ppp authentication pap template1
  ppp authorization template1
!

```



Note

In some versions of Cisco IOS software, it is better to use the explicit attribute instead of interface-config because it provides better scalability (full VAccess interfaces are not required, and sub interfaces could be used to provide the service). In such a case, you might configure “attribute type ip-unnumbered ‘FastEthernet0’ service ppp protocol ip” instead of “attribute type interface-config ‘ip unnumbered FastEthernet0’ service ppp protocol lcp.”

Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version: Example

The following output example of the **show aaa attributes** command lists RADIUS attributes, which can be used when configuring this feature.

```
Router# show aaa attributes protocol radius
```

```
IETF defined attributes:
```

```

Type=4      Name=acl                      Format=Ulong
  Protocol:RADIUS
      Unknown      Type=11      Name=Filter-Id      Format=Binary

```

Converts attribute 11 (Filter-Id) of type Binary into an internal attribute named "acl" of type Ulong. As such, one can configure this attributes locally by using the attribute type "acl."

```
Cisco VSA attributes:
```

```
Type=157   Name=interface-config          Format=String
```

```
Simply expects a string for the attribute of type "interface-config."
```



Note

The **aaa attribute list** command requires the Cisco IOS AAA version of an attribute, which is defined in the "Name" field above.

Additional References

The following sections provide references related to Local AAA Server.

Related Documents

Related Topic	Document Title
AAA, AAA attribute lists, AAA method lists, and subscriber profiles	The chapter " Configuring Local AAA Server, User Database—Domain to VRF " in <i>Cisco 10000 Series Broadband Aggregation and Leased-Line Configuration Guide</i>
Cisco IOS security commands	Cisco IOS Security Command Reference , Release 12.3T
Other Cisco IOS commands	Cisco IOS Command Reference , Release 12.3T

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

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 modified commands only.

- [aaa attribute list](#)
- [attribute type](#)

aaa attribute list

To define an authentication, authorization, and accounting (AAA) attribute list locally on a router, use the **aaa attribute list** command in global configuration mode. To remove the AAA attribute list, use the **no** form of this command.

aaa attribute list *list-name*

no aaa attribute list *list-name*

Syntax Description

<i>list-name</i>	Name of the local attribute list.
------------------	-----------------------------------

Command Default

A local attribute list is not defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XI1	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

There is no limit to the number of lists that can be defined (except for NVRAM storage limits).

Examples

The following example shows that the attribute list named “TEST” is to be added to the subscriber profile “cisco.com”:

```
aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
  attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
  attribute type interface-config "ip vrf forwarding blue" service ppp protocol lcp
!
ip vrf blue
  description vrf blue template1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
subscriber authorization enable
!
subscriber profile cisco.com
  service local
  aaa attribute list TEST
!
bba-group pppoe grp1
  virtual-template 1
```

```
service profile cisco.com
!
interface Virtual-Template1
no ip address
no snmp trap link-status
no peer default ip address
no keepalive
ppp authentication pap template1
ppp authorization template1
!
```

Related Commands

Command	Description
attribute type	Defines an attribute type that is to be added to an attribute list locally on a router.

attribute type

To define an attribute type that is to be added to an attribute list locally on a router, use the **attribute type** command in global configuration mode. To remove the attribute type from the list, use the **no** form of this command.

```
attribute type {name}{value} [service service] [protocol protocol] [tag]
```

```
no attribute type {name}{value} [service service] [protocol protocol] [tag]
```

Syntax Description

<i>name</i>	Defines the Cisco IOS authentication, authorization, and accounting (AAA) internal name of the Internet Engineering Task Force (IETF) RADIUS attribute to be added to the attribute list.
<i>value</i>	Defines a string, binary, or IPv4 address value. This is the RADIUS attribute that is being defined in Cisco IOS AAA format. When a string is added to the attribute value, the string should be inside quotation marks. For example, if the value is “interface-config” and the string is “ip unnumbered FastEthernet0,” you would write interface-config “ip unnumbered FastEthernet0”.
service <i>service</i>	(Optional) Access method, which is typically PPP.
protocol <i>protocol</i>	(Optional) Type of protocol, which can be ATM, IP, or virtual private dial-up network (VPDN).
<i>tag</i>	(Optional) Provides a means of grouping attributes that refer to the same VPDN tunnel.

Command Default

An attribute type is not added to the attribute list.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Attributes are added to the attribute list each time a new attribute type is defined.

When using the **no** form of this command, the entire line must be provided to avoid ambiguity.

Attributes are not validated at configuration. The AAA subsystem “knows” only the format that is expected by the services when the service defines a given attribute inside a definition file. However, it cannot validate the attribute information itself. This validation is done by a service when it first uses the attribute. This validation applies whether the AAA server is RADIUS or TACACS+. Thus, if you are not familiar with configuring a AAA server, it is advisable that you test your attribute list on a test device with the service that will be using the list before configuring and using it in a production environment.

Examples

The following example shows that the attribute list named “TEST” is to be added to the subscriber profile “cisco.com.” The attribute TEST includes the attribute types interface-config “ip unnumbered FastEthernet0” and interface-config “ip vrf forwarding blue.”

```

aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
  attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
  attribute type interface-config "ip vrf forwarding blue" service ppp protocol lcp
!
ip vrf blue
  description vrf blue template1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
subscriber authorization enable
!
subscriber profile cisco.com
  service local
  aaa attribute list TEST
!
bba-group pppoe grp1
  virtual-template 1
  service profile cisco.com
!
interface Virtual-Template1
  no ip address
  no snmp trap link-status
  no peer default ip address
  no keepalive
  ppp authentication pap template1
  ppp authorization template1
!

```

Related Commands

Command	Description
aaa attribute list	Defines a AAA attribute list locally on a router.

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)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2006 Cisco Systems, Inc. All rights reserved.