



Dial-on-Demand Authentication Enhancements

This feature module describes the Dial-on-Demand Authentication Enhancements feature and includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 3
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 4
- Configuration Examples, page 5
- Command Reference, page 5
- Glossary, page 8

Feature Overview

Large scale dialout eliminates the need to configure dialer maps on every network access server for every destination. Instead, you can create remote site profiles that contain outgoing call attributes (telephone number, service type, and so on) on the authentication, authorization and accounting (AAA) server. The profile is downloaded by the network access server (NAS) when packet traffic requires a call to be placed to a remote site.

This feature provides the following enhancements to dial-on-demand authentication:

- The NAS IP address plus a configured suffix can be sent to the RADIUS server as a username for authentication.
- A password other than the default password “cisco” can be sent to the RADIUS server for authentication.
- The username for two-way authentication is specified by a new vendor-specific attribute (VSA), “outbound:send-name=<string>”.

This feature also introduces modifications to the **dialer aaa** command, which provides username configuration capability for dial-on-demand.

Benefits

- This feature adds support for the new username format of IP address plus configured suffix.
- This feature adds support for a nondefault password configured by the user.
- This feature adds support for a new VSA, “outbound:send-name=<string>”, which specifies the username for two-way authentication.

Restrictions

- Dial-on-demand only supports IP over PPP encapsulation.
- Dial-on-demand does not support tunneling protocols such as Layer 2 Forwarding Protocol (L2F) or Layer 2 Tunneling Protocol (L2TP).
- Virtual profiles depend on PPP authentication; however, PPP authentication will create a problem for Ascend devices, which do not allow devices to authenticate users when answering a call (bidirectional authentication is not supported).
- The IP address of the remote device must be known before dialing out. Dial-on-Demand does not support dynamic IP address assignment.

Related Features and Technologies

- Dial-on-Demand
- Large Scale Dialout
- RADIUS

Related Documents

- *Cisco IOS Dial Services Configuration Guide: Terminal Services*, Release 12.1
- *Cisco IOS Dial Services Configuration Guide: Network Services*, Release 12.1
- *Cisco IOS Dial Services Command Reference*, Release 12.1
- *Cisco IOS Security Configuration Guide*, Release 12.1
- *Cisco IOS Security Command Reference*, Release 12.1
- *Large Scale Dialout*, Release 12.0(3)T feature module
- *RADIUS Attribute 44 (Accounting Session ID) in Access Requests*, Release 12.0(7)T feature module

Supported Platforms

- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 4000-M, 4500-M, 4700-M
- Cisco 4500 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco AS5200
- Cisco AS5300
- Cisco AS5800

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of MIBs supported by platform and Cisco IOS release and to download MIB modules, go to the Cisco MIB web site on Cisco Connection Online (CCO) at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

To use the Dial-on-Demand Authentication Enhancements feature, you must complete the following tasks:

- You must configure AAA network security services using the **aaa new-model** and **aaa authorization configuration** global configuration commands. For more information about AAA, refer to the "AAA Overview" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.1. The *Cisco IOS Security Command Reference*, Release 12.1, describes the commands used to configure AAA.
- You will also need to configure your NAS to communicate with the applicable security server, either RADIUS or TACACS+.
 - If you are using RADIUS and Ascend attributes, use the nonstandard keyword with the **radius-server host** command to enable your Cisco router, acting as a NAS, to recognize that the RADIUS security server is using a vendor-proprietary version of RADIUS. Use the

radius-server key command to specify the shared secret text string used between your Cisco router and the RADIUS server. For more information, refer to the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.1.

- If you are using TACACS+, use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons. Use the **tacacs-server key** command to specify the shared secret text string used between your Cisco router and the TACACS+ daemon. For more information, refer to the "Configuring TACACS+" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.1.

Configuration Tasks

See the following sections for configuration tasks for the Dial-on-Demand Authentication Enhancements feature. Each task in the list is identified as either optional or required.

- Configuring Suffix and Password in the RADIUS Access-Request Message
- Verifying Dialing Information

Configuring Suffix and Password in the RADIUS Access-Request Message

With the Dial-on-Demand Authentication Enhancements feature, you can configure the username in the access-request message to RADIUS. Currently the username is specified in the downloaded static routes, or if no name is specified, the destination IP address will be used. In either case, "-out" is the default suffix of the username and is appended to the username. The new format for composing the username attribute in the access-request messages is IP address plus configured suffix.

To provide username configuration capability for dial-on-demand, the **dialer aaa** command is implemented with the new **suffix** and **password** keywords under the **interface dialer** global configuration command:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables the AAA access control model.
Step 2	Router(config)# aaa route download min	Enables the download static route feature and sets the amount of time between downloads.
Step 3	Router(config)# aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
Step 4	Router(config)# interface dialer 1	Defines a dialer rotary group.
Step 5	Router(config-if)# dialer aaa	Allows a dialer to access the AAA server for dialing information.
Step 6	Router(config-if)# dialer aaa suffix @CiscoDoD password cisco	Allows a dialer to access the AAA server for dialing information and specifies a suffix and nondefault password for authentication.

Verifying Dialing Information

	Command	Purpose
Step 1	Router(config)# show run	Shows the configuration of access to the AAA server.

Configuration Examples

This section provides the following configuration example: Setting up the RADIUS Profile for Two-Way Authentication Example.

Setting up the RADIUS Profile for Two-Way Authentication Example

In the case of two-way authentication, the callback box will need to authenticate the NAS. The authentication username and password do not need to be configured locally on the NAS. Instead, they can be included in the access-accept message for dial-on-demand authentication. Currently, large scale dialout allows passwords to be specified in the dialout profile using the Cisco VSA “outbound:send-secret”.

A new VSA will be implemented to specify the username to use for two-way authentication. The new Cisco VSA has the following syntax:

```
cisco-avpair = "outbound:send-name=<string>"
```



Note

The **ppp authentication** command must be configured with the **radius** method.

Interface configuration should not have the **ppp pap sent-name password** command configured. For PAP, “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For CHAP, “preauth:send-name” will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use the name defined in “preauth:send-name” in the challenge packet to the caller box. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” will be used in the response packet.

Command Reference

This section documents the modified **dialer aaa** command. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

dialer aaa

To allow a dialer to access the authentication, authorization, and accounting (AAA) server for dialing information, use the **dialer aaa** interface configuration command. To disable this function, use the **no** form of this command.

```
dialer aaa [suffix string1] [password string2]
```

```
no dialer aaa [suffix string1] [password string2]
```

Syntax Description

suffix	(Optional) Defines a suffix for authentication.
<i>string1</i>	(Optional) Text to be appended after the IP address.
password	(Optional) Defines a nondefault password for authentication.
<i>string2</i>	(Optional) Password for RADIUS access-request messages.

Defaults

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(5)T	The suffix and password keywords were added.

Usage Guidelines

With this command, you can specify a suffix, a password, or both. If you do not specify a password, the default password will be “cisco.”



Note

Only IP addresses can be specified as usernames for the **dialer aaa suffix** command.

Examples

This example shows a user sending out packets from interface Dialer1 with a destination IP address of 1.1.1.1. The username in the access-request message is “1.1.1.1@CiscoDoD” and the password is “cisco”.

```
interface dialer1
dialer aaa
dialer aaa suffix @CiscoDoD password cisco
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
aaa new-model	Enables the AAA access control model.

Command	Description
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS server host.

Glossary

AAA—authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

authentication, authorization, and accounting—See AAA.

Challenge Handshake Authentication Protocol—See CHAP.

CHAP—Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access. Compare to PAP.

L2F—Layer 2 Forwarding Protocol. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

L2TP—Layer 2 Tunnel Protocol. Protocol that is one of the key building blocks for virtual private networks in the dial access space and is endorsed by Cisco and other internetworking industry leaders. This protocol combines the best of Cisco's Layer 2 Forwarding (L2F) protocol and Microsoft's Point-to-Point Tunneling Protocol (PPTP).

Layer 2 Forwarding Protocol—See L2F.

Layer 2 Tunnel Protocol—See L2TP.

Microsoft Challenge Handshake Authentication Protocol—See MS-CHAP.

MS-CHAP—Microsoft Challenge Handshake Authentication Protocol. Microsoft's version of CHAP; an extension to RFC 1994. Like the standard version of CHAP, it is used for PPP authentication. In this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows and a Cisco router or Cisco access server acting as a network access server (NAS).

NAS—network access server. Cisco platform (or collection of platforms such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the Public Switched Telephone Network).

network access server—See NAS.

PAP—Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines. Compare with CHAP.

Password Authentication Protocol—See PAP.

RADIUS—Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

Remote Authentication Dial-In User Service—See RADIUS.

vendor-specific attribute—See VSA.

VSA—vendor-specific attribute. An attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = "protocol:attribute=value".