

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 22 lists the supported TACACS+ AV pairs.

Table 22 Supported TACACS+ AV Pairs

Attribute	Description	Cisco IOS Release 11.0	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
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 slip , ppp , arap , shell , tty-daemon , connection , and system . This attribute must always be included.	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 lcp , ip , ipx , atalk , vines , lat , xremote , tn3270 , telnet , rlogin , pad , vpdn , osicp , deccp , ccp , cdp , bridging , xns , nbf , bap , multilink , and unknown .	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
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 may be specified, and they are order dependent.	yes	yes	yes	yes

Table 22 Supported TACACS+ AV Pairs (Continued)

Attribute	Description	Cisco IOS Release 11.0	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
acl=x	ASCII number representing a connection access list. Used only when service=shell.	yes	yes	yes	yes
inacl=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
inacl#<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
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
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
zonelist=x	A numeric zonelist value. Used with service=arap. Specifies an AppleTalk zonelist for ARA (for example, zonelist=5).	yes	yes	yes	yes
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

Table 22 Supported TACACS+ AV Pairs (Continued)

Attribute	Description	Cisco IOS Release 11.0	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
addr-pool=x	<p>Specifies the name of a local pool from which to get the address of the remote host. Used with <code>service=ppp</code> and <code>protocol=ip</code>.</p> <p>Note that addr-pool 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 ip-local pool 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 <code>addr-pool=boo</code> or <code>addr-pool=moo</code> to indicate the address pool from which you want to get this remote node's address.</p>	yes	yes	yes	yes
routing=x	<p>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>).</p>	yes	yes	yes	yes
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 ip route 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

Table 22 Supported TACACS+ AV Pairs (Continued)

Attribute	Description	Cisco IOS Release 11.0	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
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 service=ppp and protocol=ip, and service=ppp and protocol=ipx.	no	no	no	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
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
autocmd=x	Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet muruga.com). Used only with service=shell.	yes	yes	yes	yes
noescape=x	Prevents user from using an escape character. Used with service=shell. Can be either true or false (for example, noescape=true).	yes	yes	yes	yes
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
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
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 may 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
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

Table 22 Supported TACACS+ AV Pairs (Continued)

Attribute	Description	Cisco IOS Release 11.0	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
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
nocallback-verify	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.	no	yes	yes	yes
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 vpdn outgoing command. Used with service=ppp and protocol=vpdn.	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
nas-password	Specifies the password for the network access server during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.	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
rte-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 service=ppp and protocol=ip, and with service=ppp and protocol=ipx.	no	no	no	yes
rte-ftp-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
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

Table 22 Supported TACACS+ AV Pairs (Continued)

Attribute	Description	Cisco IOS Release 11.0	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
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
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
pool-def#<n>	Used to define IP address pools on the network access server. Used with service=ppp and protocol=ip.	no	no	no	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 vpdn outgoing global configuration command.	no	no	yes	yes
max-links=<n>	Restricts the number of links that a user can have in a multilink bundle. Used with service=ppp and protocol=multilink. The range for <n> is from 1 to 255.	no	no	no	yes
load-threshold=<n>	Sets the load threshold 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 <n> is from 1 to 255.	no	no	no	yes
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
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 service=ppp and protocol=ip. The IP address identifying each Windows NT server is entered in dotted decimal format.	no	no	no	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 23 lists the supported TACACS+ accounting AV pairs.

Table 23 Supported TACACS+ Accounting AV Pairs

Attribute	Description	Cisco IOS Release 11.0	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
service	The service the user used.	yes	yes	yes	yes
port	The port the user was logged in to.	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
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
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
elapsed_time	The elapsed time in seconds for the action. Useful when the device does not keep real time.	yes	yes	yes	yes
timezone	The time zone abbreviation for all timestamps included in this packet.	yes	yes	yes	yes
priv_level	The privilege level associated with the action.	yes	yes	yes	yes
cmd	The command the user executed.	yes	yes	yes	yes
protocol	The protocol associated with the action.	yes	yes	yes	yes
bytes_in	The number of input bytes transferred during this connection.	yes	yes	yes	yes
bytes_out	The number of output bytes transferred during this connection.	yes	yes	yes	yes
paks_in	The number of input packets transferred during this connection.	yes	yes	yes	yes
paks_out	The number of output packets transferred during this connection.	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

Table 23 Supported TACACS+ Accounting AV Pairs (Continued)

Attribute	Description	Cisco IOS Release 11.0	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
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

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.