



RDBMS Synchronization Import Definitions

RDBMS synchronization import definitions are a listing of the action codes allowable in an `accountActions` table. The RDBMS Synchronization feature of Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS, uses a table named `accountActions` as input for automated or manual updates of the ACS internal database. For more information about the RDBMS Synchronization feature and `accountActions`, see [RDBMS Synchronization, page 9-17](#).

This chapter contains the following topics:

- [accountActions Specification, page F-1](#)
- [Supported Versions for ODBC Datasources, page F-3](#)
- [Action Codes, page F-3](#)
- [ACS Attributes and Action Codes, page F-22](#)
- [An Example of accountActions, page F-25](#)

accountActions Specification

Whether you create `accountActions` by hand in a text editor or through automation using a third-party system that writes to `accountActions`, you must adhere to the `accountActions` specification and must only use the action codes detailed in [Action Codes, page F-3](#). Otherwise, RDBMS Synchronization may import incorrect information into the ACS internal database or may fail to occur at all.

accountActions Format

Each row in `accountActions` has 14 fields (or columns). [Table F-1](#) lists the fields that compose `accountActions`. [Table F-1](#) also reflects the order in which the fields appear in `accountActions`.

The one-letter or two-letter abbreviations given in the Mnemonic column are a shorthand notation used to indicate required fields for each action code in [Action Codes, page F-3](#).

To see an example `accountActions`, see [An Example of accountActions, page F-25](#).

Table F-1 accountActions Fields

Field Name	Mnemonic	Type	Size (Max. Length)	Comments
SequenceId	SI	AutoNumber	32	The unique action ID.
Priority	P	Integer	1	The priority with which this update is to be treated. Zero (0) is the lowest priority.
UserName	UN	String	32	The name of the user to which the transaction applies.
GroupName	GN	String	32	The name of the group to which the transaction applies.
Action	A	Number	0-2 ¹⁶	The action required. (See Action Codes , page F-3.)
ValueName	VN	String	255	The name of the parameter to change.
Value1	V1	String	255	The new value (for numeric parameters, this is a decimal string).
Value2	V2	String	255	The name of a TACACS+ protocol; for example, “ip” or RADIUS VSA Vendor ID.
Value3	V3	String	255	The name of a TACACS+ service; for example, “ppp” or the RADIUS VSA attribute number.
DateTime	DT	DateTime	—	The date and time the action was created.
MessageNo	MN	Integer	—	Used to number related transactions for audit purposes.
ComputerNames	CN	String	32	RESERVED by CSDBSync.
AppId	AI	String	255	The type of configuration parameter to change.
Status	S	Number	32	TRI-STATE:0=not processed, 1=done, 2=failed. This value should normally be set to 0.

accountActions Mandatory Fields

For all actions, the following fields cannot be empty and must have a valid value:

- Action
- SequenceID
- Status

In addition to the previous required fields, the DateTime, UserName and GroupName fields are also often required to have a valid value:

- If a transaction is acting upon a user account, a valid value is required in the UserName field.
- If a transaction is acting upon a group, a valid value is required in the GroupName field.
- If a transaction is acting upon a AAA client configuration, neither the UserName field nor the GroupName field require a value.



Note

The UserName and GroupName fields are mutually exclusive; only one of these two fields can have a value and neither field is always required.

accountActions Processing Order

ACS reads rows from accountActions and processes them in a specific order. ACS determines the order first by the values in the Priority fields (mnemonic: P) and then by the values in the Sequence ID fields (mnemonic: SI). ACS processes the rows with the highest Priority field. The lower the number in the Priority field, the higher the priority. For example, if row A has the value 1 in its Priority field and row B has the value 2 in its Priority field, ACS would process row A first, regardless of whether row B has a lower sequence ID or not. If rows have an equal priority, ACS processes them by their sequence ID, with the lowest sequence ID processed first.

Thus, the Priority field (P) enables transactions of higher importance to occur first, such as deleting a user or changing a password. In the most common implementations of RDBMS Synchronization, a third-party system writes to accountActions in batch mode, with all actions (rows) assigned a priority of zero (0).

**Note**

When changing transaction priorities, be careful that they are processed in the correct order; for example, a user account must be created before the user password is assigned.

You can use the MessageNo field (mnemonic: MN) to associate related transactions, such as the addition of a user and subsequent actions to set password values and status. You can use the MessageNo field to create an audit trail for a third-party system that writes to accountActions.

Supported Versions for ODBC Datasources

The following versions are supported for RDBMS synchronization through ODBC.

- MS-SQL version 3.80 later
- ODBC version 3.80 or later

Action Codes

This section provides the action codes valid for use in the Action field (mnemonic: A) of accountActions. The Required column uses the field mnemonic names to indicate which fields should be completed, except for the mandatory fields, which are assumed. For more information about the mnemonic names of accountActions fields, see [Table F-1](#). For more information about the mandatory fields, see [accountActions Mandatory Fields, page F-2](#).

If an action can be applied to a user or group, UN|GN appears, using the vertical bar (|) to indicate that either one of the two fields is required. To make the action affect only the user, leave the group name empty; to make the action affect only the group, leave the user name empty.

This section contains the following topics:

- [Action Codes for Setting and Deleting Values, page F-4](#)
- [Action Codes for Creating and Modifying User Accounts, page F-4](#)
- [Action Codes for Initializing and Modifying Access Filters, page F-9](#)
- [Action Codes for Modifying TACACS+ and RADIUS Group and User Settings, page F-12](#)
- [Action Codes for Modifying Network Configuration, page F-17](#)

Action Codes for Setting and Deleting Values

The two most fundamental action codes are SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2), described in [Table F-2](#).

The SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2) actions, described in [Table F-2](#), instruct RDBMS Synchronization to assign a value to various internal attributes in ACS. Unless a Cisco representative asks you to use these action codes for other purposes, you can only use these action codes for assigning values to user-defined fields (see [User-Specific Attributes](#), page F-22).

Table F-2 Action Codes for Setting and Deleting Values

Action Code	Name	Required	Description
1	SET_VALUE	UNIGN, AI, VN, V1, V2	<p>Sets a value (V1) named (VN) of type (V2) for App ID (AI).</p> <p>App IDs (AI) can be one of the following:</p> <ul style="list-style-type: none"> • APP_CSAUTH • APP_CSTACACS • APP_CSRADIUS • APP_CSADMIN <p>Value types (V2) can be one of the following:</p> <ul style="list-style-type: none"> • TYPE_BYTE—Single 8-bit number. • TYPE_SHORT—Single 16-bit number. • TYPE_INT—Single 32-bit number. • TYPE_STRING—Single string. • TYPE_ENCRYPTED_STRING—Single string to be saved encrypted. • TYPE_MULTI_STRING—Tab-separated set of substrings. • TYPE_MULTI_INT—Tab-separated set of 32-bit numbers. <p>For example:</p> <pre>UN = "fred" AI = "APP_CSAUTH" VN = "My Value" V2 = "TYPE_MULTI_STRING" V1 = "str1tabstr2tabstr3"</pre>
2	DELETE_VALUE	UNIGN, AI, VN	Deletes value (VN) for App ID (AI) and user (UN) or group (GN).

Action Codes for Creating and Modifying User Accounts

[Table F-3](#) lists the action codes for creating, modifying, and deleting user accounts.



Note

Before you can modify a user account, such as assigning a password, you must create the user account, in the web interface or by using the ADD_USER action (action code: 100).

Transactions using these codes affect the configuration that appears in the User Setup section of the web interface. For more information about the User Setup section, see [Chapter 7, “User Management.”](#)

Table F-3 User Creation and Modification Action Codes

Action Code	Name	Required	Description
100	ADD_USER	UNIGN, V1	Creates a user (32 characters maximum). V1 is used as the initial password. Optionally, the user can also be assigned to a group.
101	DELETE_USER	UN	Removes a user.
102	SET_PAP_PASS	UN, V1	Sets the PAP password for a user (64 ASCII characters maximum). CHAP/ARAP will also default to this.
103	SET_CHAP_PASS	UN, V1	Sets the CHAP/ARAP password for a user (64 characters maximum).
104	SET_OUTBOUND_CHAP_PASS	UN, V1	Sets the CHAP/ARAP password for a user (32 characters maximum).
105	SET_T+_ENABLE_PASS	UN, VN, V1, V2, V3	<p>Sets the TACACS+ enable password (V1) (32 characters maximum) and Max Privilege level (V2) (0-15).</p> <p>The enable type (V3) should be one of the following:</p> <ul style="list-style-type: none"> • ENABLE_LEVEL_AS_GROUP—Max privilege taken from group setting. • ENABLE_LEVEL_NONE—No T+ enable configured. • ENABLE_LEVEL_STATIC—Value set in V2 used during enable level check. <p>You can use VN to link the enable password to an external authenticator, as per action 108 SET_PASS_TYPE.</p>
106	SET_GROUP	UN, GN	Sets the ACS group assignment of the user.
108	SET_PASS_TYPE	UNIGN, V1	<p>Sets the password type of the user. This can be one of the ACS internal database password types or any of the external databases supported:</p> <ul style="list-style-type: none"> • PASS_TYPE_CSDB—CSDB internal password. • PASS_TYPE_CSDB_UNIX—CSDB internal password (UNIX encrypted). • PASS_TYPE_NT—External Windows user database password. • PASS_TYPE_NDS—External Novell database password. • PASS_TYPE_LDAP—External generic LDAP database password. • PASS_TYPE_LEAP—External LEAP proxy RADIUS server database password. • PASS_TYPE_RADIUS_TOKEN—External RADIUS token server database password.

Table F-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
109	REMOVE_PASS_STATUS	UN,V1	Removes a password status flag. This action results in the status states being linked in a logical XOR condition. V1 should contain one of the following: <ul style="list-style-type: none"> PASS_STATUS_EXPIRES—Password expires on a given date. PASS_STATUS_NEVER—Password never expires. PASS_STATUS_WRONG—Password expires after a given number of login attempts using the wrong password. PASS_STATUS_DISABLED—The account has been disabled.
110	ADD_PASS_STATUS	UN, V1	Defines how a password should be expired by ACS. To set multiple password states for a user, use multiple instances of this action. This action results in the status states being linked in a logical XOR condition. V1 should contain one of the following: <ul style="list-style-type: none"> PASS_STATUS_EXPIRES—Password expires on a given date. PASS_STATUS_NEVER—Password never expires. PASS_STATUS_WRONG—Password expires after a given number of login attempts by using the wrong password. PASS_STATUS_RIGHT—Password expires after a given number of login attempts by using the correct password. PASS_STATUS_DISABLED—The account has been disabled.
112	SET_PASS_EXPIRY_WRONG	UN,V1	Sets the maximum number of bad authentications allowed (automatic reset on good password if not exceeded) and resets the current count.
113	SET_PASS_EXPIRY_DATE	UN,V1	Sets the date on which the account expires. The date format should be YYYYMMDD.
114	SET_MAX_SESSIONS	UNIGN, V1	Sets the maximum number of simultaneous sessions for a user or group. V1 should contain one of the following values: <ul style="list-style-type: none"> MAX_SESSIONS_UNLIMITED MAX_SESSIONS_AS_GROUP 1-65534
115	SET_MAX_SESSIONS_GROUP_USER	GN,V1	Sets the max sessions for a user of the group to one of the following values: <ul style="list-style-type: none"> MAX_SESSIONS_UNLIMITED 1-65534

Table F-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
260	SET_QUOTA	VN,V1, V2	<p>Sets a quota for a user or group.</p> <p>VN defines the quota type. Valid values are:</p> <ul style="list-style-type: none"> online time—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2. sessions—The quota limits the user or group by the number of sessions on the network for the period defined in V2. <p>V1 defines the quota. If VN is set to sessions, V1 is the maximum number of sessions in the period defined in V2. If VN is set to online time, V1 is the maximum number of seconds.</p> <p>V2 holds the period for the quota. Valid values are:</p> <ul style="list-style-type: none"> QUOTA_PERIOD_DAILY—The quota is enforced in 24-hour cycles, from 12:01 A.M. to midnight. QUOTA_PERIOD_WEEKLY—The quota is enforced in 7-day cycles, from 12:01 A.M. Sunday until midnight Saturday. QUOTA_PERIOD_MONTHLY—The quota is enforced in monthly cycles, from 12:01 A.M. on the first of the month until midnight on the last day of the month. QUOTA_PERIOD_ABSOLUTE—The quota is enforced in an ongoing basis, without an end.
261	DISABLE_QUOTA	UNIGN, VN	<p>Disables a group or user usage quota.</p> <p>VN defines the quota type. Valid values are:</p> <ul style="list-style-type: none"> online time—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2. sessions—The quota limits the user or group by the number of sessions on the network for the period defined in V2.
262	RESET_COUNTERS	UNIGN	Resets usage quota counters for a user or group.
263	SET_QUOTA_APPLY_TYPE	V1	<p>Defines whether a user usage quota is determined by the user group quota or by a quota unique to the user. V1 makes this specification. Valid values for V1 are:</p> <ul style="list-style-type: none"> ASSIGNMENT_FROM_USER ASSIGNMENT_FROM_GROUP

Table F-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
270	SET_DCS_TYPE	UNIGN, VN, V1, Optional-ly V2	<p>Sets the type of device command set (DCS) authorization for a group or user.</p> <p>VN defines the service. Valid service types are:</p> <ul style="list-style-type: none"> • shell—Cisco IOS shell command authorization. • pixshell—Cisco PIX command authorization. <p>Note If additional DCS types have been added to your ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as: PIX Shell (pixshell)</p> <p>V1 defines the assignment type. The valid values for VN are:</p> <ul style="list-style-type: none"> • none—Sets no DCS for the user or group. • as group—For users only, this value signifies that the user DCS settings for the service specified should be the same as the user group DCS settings. • static—Sets a DCS for the user or group for all devices enabled to perform command authorization for the service specified. <p>If V1 is set to static, V2 is required and must contain the name of the DCS to assign to the user or group for the given service.</p> <ul style="list-style-type: none"> • ndg—Specifies that command authorization for the user or group is to be done on a per-NDG basis. Use action 271 to add DCS to NDG mappings for the user or group. <p>Note Changing a user or group assignment type (V1) results in clearing previous data, including NDG to DCS mappings (defined by action 271).</p>

Table F-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
271	SET_DCS_NDG_MAP	UNIGN, VN, V1, V2	<p>Use this action code to map between the device command set and the NDG when the assignment type specified by a 270 action code is <code>ndg</code>.</p> <p>VN defines the service. Valid service types are:</p> <ul style="list-style-type: none"> shell—Cisco IOS shell command authorization. pixshell—Cisco PIX command authorization. <p>Note If additional DCS types have been added to your ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as: PIX Shell (pixshell)</p> <p>V1 defines the name of the NDG. Use the name of the NDG as it appears in the web interface. For example, if you have configured an NDG named <i>East Coast NASs</i> and want to use action 271 to apply a DCS to that NDG, V1 should be <i>East Coast NASs</i>.</p> <p>V2 defines the name of the DCS. Use the name of the DCS as it appears in the web interface. For example, if you have configured a DCS named <i>Tier2 PIX Admin DCS</i> and want to use action 271 to apply it to an NDG, V2 should be <i>Tier2 PIX Admin DCS</i>.</p>

Action Codes for Initializing and Modifying Access Filters

Table F-4 lists the action codes for initializing and modifying AAA client access filters. AAA client access filters control Telnet access to a AAA client. Dial access filters control access by dial-up users.

Transactions using these codes affect the configuration that appears in the User Setup and Group Setup sections of the web interface. For more information about the User Setup section, see [Chapter 7, “User Management.”](#) For more information about the Group Setup section, see [Chapter 6, “User Group Management.”](#)

Table F-4 Action Codes for Initializing and Modifying Access Filters

Action Code	Name	Required	Description
120	INIT_NAS_ACCESS_CONTROL	UNIGN, V1	Clears the AAA client access filter list and initialize permit or deny for any forthcoming filters. V1 should be one of the following values: <ul style="list-style-type: none"> ACCESS_PERMIT ACCESS_DENY
121	INIT_DIAL_ACCESS_CONTROL	UNIGN, V1	Clears the dial-up access filter list and initialize permit/deny for any forthcoming filters. V1 should be one of the following values: <ul style="list-style-type: none"> ACCESS_PERMIT ACCESS_DENY
122	ADD_NAS_ACCESS_FILTER	UNIGN, V1	Adds a AAA client filter for the user/group. V1 should contain a single (AAA client name, AAA client port, remote address, CLID) tuple; for example: NAS01, tty0, 0898-69696969 Optionally, the AAA client name can be <i>All AAA clients</i> to specify that the filter applies to all configured AAA clients and an asterisk (*) to represent all ports.
123	ADD_DIAL_ACCESS_FILTER	UNIGN, V1, V2	Adds a dial-up filter for the user/group. V1 should contain one of the following values: <ul style="list-style-type: none"> Calling station ID Called station ID Calling and called station ID; for example: 01732-875374, 0898-69696969 NAS IP address, NAS port; for example: 10.45.6.123, tty0 V2 should contain the filter type as one of the following values: <ul style="list-style-type: none"> CLID—The user is filtered by the calling station ID. DNIS—The user is filtered by the called station ID. CLID/DNIS—The user is filtered by calling and called station IDs. NAS/PORT—The user is filtered by NAS IP and NAS port address.
130	SET_TOKEN_CACHE_SESSION	GN, V1	Enables or disables token caching for an entire session; V1 is 0=disable, 1=enable.
131	SET_TOKEN_CACHE_TIME	GN, V1	Sets the duration that tokens are cached. V1 is the token cache duration in seconds.

Table F-4 Action Codes for Initializing and Modifying Access Filters (continued)

Action Code	Name	Required	Description
140	SET_TODDOW_ACCESS	UNIGN, V1	Sets periods during which access is permitted. V1 contains a string of 168 characters. Each character represents a single hour of the week. A 1 represents an hour that is permitted, while a 0 represents an hour that is denied. If this parameter is not specified for a user, the group setting applies. The default group setting is 111111111111 and so on.
150	SET_STATIC_IP	UN, V1, V2	<p>Configures the (TACACS+ and RADIUS) IP address assignment for this user.</p> <p>V1 holds the IP address in the following format: xxx.xxx.xxx.xxx</p> <p>V2 should be one of the following:</p> <ul style="list-style-type: none"> • ALLOC_METHOD_STATIC—The IP address in V1 is assigned to the user in the format xxx.xxx.xxx.xxx. • ALLOC_METHOD_NAS_POOL—The IP pool named in V1 (configured on the AAA client) will be assigned to the user. • ALLOC_METHOD_AAA_POOL—The IP pool named in V1 (configured on the AAA server) will be assigned to the user. • ALLOC_METHOD_CLIENT—The dial-in client will assign its own IP address. • ALLOC_METHOD_AS_GROUP—The IP address assignment configured for the group will be used.
151	SET_CALLBACK_NO	UNIGN, V1	<p>Sets the callback number for this user or group (TACACS+ and RADIUS). V1 should be one of the following:</p> <ul style="list-style-type: none"> • Callback number—The phone number the AAA client is to call back. • none—No callback is allowed. • roaming—The dial-up client determines the callback number. • as group—Use the callback string or method defined by the group.

Action Codes for Modifying TACACS+ and RADIUS Group and User Settings

Table F-5 lists the action codes for creating, modifying, and deleting TACACS+ and RADIUS settings for ACS groups and users. In the event that ACS has conflicting user and group settings, user settings always override group settings.

Transactions using these codes affect the configuration displayed in the User Setup and Group Setup sections of the web interface. For more information about the User Setup section, see [Chapter 7, “User Management.”](#) For more information about the Group Setup section, see [Chapter 6, “User Group Management.”](#)

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings

Action Code	Name	Required	Description
161	DEL_RADIUS_ATTR	UNIGN, VN, Optionally V2, V3	<p>Deletes the named RADIUS attribute for the group or user, where:</p> <ul style="list-style-type: none"> • VN = “Vendor-Specific” • V2 = IETF vendor ID • V3 = VSA attribute ID <p>For example, to specify the Cisco IOS/PIX vendor ID and the Cisco AV Pair:</p> <pre>VN = "Vendor-Specific" V2 = "9" V3 = "1"</pre>

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
163	ADD_RADIUS_ATTR	UNIGN, VN, V1, Optionally V2, V3	<p>Adds to the attribute named (VN) the value (V1) for the user/group (UNIGN). For example, to set the IETF RADIUS Reply-Message attribute (attr. 18) for a group:</p> <pre>GN = "Group 1" VN = "Reply-Message" V1 = "Greetings"</pre> <p>As another example, to set the IETF RADIUS Framed-IP-Address attribute (attr. 9) for a user:</p> <pre>UN = "fred" VN = "Framed-IP-Address" V1 = "10.1.1.1"</pre> <p>To add a vendor-specific attribute (VSA), set VN = "Vendor-Specific" and use V2 and V3 as follows:</p> <ul style="list-style-type: none"> • V2 = IETF vendor ID • V3 = VSA attribute ID <p>For example, to add the Cisco IOS/PIX RADIUS cisco-av-pair attribute with a value of "addr-pool=pool1":</p> <pre>VN="Vendor-Specific" V1 = "addr-pool=pool1" V2 = "9" V3 = "1"</pre> <p>RADIUS attribute values can be one of the following:</p> <ul style="list-style-type: none"> • INTEGER • TIME • IP ADDRESS • STRING
170	ADD_TACACS_SERVICE	UNIGN, VN, V1, V3, Optionally V2	<p>Permits the service for that user or group of users. For example:</p> <pre>GN = "Group 1" V1 = "ppp" V2 = "ip"</pre> <p>or</p> <pre>UN = "fred" V1 = "ppp" V2 = "ip"</pre> <p>or</p> <pre>UN = "fred" V1 = "exec"</pre>

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
171	REMOVE_TACACS_SERVICE	UNIGN, V1 Optionally V2	Denies the service for that user or group of users. For example: GN = "Group 1" V1 = "ppp" V2 = "ip" or UN = "fred" V1 = "ppp" V2 = "ip" or UN = "fred" V1 = "exec" This also resets the valid attributes for the service.
172	ADD_TACACS_ATTR	UNIGN, VN, V1, V3 Optionally V2	Sets a service-specific attribute. The service must already have been permitted via the web interface or using Action 170: GN = "Group 1" VN = "routing" V1 = "ppp" V2 = "ip" V3 = "true" or UN = "fred" VN = "route" V1 = "ppp" V2 = "ip" V3 = 10.2.2.2
173	REMOVE_TACACS_ATTR	UNIGN, VN, V1 Optionally V2	Removes a service-specific attribute: GN = "Group 1" V1 = "ppp" V2 = "ip" VN = "routing" or UN = "fred" V1 = "ppp" V2 = "ip" VN = "route"

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
174	ADD_IOS_COMMAND	UNIGN, VN, V1	<p>Authorizes the given Cisco IOS command and determines if any arguments given to the command are to be found in a defined set or are not to be found in a defined set. The defined set is created using Actions 176 and 177:</p> <p>GN = "Group 1" VN = "telnet" V1 = "permit"</p> <p>or</p> <p>UN = "fred" VN = "configure" V1 = "deny"</p> <p>The first example permits the Telnet command to be authorized for users of Group 1. Any arguments can be supplied to the Telnet command as long as they are not matched against any arguments defined via Action 176.</p> <p>The second example permits the configure command to be authorized for user <i>fred</i>, but only if the arguments supplied are permitted by the filter defined by a series of Action 176.</p>
175	REMOVE_IOS_COMMAND	UNIGN, VN	<p>Removes command authorization for the user or group:</p> <p>GN = "Group 1" VN = "telnet"</p> <p>or</p> <p>UN = "fred" VN = "configure"</p> <p>Users of Group 1 can no longer use the Cisco IOS telnet command.</p> <p>User fred can no longer use the configure command.</p>

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
176	ADD_IOS_COMMAND_ARG	UNIGN, VN, V1, V2	<p>Specifies a set of command-line arguments that are permitted or denied for the Cisco IOS command contained in VN. The command must have already been added via Action 174:</p> <pre>GN = "Group 1" VN = "telnet" V1 = "permit" V2 = "10.1.1.2"</pre> <p>or</p> <pre>UN = "fred" VN = "show" V1 = "deny" V2 = "run"</pre> <p>The first example will allow the telnet command with argument 10.1.1.2 to be used by any user in Group 1.</p> <p>The second example ensures that user fred cannot issue the Cisco IOS command show run.</p>
177	REMOVE_IOS_COMMAND_ARG	UNIGN, VN, V2	<p>Removes the permit or deny entry for the given Cisco IOS command argument:</p> <pre>GN = "Group 1" VN = "telnet" V2 = "10.1.1.1"</pre> <p>or</p> <pre>UN = "fred" VN = "show" V2 = "run"</pre>
178	SET_PERMIT_DENY_UNMATCHED_IOS_COMMANDS	UNIGN, V1	<p>Sets unmatched Cisco IOS command behavior. The default is that any Cisco IOS commands not defined via a combination of Actions 174 and 175 will be denied. This behavior can be changed so that issued Cisco IOS commands that do not match any command/command argument pairs are authorized:</p> <pre>GN = "Group 1" V1 = "permit"</pre> <p>or</p> <pre>UN = "fred" V1 = "deny"</pre> <p>The first example will permit any command not defined by Action 174.</p>
179	REMOVE_ALL_IOS_COMMANDS	UNIGN	This action removes all Cisco IOS commands defined for a particular user or group.
210	RENAME_GROUP	GN, V1	Renames an existing group to the name supplied in V1.

Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
211	RESET_GROUP	GN	Resets a group back to the factory default.
212	SET_VOIP	GN, V1	Enables or disables Voice over IP (VoIP) support for the group named: <ul style="list-style-type: none"> • GN = name of group • V1 = ENABLE or DISABLE

Action Codes for Modifying Network Configuration

[Table F-6](#) lists the action codes for adding AAA clients, AAA servers, network device groups, and proxy table entries. Transactions using these codes affect the configuration that appears in the Network Configuration section of the web interface. For more information about the Network Configuration section, see [Chapter 4, “Network Configuration.”](#)

Table F-6 Action Codes for Modifying Network Configuration

Action Code	Name	Required	Description
220	ADD_NAS	VN, V1, V2, V3	<p>Adds a new AAA client (named in VN) with an IP address (V1), shared secret key (V2), and vendor (V3). Valid vendors are:</p> <ul style="list-style-type: none"> • VENDOR_ID_IETF_RADIUS—For IETF RADIUS. • VENDOR_ID_CISCO_RADIUS—For Cisco IOS/PIX RADIUS. • VENDOR_ID_CISCO_TACACS—For Cisco TACACS+. • VENDOR_ID_AIRSPACE_RADIUS —For Cisco Airespace RADIUS. • VENDOR_ID_ASCEND_RADIUS—For Ascend RADIUS. • VENDOR_ID_ALTIGA_RADIUS—For Cisco 3000/ASA/PIX 7.x+ RADIUS. • VENDOR_ID_AIRONET_RADIUS—For Cisco Aironet RADIUS. • VENDOR_ID_NORTEL_RADIUS—For Nortel RADIUS. • VENDOR_ID_JUNIPER_RADIUS—For Juniper RADIUS. • VENDOR_ID_CBBMS_RADIUS—For Cisco BBMS RADIUS. <p>For example:</p> <pre>VN = AS5200-11 V1 = 192.168.1.11 V2 = byZantine32 V3 = VENDOR_ID_CISCO_RADIUS</pre>
221	SET_NAS_FLAG	VN, V1	<p>Sets one of the per-AAA client flags (V1) for the named AAA client (VN). Use the action once for each flag required. Valid values for per-AAA client flags are:</p> <ul style="list-style-type: none"> • FLAG_SINGLE_CONNECT • FLAG_LOG_KEEP_ALIVE • FLAG_LOG_TUNNELS
222	DEL_HOST	VN	Deletes the named AAA client (VN).
223	ADD_NAS_BY_IETF_CODE	VN, V1, V2, V3	Adds a new AAA client (named in VN) with an IP address (V1), shared secret key (V2), and the enterprise code for the vendor (V3).
230	ADD_AAA_SERVER	VN, V1, V2	Adds a new AAA server named (VN) with IP address (V1), shared secret key (V2).

Table F-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
231	SET_AAA_TYPE	VN, V1	Sets the AAA server type for server (VN) to value in V1, which should be one of the following: <ul style="list-style-type: none"> TYPE_ACS TYPE_TACACS TYPE_RADIUS The default is AAA_SERVER_TYPE_ACS.
232	SET_AAA_FLAG	VN, V1	Sets one of the per-AAA client flags (V1) for the named AAA server (VN): <ul style="list-style-type: none"> FLAG_LOG_KEEP_ALIVE FLAG_LOG_TUNNELS Use the action once for each flag required.
233	SET_AAA_TRAFFIC_TYPE	VN, V1	Sets the appropriate traffic type (V1) for the named AAA server (VN): <ul style="list-style-type: none"> TRAFFIC_TYPE_INBOUND TRAFFIC_TYPE_OUTBOUND TRAFFIC_TYPE_BOTH The default is TRAFFIC_TYPE_BOTH.
234	DEL_AAA_SERVER	VN	Deletes the named AAA server (VN).
240	ADD_PROXY	VN, V1, V2, V3	Adds a new proxy markup (VN) with markup type (V1) strip markup flag (V2) and accounting flag (V3). <p>The markup type (V1) must be one of the following:</p> <ul style="list-style-type: none"> MARKUP_TYPE_PREFIX MARKUP_TYPE_SUFFIX <p>The markup strip flag should be TRUE if the markup is to be removed from the username before forwarding.</p> <p>The accounting flag (V3) should be one of the following:</p> <ul style="list-style-type: none"> ACCT_FLAG_LOCAL ACCT_FLAG_REMOTE ACCT_FLAG_BOTH
241	ADD_PROXY_TARGET	VN, V1	Adds to named proxy markup (VN) the host name (V1). The host should already be configured in ACS. <p>Note The order in which proxy targets are added sets the proxy search order; the first target added is the first target proxied to, and so on. The order must be changed through the web interface.</p>
242	DEL_PROXY	VN	Deletes the named proxy markup (VN).
250	ADD_NDG	VN	Creates a network device group (NDG) named (VN).

Table F-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
251	DEL_NDG	VN	Deletes the named NDG.
252	ADD_HOST_TO_NDG	VN, V1	Adds to the named AAA client/AAA server (VN) the NDG (V1).
270	SET_DCS_ASSIGNMENT	—	—
271	ADD_NDG_TO_DCS_MAPPING	—	—
300	RESTART_PROTO_MODULES	—	Restarts the CSRadius and CSTacacs services to apply new settings.
350	ADD_UDV	VN, V1, V2	<p>Adds a RADIUS vendor to the ACS vendor database. Vendors added to ACS by this method are known as User-Defined Vendors (UDV).</p> <p>VN contains the name of the Vendor.</p> <p>Note ACS adds <i>RADIUS(...)</i> to the name entered in the Variable Name field. For example, if you enter the name <i>MyCo</i>, ACS displays <i>RADIUS (MyCo)</i> in the web interface.</p> <p>V1 contains the user-defined vendor slot number or AUTO_ASSIGN_SLOT. ACS has ten vendor slots, numbered 0 through 9. If you specify AUTO_ASSIGN_SLOT, ACS selects the next available slot for your vendor.</p> <p>Note If you want to replicate UDVs between ACSs, you must assign the UDV to the same slot number on both ACSs.</p> <p>V2 contains the IANA-assigned enterprise code for the vendor.</p>
351	DEL_UDV	V1	<p>Removes the vendor with the IETF code specified in V1 and any defined VSAs.</p> <p>Note Action code 351 does not remove any instances of VSAs assigned to ACS groups or users. If ACS has AAA clients configured with the UDV specified in V1, the delete operation fails.</p>

Table F-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
352	ADD_VSA	VN, V1, V2, V3	<p>Adds a new VSA to the vendor specified by the vendor IETF code in V1.</p> <p>VN is the VSA name. If the vendor name is <i>MyCo</i> and the attribute is assigned a group ID, we recommend prefixing the vendor name or an abbreviation to all VSAs. For example, VSAs could be <i>MyCo-Assigned-Group-Id</i>.</p> <p>Note VSA names must be unique to the vendor and to the ACS dictionary. For example, <i>MyCo-Framed-IP-Address</i> is allowed but <i>Framed-IP-Address</i> is not, because <i>Framed-IP-Address</i> is used by IETF action code 8 in the RADIUS attributes.</p> <p>V2 is the VSA number. This must be in the 0-255 range.</p> <p>V3 is the VSA type as one of following values:</p> <ul style="list-style-type: none"> • INTEGER • STRING • IPADDR <p>By default, VSAs are assumed to be outbound (or authorization) attributes. If the VSA is either multi-instance or used in accounting messages, use SET_VSA_PROFILE (Action code 353).</p>
353	SET_VSA_PROFILE	V1, V2, V3	<p>Sets the inbound/outbound profile of the VSA. The profile specifies usage IN for accounting, OUT for authorization, or MULTI if more than a single instance is allowed per RADIUS message. Combinations are allowed.</p> <p>V1 contains the vendor IETF code.</p> <p>V2 contains the VSA number.</p> <p>V3 contains the profile, one of the following:</p> <p>IN OUT IN OUT MULTI OUT MULTI IN OUT</p>

Table F-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
354	ADD_VSA_ENUM	VN, V1, V2, V3	<p>Sets meaningful enumerated values, if the VSA attribute has enumerated. In the User Setup section, the ACS web interface displays the enumeration strings in a list.</p> <p>VN contains the VSA Enum Name.</p> <p>V1 contains the vendor IETF code.</p> <p>V2 contains the VSA number.</p> <p>V3 contains the VSA Enum Value.</p> <p>Example:</p> <pre>VN = Disabled V1 = 9034 V2 = MyCo-Encryption V3 = 0</pre> <p>or</p> <pre>VN = Enabled V1 = 9034 V2 = MyCo-Encryption V3 = 1</pre>
355	ADOPT_NEW_UDV_OR_VSA	—	Restarts the CSAdmin, CSRADIUS, and CSLog services. These services must be restarted before new UDVs or VSAs can become usable.

ACS Attributes and Action Codes

This section complements the previous section by providing an inverse reference; it provides topics with tables that list ACS attributes, their data types and limits, and the action codes you can use to act upon the ACS attributes.

This section contains the following topics:

- [User-Specific Attributes, page F-22](#)
- [User-Defined Attributes, page F-24](#)
- [Group-Specific Attributes, page F-24](#)

User-Specific Attributes

[Table F-7](#) lists the attributes that define an ACS user, including their data types, limits, and default values. It also provides the action code you can use in accountActions to affect each attribute. Although there are many actions available, adding a user requires only one transaction: ADD_USER. You can safely leave other user attributes at their default values. The term NULL is not simply an empty string, but means not set; that is, the value will not be processed. Some features are processed only if they have a value assigned to them. For more information about action codes, see [Action Codes, page F-3](#).

Table F-7 *User-Specific Attributes*

Attribute	Actions	Logical Type	Limits	Default
Username	100, 101	String	1-64 characters	—
ASCII/PAP Password	100, 102	String	4-32 characters	Random string
CHAP Password	103	String	4-32 characters	Random string
Outbound CHAP Password	104	String	4-32 characters	NULL
TACACS+ Enable Password	105	String Password	4-32 characters	NULL
		Integer privilege level	0-15 characters	NULL
Group	106	String	0-100 characters	Default Group
Password Supplier	107	Enum	See Table F-3 .	LIBRARY_CSDB
Password Type	108	Enum	See Table F-3 .	PASS_TYPE_CSDB (password is cleartext PAP)
Password Expiry Status	109, 110	Bitwise Enum	See Table F-3 .	PASS_STATUS_NEVER (never expires)
Expiry Data	112, 113	Short wrong max/current	0-32,767	—
		Expiry date	—	—
Max Sessions	114	Unsigned short	0-65535	MAX_SESSIONS_AS_GROUP
TODDOW Restrictions	140	String	168 characters	111111111111
NAS Access Control	120, 122	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	
		ACL String (See Table F-4 .)	0-31 KB	
Dial-Up Access Control	121, 123	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	NULL
		ACL String (See Table F-4 .)	0-31 KB	NULL
Static IP Address	150	Enum scheme	(See Table F-4 .)	Client
		String IP/Pool name	0-31 KB	NULL
Callback Number	151	String	0-31 KB	NULL
TACACS Attributes	160, 162	Formatted String	0-31 KB	NULL
RADIUS Attributes	170, 173	Formatted String	0-31 KB	NULL
UDF 1	1, 2	String Real Name	0-31 KB	NULL
UDF 2	1, 2	String Description	0-31 KB	NULL
UDF 3	1, 2	String	0-31 KB	NULL

Table F-7 User-Specific Attributes (continued)

Attribute	Actions	Logical Type	Limits	Default
UDF 4	1, 2	String	0-31 KB	NULL
UDF 5	1, 2	String	0-31 KB	NULL

User-Defined Attributes

User-defined attributes (UDAs) are string values that can contain any data, such as social security number, department name, telephone number, and so on. You can configure ACS to include UDAs on accounting logs about user activity. For more information about configuring UDAs, see [User Data Configuration Options, page 3-4](#).

RDBMS Synchronization can set UDAs by using the SET_VALUE action (code 1) to create a value called USER_DEFINED_FIELD_0 or USER_DEFINED_FIELD_1. For accountActions rows defining a UDA value, the AppId (AI) field must contain APP_CSAUTH and the Value2(V2) field must contain TYPE_STRING.

Table F-8 lists the data fields that define UDAs. For more information about action codes, see [Action Codes, page F-3](#).

Table F-8 User-Defined Attributes

Action	Username (UN)	ValueName (VN)	Value1 (V1)	Value2 (V2)	AppId (AI)
1	fred	USER_DEFINED_FIELD_0	SS123456789	TYPE_STRING	APP_CSAUTH
1	fred	USER_DEFINED_FIELD_1	Engineering	TYPE_STRING	APP_CSAUTH
1	fred	USER_DEFINED_FIELD_2	949-555-1111	TYPE_STRING	APP_CSAUTH



Note

If more than two UDAs are created, only the first two are passed to accounting logs.

Group-Specific Attributes

Table F-9 lists the attributes that define an ACS group, including their data types, limits, and default values. It also provides the action code that you can use in your accountActions table to affect each field. For more information about action codes, see [Action Codes, page F-3](#).

Table F-9 Group-Specific Attributes

Attribute	Actions	Logical Type	Limits	Default
Max Sessions	114	Unsigned short	0-65534	MAX_SESSIONS_UNLIMITED
Max Sessions for user of group	115	Unsigned short	0-65534	MAX_SESSIONS_UNLIMITED
Token caching for session	130	Bool	T/F	NULL
Token caching for duration	131	Integer time in seconds	0-65535	NULL

Table F-9 Group-Specific Attributes (continued)

Attribute	Actions	Logical Type	Limits	Default
TODDOW Restrictions	140	String	168 characters	111111111111
NAS Access Control	120, 122	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	
		ACL String (See Table F-4.)	0-31 KB	
Dial-Up Access Control	121, 123	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	NULL
		ACL String (See Table F-4.)	0-31 KB	NULL
Static IP Address	150	Enum scheme	(See Table F-4.)	Client
		String IP/Pool name	0-31 KB	NULL
TACACS Attributes	160, 162	Formatted String	0-31 KB	NULL
RADIUS Attributes	170, 173	Formatted String	0-31 KB	NULL
VoIP Support	212	Bool disabled	T/F	NULL

An Example of accountActions

Table F-10 presents an sample instance of accountActions that contains some of the action codes described in Action Codes, page F-3. First user *fred* is created, along with his passwords, including a TACACS_ Enable password with privilege level 10. Fred is assigned to *Group 2*. His account expires after December 31, 1999, or after 10 incorrect authentication attempts. Attributes for Group 2 include Time-of-Day/Day-of-Week restrictions, token caching, and some RADIUS attributes.



Note

This example omits several columns that should appear in any accountActions table. The omitted columns are Sequence ID (SI), Priority (P), DateTime (DT), and MessageNo (MN).

Table F-10 Example accountActions Table

Action	User name (UN)	Group Name (GN)	Value Name (VN)	Value1 (V1)	Value2 (V2)	Value3 (V3)	AppId (AI)
100	fred	—	—	fred	—	—	—
102	fred	—	—	freds_password	—	—	—
103	fred	—	—	freds_chap_password	—	—	—
104	fred	—	—	freds_outbound_password	—	—	—
105	fred	—	—	freds_enable_password	10	—	—
106	fred	Group 2	—	—	—	—	—
150	fred	—	—	123.123.123.123	—	—	—

Table F-10 Example accountActions Table (continued)

Action	User name (UN)	Group Name (GN)	Value Name (VN)	Value1 (V1)	Value2 (V2)	Value3 (V3)	Appld (AI)
151	fred	—	—	01832-123900	—	—	—
109	fred	—	—	PASS_STATUS_NEVER	—	—	—
110	fred	—	—	PASS_STATUS_WRONG	—	—	—
110	fred	—	—	PASS_STATUS_EXPIRES	—	—	—
112	fred	—	—	10	—	—	—
113	fred	—	—	19991231	—	—	—
114	fred	—	—	50	—	—	—
115	fred	—	—	50	—	—	—
120	fred	—	—	ACCESS_PERMIT	—	—	—
121	fred	—	—	ACCESS_DENY	—	—	—
122	fred	—	—	NAS01,tty0,01732-975374	—	—	—
123	fred	—	—	01732-975374,01622-123123	CLID/ DNIS	—	—
1	fred	—	USER_DEFINED_FIELD_0	Fred Jones	TYPE_STRING	—	APP_CSAUTH
140	—	Group 2	—	[a string of 168 ones (1)]	—	—	—
130	—	Group 2	—	DISABLE	—	—	—
131	—	Group 2	—	61	—	—	—
163	—	Group 2	Reply-Message	Welcome to Your Internet Service	—	—	—
163	—	Group 2	Vendor-Specific	addr-pool=pool2	9	1	—