



Authentication Proxy Accounting for HTTP

This feature module describes the Authentication Proxy Accounting for HTTP feature and includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 3
- Configuration Tasks, page 3
- Configuration Examples, page 4
- Command Reference, page 5
- Glossary, page 10

Feature Overview

The Authentication Proxy Accounting for HTTP feature provides “start” and “stop” accounting records with enough information to be used for billing and security auditing purposes. Thus, you can monitor the actions of authenticated hosts that use the authentication proxy service.

When an authentication proxy cache and associated dynamic access control lists (ACLs) are created, the authentication proxy will start to track the traffic from the authenticated host. Accounting saves data about this event in a data structure stored with the data of other users. If the accounting start option is enabled, you can generate an accounting record (a “start” record) at this time. Subsequent traffic from the authenticated host will be recorded when the dynamic ACL created by the authentication proxy receives the packets.

When an authentication proxy cache expires and is deleted, additional data, such as elapsed time, is added to the accounting information and a “stop” record is sent to the server. At this point, the information is deleted from the data structure.



Note

RADIUS attributes 42 and 47 will specify the traffic history from the authenticated host.

The accounting records for the authentication-proxy user session are related to the cache and the dynamic ACL usage.

Accounting Attributes

The accounting records must include the following authentication, authorization, and accounting (AAA) RADIUS attributes for both RADIUS and TACACS+:

- RADIUS attribute 42 (Acct-Input-Octets)
This attribute specifies how many octets have been received from the authenticated host over the course of the provided service.
- RADIUS attribute 47 (Acct-Input-Packets)
This attribute specifies how many packets have been received from the authenticated host over the course of the service provided to a framed user.
- RADIUS attribute 46 (Acct-Session-Time)
This attribute specifies for how long (in seconds) the user has been receiving service.

For more information on RADIUS attributes, refer to the appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*, Release 12.1.

Benefits

This feature provides “start” and “stop” accounting records that can be used for billing, security, or resource allocation purposes, thereby allowing users to track traffic from the authenticated hosts.

Related Documents

The following documents provide information related to the Authentication Proxy Accounting for HTTP feature:

- *Cisco IOS Security Configuration Guide*, Release 12.1
- *Cisco IOS Security Command Reference*, Release 12.1

Supported Platforms

The Authentication Proxy Accounting for HTTP feature is supported on the following platforms:

- Cisco 2600
- Cisco 3620
- Cisco 3640
- Cisco 7100
- Cisco 7200
- Cisco 7500

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.

Configuration Tasks

See the following section for configuration tasks for the Authentication Proxy Accounting for HTTP feature:

Configuring Authentication Proxy Accounting for HTTP (Optional)

Configuring Authentication Proxy Accounting for HTTP

To configure authentication proxy for accounting, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA.
Step 2	Router(config)# aaa authentication login default group tacacs+	Defines the list of authentication methods at login.
Step 3	Router(config)# aaa authorization auth-proxy default group tacacs+	Uses the auth-proxy keyword to enable authentication proxy for AAA methods.
Step 4	Router(config)# aaa accounting auth-proxy default start-stop group tacacs+	Uses the auth-proxy keyword to set up the authorization policy as dynamic ACLs that can be downloaded. This command activates authentication proxy accounting.
Step 5	Router(config)# tacacs-server host hostname	Specifies an AAA server. For RADIUS servers, use the radius-server host command.

	Command	Purpose
Step 6	Router(config)# tacacs-server key <i>string</i>	Sets the authentication and encryption key for communications between the router and the AAA server. For RADIUS servers, use the radius server key command.
Step 7	Router(config)# access-list <i>access-list number</i> permit tcp host <i>source</i> eq tacacs host <i>destination</i>	Creates an ACL entry to allow the AAA server to return traffic to the firewall. The source address is the IP address of the AAA server, and the destination is the IP address of the router interface where the AAA server resides.

After you configure authentication proxy for accounting, you must configure the HTTP server and authentication proxy.

For information on completing these tasks, refer to the chapter “Configuring Authentication Proxy” in the *Cisco IOS Security Configuration Guide*, Release 12.1.

Verifying Authentication Proxy Accounting for HTTP

To check the current authentication proxy configuration, use the **show ip auth-proxy configuration** command in privileged EXEC mode.

To display the user authentication entries, use the **show ip auth-proxy cache** command in privileged EXEC mode.

To display dynamic access list entries, use the **show ip access-lists** command in privileged EXEC mode.

Configuration Examples

This section provides the following configuration example:

Authentication Proxy Accounting Example

Authentication Proxy Accounting Example

The following example shows how to configure authentication proxy with the accounting feature:

```
!
aaa new-model
aaa authentication login default group tacacs+
aaa authentication login special none
aaa authorization exec default group tacacs+
aaa authorization network default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
!
```

```
!  
ip inspect name fw http java-list 10  
ip inspect name fw udp timeout 15  
ip inspect name fw tcp timeout 3600  
ip auth-proxy auth-proxy-banner  
ip auth-proxy auth-proxy-audit  
ip auth-proxy auth-cache-time 1  
ip auth-proxy name pxy http  
!  
interface Ethernet0/0  
 ip address 192.168.28.8 255.255.255.0 secondary  
 ip address 172.21.227.147 255.255.255.224  
 ip access-group 132 in  
 ip inspect fw in  
 ip auth-proxy pxy  
!  
interface Ethernet0/1  
 ip address 192.168.208.8 255.255.255.0 secondary  
 ip address 172.21.227.177 255.255.255.224  
 no ip mroute-cache  
!  
ip http server  
!  
ip http access-class 2  
!  
ip http authentication aaa  
!  
access-list 2 deny any  
access-list 10 permit any  
access-list 132 permit tcp host 171.71.39.30 eq tacacs host 192.168.208.8  
access-list 132 deny tcp any any  
access-list 132 deny udp any any  
access-list 132 permit ip any any  
tacacs-server host 171.71.39.30  
tacacs-server key cisco  
!  
line con 0  
 exec-timeout 0 0  
 password lab  
 login authentication special  
 transport input none  
line aux 0  
line vty 0 4  
 password lab  
!  
no scheduler allocate  
end
```

Command Reference

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

aaa accounting

To enable AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

```
aaa accounting {auth-proxy | system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | wait-start | none} [broadcast] method1 [method2...]
```

```
no aaa accounting {system | network | exec | connection | commands level} {default | list-name}
```

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user sessions.
system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests, including SLIP ¹ , PPP ² , PPP NCPs ³ , and ARA ⁴ .
exec	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the autocommand command.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, LAT ⁵ , TN3270, PAD ⁶ , and rlogin.
commands	Runs accounting for all commands at the specified privilege level.
<i>level</i>	Specific command level to track for accounting. Valid entries are integers from 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
<i>list-name</i>	Character string used to name the list of accounting methods.
start-stop	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
stop-only	Sends a “stop” accounting notice at the end of the requested user process.
wait-start	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process does not begin until the “start” accounting notice is received by the server.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, fail over occurs using the backup servers defined within that group.
<i>method1</i> [<i>method2...</i>]	At least one of the keywords described in Table 1.

1. SLIP = Serial Line Internet Protocol
2. PPP = Point-to-Point Protocol
3. PPP NCPs = Point-to-Point Protocol Network Control Protocols
4. ARA = AppleTalk Remote Access
5. LAT = local-area transport
6. PAD = packet assembler/disassembler

Defaults

AAA accounting is disabled. If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added.
12.1(1)T	The optional broadcast keyword was added.
12.1(5)T	The auth-proxy keyword was added.

Usage Guidelines

Use the **aaa accounting** command to enable accounting and to create named method lists defining specific accounting methods on a per-line or per-interface basis.

Table 1 contains descriptions of accounting method keywords.

Table 1 AAA Accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group group-name	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.

In Table 1, the **group radius**, **group tacacs+**, and **group group-name** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- **RADIUS**—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- **TACACS+**—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding the names of methods, such as radius or tacacs+) and *method* identifies the methods tried in the given sequence.

Named accounting method lists are specific to the indicated type of accounting. Method list keywords are described in Table 2.

Table 2 AAA Accounting Methods lists

Keyword	Description
auth-proxy	Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service.
commands	Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level.
connection	Creates a method list to provide accounting information about all outbound connections made from the network access server.
exec	Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times.
network	Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARA sessions.



Note

System accounting does not use named accounting lists; you can only define the default list for system accounting.

For minimal accounting, include the **stop-only** keyword to send a “stop” record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a “start” accounting notice at the beginning of the requested process and a “stop” accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. Like the **start-stop** keyword, the **wait-start** keyword sends “start” and “stop” accounting notices; however, the requested user process does not begin until the “start” accounting notice is received by the accounting server. The **none** keyword disables accounting services for the specified line or interface.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, refer to the appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the appendix “TACACS+ Attribute-Value Pairs” in the *Cisco IOS Security Configuration Guide*.



Note

This command cannot be used with TACACS or extended TACACS.

Examples

The following example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only group tacacs+
```

The following example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a stop-only restriction. The **aaa accounting** command activates authentication proxy accounting.

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
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.

access control list—See ACL.

ACL—access control list. List kept by routers to control access to or from the router for a number of services. For example, an access control list can prevent packets with a certain IP address from leaving a particular interface in the router.

authentication, authorization, and accounting—See AAA.

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.

TACACS+—Terminal Access Controller Access Control System Plus. Database for authenticating users who are attempting to gain access to a router or network access server. TACACS+ databases typically run on a UNIX or Windows NT workstation.

Terminal Access Controller Access Control System Plus—See TACACS+.