

# TACACS+ Attribute-Value Pairs

---

Terminal Access Controller Access Control System Plus (TACACS+) attribute-value (AV) pairs are used to define specific authentication, authorization, and accounting elements in a user profile, which is stored on the TACACS+ daemon. This appendix lists the TACACS+ AV pairs currently supported.

## TACACS+ AV Pairs

Table 35 lists the supported TACACS+ AV pairs and specifies the Cisco IOS release in which they are implemented.

**Table 35** Supported TACACS+ AV Pairs

Attribute	Description	11.0	11.1	11.2	11.3	12.0
acl=x	ASCII number representing a connection access list. Used only when service=shell.	yes	yes	yes	yes	yes
addr-pool=x	<p>Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip.</p> <p>Note that <b>addr-pool</b> works in conjunction with local pooling. It specifies the name of a local pool (which must be preconfigured on the network access server). Use the <b>ip-local pool</b> command to declare local pools. For example:</p> <pre>ip address-pool local ip local pool boo 10.0.0.1 10.0.0.10 ip local pool moo 10.0.0.1 10.0.0.20</pre> <p>You can then use TACACS+ to return addr-pool=boo or addr-pool=moo to indicate the address pool from which you want to get this remote node's address.</p>	yes	yes	yes	yes	yes

**Table 35 Supported TACACS+ AV Pairs (Continued)**

Attribute	Description	11.0	11.1	11.2	11.3	12.0
addr=x	A network address. Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP. For example, addr=10.2.3.4.	yes	yes	yes	yes	yes
autocmd=x	Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet domain.com). Used only with service=shell.	yes	yes	yes	yes	yes
callback-dialstring	Sets the telephone number for a callback (for example: callback-dialstring=408-555-1212). Value is NULL, or a dial-string. A NULL value indicates that the service might choose to get the dialstring through other means. Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.	no	yes	yes	yes	yes
callback-line	The number of a TTY line to use for callback (for example: callback-line=4). Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.	no	yes	yes	yes	yes
callback-rotary	The number of a rotary group (between 0 and 100 inclusive) to use for callback (for example: callback-rotary=34). Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.	no	yes	yes	yes	yes
cmd-arg=x	An argument to a shell (EXEC) command. This indicates an argument for the shell command that is to be run. Multiple cmd-arg attributes can be specified, and they are order dependent.	yes	yes	yes	yes	yes
cmd=x	A shell (EXEC) command. This indicates the command name for a shell command that is to be run. This attribute must be specified if service equals "shell." A NULL value indicates that the shell itself is being referred to.	yes	yes	yes	yes	yes

**Table 35 Supported TACACS+ AV Pairs (Continued)**

Attribute	Description	11.0	11.1	11.2	11.3	12.0
dns-servers=	Identifies a DNS server (primary or secondary) that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with service=ppp and protocol=ip. The IP address identifying each DNS server is entered in dotted decimal format.	no	no	no	yes	yes
gw-password	Specifies the password for the home gateway during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.	no	no	yes	yes	yes
idletime=x	Sets a value, in minutes, after which an idle session is terminated. Does not work for PPP. A value of zero indicates no timeout.	no	yes	yes	yes	yes
inac1#<n>	ASCII access list identifier for an input access list to be installed and applied to an interface for the duration of the current connection. Used with service=ppp and protocol=ip, and service service=ppp and protocol =ipx. Per-user access lists do not currently work with ISDN interfaces.	no	no	no	yes	yes
inac1=x	ASCII identifier for an interface input access list. Used with service=ppp and protocol=ip. Per-user access lists do not currently work with ISDN interfaces.	yes	yes	yes	yes	yes
interface-config=	Specifies user-specific AAA interface configuration information with Virtual Profiles. The information that follows the equal sign (=) can be any Cisco IOS interface configuration command.	no	no	no	yes	yes
ip-addresses	Space-separated list of possible IP addresses that can be used for the end-point of a tunnel. Used with service=ppp and protocol=vpdn.	no	no	yes	yes	yes

**Table 35 Supported TACACS+ AV Pairs (Continued)**

Attribute	Description	11.0	11.1	11.2	11.3	12.0
link-compression=	<p>Defines whether to turn on or turn off “stac” compression over a PPP link.</p> <p>Link compression is defined as a numeric value as follows:</p> <ul style="list-style-type: none"> <li>• 0: None</li> <li>• 1: Stac</li> <li>• 2: Stac-Draft-9</li> <li>• 3: MS-Stac</li> </ul>	no	no	no	yes	yes
load-threshold=<n>	<p>Sets the load threshold for the caller at which additional links are either added to or deleted from the multilink bundle. If the load goes above the specified value, additional links are added. If the load goes below the specified value, links are deleted. Used with service=ppp and protocol=multilink. The range for &lt;n&gt; is from 1 to 255.</p>	no	no	no	yes	yes
max-links=<n>	<p>Restricts the number of links that a user can have in a multilink bundle. Used with service=ppp and protocol=multilink. The range for &lt;n&gt; is from 1 to 255.</p>	no	no	no	yes	yes
nas-password	<p>Specifies the password for the network access server during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.</p>	no	no	yes	yes	yes
nocallback-verify	<p>Indicates that no callback verification is required. The only valid value for this parameter is 1 (for example, nocallback-verify=1). Used with service=arap, service=slip, service=ppp, service=shell. There is no authentication on callback. Not valid for ISDN.</p>	no	yes	yes	yes	yes
noescape=x	<p>Prevents user from using an escape character. Used with service=shell. Can be either true or false (for example, noescape=true).</p>	yes	yes	yes	yes	yes

**Table 35 Supported TACACS+ AV Pairs (Continued)**

Attribute	Description	11.0	11.1	11.2	11.3	12.0
nohangup=x	Used with service=shell. Specifies the nohangup option, which means that after an EXEC shell is terminated, the user is presented with another login (username) prompt. Can be either true or false (for example, nohangup=false).	yes	yes	yes	yes	yes
old-prompts	Allows providers to make the prompts in TACACS+ appear identical to those of earlier systems (TACACS and Extended TACACS). This allows administrators to upgrade from TACACS or Extended TACACS to TACACS+ transparently to users.	yes	yes	yes	yes	yes
outacl#<n>	ASCII access list identifier for an interface output access list to be installed and applied to an interface for the duration of the current condition. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Per-user access lists do not currently work with ISDN interfaces.	no	no	no	yes	yes
outacl=x	ASCII identifier for an interface output access list. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Contains an IP output access list for SLIP or PPP/IP (for example, outacl=4). The access list itself must be preconfigured on the router. Per-user access lists do not currently work with ISDN interfaces.	yes (PPP/IP only)	yes	yes	yes	yes
pool-def#<n>	Defines IP address pools on the network access server. Used with service=ppp and protocol=ip.	no	no	no	yes	yes

**Table 35 Supported TACACS+ AV Pairs (Continued)**

<b>Attribute</b>	<b>Description</b>	<b>11.0</b>	<b>11.1</b>	<b>11.2</b>	<b>11.3</b>	<b>12.0</b>
pool-timeout=	Defines (in conjunction with pool-def) IP address pools on the network access server. During IPCP address negotiation, if an IP pool name is specified for a user (see the addr-pool attribute), a check is made to see if the named pool is defined on the network access server. If it is, the pool is consulted for an IP address.	no	no	yes	yes	yes
ppp-vj-slot-compression	Instructs the Cisco router not to use slot compression when sending VJ-compressed packets over a PPP link.	no	no	no	yes	yes
priv-lvl=x	Privilege level to be assigned for the EXEC. Used with service=shell. Privilege levels range from 0 to 15, with 15 being the highest.	yes	yes	yes	yes	yes
protocol=x	A protocol that is a subset of a service. An example would be any PPP NCP. Currently known values are <b>lcp, ip, ipx, atalk, vines, lat, xremote, tn3270, telnet, rlogin, pad, vpdn, osicp, deccp, ccp, cdp, bridging, xns, nbf, bap, multilink, and unknown.</b>	yes	yes	yes	yes	yes

Table 35 Supported TACACS+ AV Pairs (Continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0
route	<p>Specifies a route to be applied to an interface. Used with <code>service=slip</code>, <code>service=ppp</code>, and <code>protocol=ip</code>.</p> <p>During network authorization, the route attribute can be used to specify a per-user static route, to be installed by TACACS+ as follows:</p> <pre>route="dst_address mask [ gateway ]"</pre> <p>This indicates a temporary static route that is to be applied. The <i>dst_address</i>, <i>mask</i>, and <i>gateway</i> are expected to be in the usual dotted-decimal notation, with the same meanings as in the familiar <b>ip route</b> configuration command on a network access server.</p> <p>If <i>gateway</i> is omitted, the peer's address is the gateway. The route is expunged when the connection terminates.</p>	no	yes	yes	yes	yes
route#<n>	Like the route AV pair, this specifies a route to be applied to an interface, but these routes are numbered, allowing multiple routes to be applied. Used with <code>service=ppp</code> and <code>protocol=ip</code> , and <code>service=ppp</code> and <code>protocol=ipx</code> .	no	no	no	yes	yes
routing=x	Specifies whether routing information is to be propagated to and accepted from this interface. Used with <code>service=slip</code> , <code>service=ppp</code> , and <code>protocol=ip</code> . Equivalent in function to the <code>/routing</code> flag in SLIP and PPP commands. Can either be true or false (for example, <code>routing=true</code> ).	yes	yes	yes	yes	yes
rite-ftp-in#<n>	Specifies an input access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with <code>service=ppp</code> and <code>protocol=ip</code> , and with <code>service=ppp</code> and <code>protocol=ipx</code> .	no	no	no	yes	yes

**Table 35 Supported TACACS+ AV Pairs (Continued)**

<b>Attribute</b>	<b>Description</b>	<b>11.0</b>	<b>11.1</b>	<b>11.2</b>	<b>11.3</b>	<b>12.0</b>
rte-flt-out#<n>	Specifies an output access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.	no	no	no	yes	yes
sap#<n>	Specifies static Service Advertising Protocol (SAP) entries to be installed for the duration of a connection. Used with service=ppp and protocol=ipx.	no	no	no	yes	yes
sap-fltr-in#<n>	Specifies an input SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.	no	no	no	yes	yes
sap-fltr-out#<n>	Specifies an output SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.	no	no	no	yes	yes
service=x	The primary service. Specifying a service attribute indicates that this is a request for authorization or accounting of that service. Current values are <b>slip, ppp, arap, shell, tty-daemon, connection,</b> and <b>system</b> . This attribute must always be included.	yes	yes	yes	yes	yes
source-ip=x	Used as the source IP address of all VPDN packets generated as part of a VPDN tunnel. This is equivalent to the Cisco <b>vpdn outgoing</b> global configuration command.	no	no	yes	yes	yes
timeout=x	The number of minutes before an EXEC or ARA session disconnects (for example, timeout=60). A value of zero indicates no timeout. Used with service=arap.	yes	yes	yes	yes	yes

**Table 35 Supported TACACS+ AV Pairs (Continued)**

Attribute	Description	11.0	11.1	11.2	11.3	12.0
tunnel-id	Specifies the username that will be used to authenticate the tunnel over which the individual user MID will be projected. This is analogous to the <i>remote name</i> in the <b>vpdn outgoing</b> command. Used with <code>service=ppp</code> and <code>protocol=vpdn</code> .	no	no	yes	yes	yes
wins-servers=	Identifies a Windows NT server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with <code>service=ppp</code> and <code>protocol=ip</code> . The IP address identifying each Windows NT server is entered in dotted decimal format.	no	no	no	yes	yes
zonelist=x	A numeric zonelist value. Used with <code>service=arap</code> . Specifies an AppleTalk zonelist for ARA (for example, <code>zonelist=5</code> ).	yes	yes	yes	yes	yes

For more information about configuring TACACS+, refer to the “Configuring TACACS+” chapter. For more information about configuring TACACS+ authentication, refer to the “Configuring Authorization” chapter.

## TACACS+ Accounting AV Pairs

Table 36 lists the supported TACACS+ accounting AV pairs and the Cisco IOS release in which they are implemented.

**Table 36 Supported TACACS+ Accounting AV Pairs**

Attribute	Description	11.0	11.1	11.2	11.3	12.0
bytes_in	The number of input bytes transferred during this connection.	yes	yes	yes	yes	yes
bytes_out	The number of output bytes transferred during this connection.	yes	yes	yes	yes	yes
cmd	The command the user executed.	yes	yes	yes	yes	yes
data-rate - This AV pair has been renamed. See <code>nas-rx-speed</code> .						

**Table 36 Supported TACACS+ Accounting AV Pairs (Continued)**

Attribute	Description	11.0	11.1	11.2	11.3	12.0
disc-cause	Specifies the reason a connection was taken off-line. The Disconnect-Cause attribute is sent in accounting-stop records. This attribute also causes stop records to be generated without first generating start records if disconnection occurs before authentication is performed. Refer to Table 37 for a list of Disconnect-Cause values and their meanings.	no	no	no	yes	yes
disc-cause-ext	Extends the disc-cause attribute to support vendor-specific reasons that a connection was taken off-line.	no	no	no	yes	yes
elapsed_time	The elapsed time in seconds for the action. Useful when the device does not keep real time.	yes	yes	yes	yes	yes
event	Information included in the accounting packet that describes a state change in the router. Events described are accounting starting and accounting stopping.	yes	yes	yes	yes	yes
mlp-links-max	Gives the count of links which are known to have been in a given multilink session at the time the accounting record is generated.	no	no	no	yes	yes
mlp-sess-id	Reports the identification number of the multilink bundle when the session closes. This attribute applies to sessions that are part of a multilink bundle. This attribute is sent in authentication-response packets.	no	no	no	yes	yes
nas-rx-speed	Specifies the average number of bits per second over the course of the connection's lifetime. This attribute is sent in accounting-stop records.	no	no	no	yes	yes
nas-tx-speed	Reports the transmit speed negotiated by the two modems.	no	no	no	yes	yes
paks_in	The number of input packets transferred during this connection.	yes	yes	yes	yes	yes
paks_out	The number of output packets transferred during this connection.	yes	yes	yes	yes	yes

**Table 36 Supported TACACS+ Accounting AV Pairs (Continued)**

<b>Attribute</b>	<b>Description</b>	<b>11.0</b>	<b>11.1</b>	<b>11.2</b>	<b>11.3</b>	<b>12.0</b>
port	The port the user was logged in to.	yes	yes	yes	yes	yes
pre-bytes-in	Records the number of input bytes before authentication. This attribute is sent in accounting-stop records.	no	no	no	yes	yes
pre-bytes-out	Records the number of output bytes before authentication. This attribute is sent in accounting-stop records.	no	no	no	yes	yes
pre-paks-in	Records the number of input packets before authentication. This attribute is sent in accounting-stop records.	no	no	no	yes	yes
pre-paks-out	Records the number of output packets before authentication. The Pre-Output-Packets attribute is sent in accounting-stop records.	no	no	no	yes	yes
pre-session-time	Specifies the length of time, in seconds, from when a call first connects to when it completes authentication.	no	no	no	yes	yes
priv_level	The privilege level associated with the action.	yes	yes	yes	yes	yes
protocol	The protocol associated with the action.	yes	yes	yes	yes	yes
reason	Information included in the accounting packet that describes the event that caused a system change. Events described are system reload, system shutdown, or when accounting is reconfigured (turned on or off).	yes	yes	yes	yes	yes
service	The service the user used.	yes	yes	yes	yes	yes
start_time	The time the action started (in seconds since the epoch, 12:00 a.m. Jan 1 1970). The clock must be configured to receive this information.	yes	yes	yes	yes	yes
stop_time	The time the action stopped (in seconds since the epoch.) The clock must be configured to receive this information.	yes	yes	yes	yes	yes
task_id	Start and stop records for the same event must have matching (unique) task_id numbers.	yes	yes	yes	yes	yes

**Table 36 Supported TACACS+ Accounting AV Pairs (Continued)**

Attribute	Description	11.0	11.1	11.2	11.3	12.0
timezone	The time zone abbreviation for all timestamps included in this packet.	yes	yes	yes	yes	yes
xmit-rate - This AV pair has been renamed. See nas-tx-speed.						

Table 37 lists the values and their meanings for the Disconnect Cause (disc-cause) attribute.

**Table 37 Disc-Causes-Ext Attribute Values**

Value	Description
Unknown (1002)	Reason unknown.
CLID-Authentication-Failure (1004)	Failure to authenticate calling-party number.
No-Carrier (1010)	No carrier detected. This value applies to modem connections.
Lost-Carrier (1011)	Loss of carrier. This value applies to modem connections.
No-Detected-Result-Codes (1012)	Failure to detect modem result codes. This value applies to modem connections.
User-Ends-Session (1020)	User terminates a session. This value applies to EXEC sessions.
Idle-Timeout (1021)	Timeout waiting for user input. This value applies to all session types.
Exit-Telnet-Session (1022)	Disconnect due to exiting Telnet session. This value applies to EXEC sessions.
No-Remote-IP-Addr (1023)	Could not switch to SLIP/PPP; the remote end has no IP address. This value applies to EXEC sessions.
Exit-Raw-TCP (1024)	Disconnect due to exiting raw TCP. This value applies to EXEC sessions.
Password-Fail (1025)	Bad passwords. This value applies to EXEC sessions.
Raw-TCP-Disabled (1026)	Raw TCP disabled. This value applies to EXEC sessions.
Control-C-Detected (1027)	Control-C detected. This value applies to EXEC sessions.
EXEC-Process-Destroyed (1028)	EXEC process destroyed. This value applies to EXEC sessions.
Timeout-PPP-LCP (1040)	PPP LCP negotiation timed out. This value applies to PPP sessions.
Failed-PPP-LCP-Negotiation (1041)	PPP LCP negotiation failed. This value applies to PPP sessions.
Failed-PPP-PAP-Auth-Fail (1042)	PPP PAP authentication failed. This value applies to PPP sessions.
Failed-PPP-CHAP-Auth (1043)	PPP CHAP authentication failed. This value applies to PPP sessions.
Raw-TCP-Disabled (1044)	PPP remote authentication failed. This value applies to PPP sessions.
PPP-Remote-Terminate (1045)	PPP received a Terminate Request from remote end. This value applies to PPP sessions.

**Table 37 Disc-Causes-Ext Attribute Values (Continued)**

Value	Description
PPP-Closed-Event (1046)	Upper layer requested that the session be closed. This value applies to PPP sessions.
Session-Timeout (1000)	Session timed out. This value applies to all session types.
Session-Failed-Security (1101)	Session failed for security reasons. This value applies to all session types.
Session-End-Callback (1102)	Session terminated due to callback. This value applies to all session types.
Invalid-Protocol (1120)	Call refused because the detected protocol is disabled. This value applies to all session types.

Table 38 lists the values and their meanings as to why the connection was terminated.

**Table 38 Disc-Cause**

Value	Description
(1)	.User request
(2)	Lost carrier
(3)	Lost service
(4)	Idle timeout
(5)	Session timeout
(6)	Admin reset
(7)	Admin reboot
(8)	Port error
(9)	NAS error
(10)	NAS request
(11)	NAS reboot
(12)	Port unneeded
(13)	Port pre-empted
(14)	Port suspended
(15)	Service unavailable
(16)	Callback
(17)	User error
(18)	Host request

For more information about configuring TACACS+, refer to the “Configuring TACACS+” chapter.  
For more information about configuring TACACS+ accounting, refer to the “Configuring Accounting” chapter.

