Monitoring AAA Configurations

AAA refers to Authentication, Authorization, and Accounting, which is a security architecture for distributed systems that determines the access given to users for specific services and the amount of resources they have used.

- Authentication—This method identifies users, including their login and password, challenge and response, messaging support, and encryption. Authentication is the way to identify a subscriber before providing access to the network and network services.
- Authorization—This method provides access control, including authorization for a subscriber or domain profile. AAA authorization sends a set of attributes to the service describing the services that the user can access. These attributes determine the user's actual capabilities and restrictions.
- Accounting—This method collects and sends subscriber usage and access information used for billing, auditing, and reporting. For example, user identities, start and stop times, performed actions, number of packets, and number of bytes. Accounting enables an operator to analyze the services that the users access as well as the amount of network resources they consume. Accounting records comprise accounting Attribute Value Pairs (AVPs) and are stored on the accounting server. This accounting information can then be analyzed for network management, client billing, and/or auditing.

These topics describe how to use the Vision client to view and manage AAA configurations. If you cannot perform an operation that is described in these topics, you may not have sufficient permissions; see Permissions for Managing AAA, page B-20.

Supported AAA Network Protocols

AAA supports the following protocols:

- Diameter—This is a networking protocol that provides centralized AAA management for devices to connect and use a network service, and an alternative to RADIUS. Diameter Applications can extend the base protocol, by adding new commands and/or attributes.
- Remote Authentication Dial In User Service (RADIUS)—This is a networking protocol that provides centralized AAA management for devices to connect and use a network service. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote

Access Server (RAS), the Virtual Private Network (VPN) server, the network switch with port-based authentication, and the Network Access Server (NAS), are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server.

- Terminal Access Controller Access Control System (TACACS) is an authentication program used on Unix and Linux based systems, along with certain network routers. TACACS allows a remote access server to communicate with an authentication server to determine whether or not a user has the proper rights to access a network or database. TACACS forwards username and password information to a centralized security server.
- TACACS+ is a networking protocol that provides centralized AAA management for devices to connect and use a network service. Derived from TACACS, TACACS+ provides for separate and modular AAA facilities and uses TCP as transport.

Viewing AAA Configurations

This topic contains the following sections:

For information on the devices that support AAA, refer to *Cisco Prime Network 5.0 Supported VNEs*.

Viewing AAA Group Profile

To view the AAA group profile:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA**. The AAA attribute details are displayed in the content pane. (The attributes that are displayed depend on the device type.)

Table 15-1 describes the fields that are displayed in the content pane.

Table 15-1 AAA Attributes

Field Name	Description
Type	Customization applied to the attribute.
Key	Unique format name applied to the attribute.
Value	Formatting applied to the attribute.

Step 3 In the **Inventory** window, choose **AAA group** node under the AAA node. In the Content pane you can view the AAA method in the **Group Type** field. The group Type displayed are None, TACACS+, RADIUS, or DIAMETER for the existing device types.

Step 4 Under the **AAA group** node, select and expand the required group and choose the **Radius Configuration** option. The group details are displayed in the content pane.

Table 15-2 describes the fields that are displayed in the Radius Configuration dialog box.

Table 15-2 Radius Configuration Details

Field Name	Description
Load Balancing Method	The load balancing method.
Ignore Preferred Server	Indicates if a transaction associated with a single AAA session should attempt to use the same server or not.
Dead Time	The deadtime for the profile.

Viewing a Dynamic Authorization Profile

To view the dynamic authorization profile:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory > AAA > Dynamic Authorization**. The authorization details are displayed in the content pane. You can click on the tabs to view more details. (The attributes that are displayed depend on the device type.)

Table 15-3 describes the fields that are displayed in the Dynamic authorization content pane.

Table 15-3 Dynamic Authorization Details

Field Name	Description
Protocol	The name of the protocol.
Server Listen Port	The port number that receives service requests.
Ignore Server Key	Indicates whether the server key must be ignored. Values are: • true • false
CoA Clients Tab	
IP Address	The IP address of the Change of Authorization (CoA) client.
VRF	The associated VRF to which the CoA client belongs. Click the hyperlink to view the relevant node under the VRF node.

Viewing a Dynamic Dictionary

To view the dynamic dictionary:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **local** > **AAA** > AAA **Dynamic Dictionaries** > *Context*. The dynamic dictionary VID details are displayed in the content pane.

Table 15-4 describes the fields that are displayed in the Dynamic dictionary content pane.

Table 15-4 Dynamic Dictionary Details

Field Name	Description
Dynamic Dictionary Name	The name of the configured diameter dynamic dictionary.
Base Static Dictionary	The static dictionary number and name from which the dynamic dictionary is derived.
AAA Dynamic Dictionary VID Entries	
Vid	The vendor ID.

Viewing a Radius Global Configuration Details

To view the radius global configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA** > **Radius Global Configuration**. The authorization details are displayed in the content pane. (The attributes that are displayed depend on the device type.)

Table 15-5 describes the fields that are displayed in the Radius global configuration content pane.

Table 15-5 Radius Global Configuration Details

Field Name	Description
Load Balancing Method	The load balancing method using which the next host is selected. The server with the least transactions outstanding is generally picked as the next host.
Ignored Preferred Server	Indicates if a transaction associated with a single AAA session should attempt to use the same server or not.
Request Timeout	The request timeout value for the device.
Dead Time	The amount of time (in minutes) after which the dead RADIUS server will be treated as active.
Retransmit	Indicates whether retransmission of data is allowed.
Retransmit Count	The retransmission count.
Dead Criteria Time	The time interval after which the device is considered unavailable.
Dead Criteria Retransmit Count	The retransmission count after the dead criteria time.
Accounting Servers/ Authentication Servers	
Server IP	The IP address of the server.
Server Port	The server port.
Preference	The preferred server.
Operational State	The current operational state of the interface.
Administrative Status	The administrative status of the interface.
Retain Administrative Status After Reboot	Indicates whether the administrative status must be retained after the system reboots.
Keepalive Representative Group	The keepalive representative group.
Request Timeout	The request timeout value for the device.
Retransmit Count	The retransmission count.

Viewing TACACS+ Global Configuration Details

To view the TACACS+ global configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory > AAA > TACACS+ Global Configuration**. The configuration details are displayed in the content pane. (The attributes that are displayed depend on the device type.)

Table 15-6 describes the fields that are displayed in the TACACS+ global configuration content pane.

Table 15-6 TACACS+ Global Configuration Details

Field Name	Description
Source Interface	Specifies that the IP address of this specified interface is used for all outgoing TACACS+ packets.
VRF	The VRF for the specified source interface configuration.
Timeout	Specifies the time to wait for the TACACS+ server to reply in seconds.
IPv4 DSCP	Specifies the IPv4 Differentiated Services Code Point (DSCP) to be used in the outgoing IP headers.
IPv6 DSCP	Specifies the IPv6 Differentiated Services Code Point (DSCP) to be used in the outgoing IP headers.
Administration	Specifies if the handling of administrative messages by the TACACS+ daemon is enabled.
Allow Unknown Attribute	Specifies if unknown TACACS+ attributes are ignored instead of trying to parse them.
Packet Max Size	Specifies the maximum size of TACACS+ packets.
DNS Alias Lookup	Specifies if IP Domain Name System (DNS) alias lookup is enabled for TACACS+ servers.
Cache Expiry Time	Specifies the length of time, in hours, for a cache database profile entry to expire.
Cache Expiry Rule	Specifies how the expired cached database profile entries in this TACACS+ server group are to be used: • Enforce—Indicates not to use expired entries. • Failover—Indicates to use an expired entry if all other methods fail.
Cache Authentication Profile Name	The name of the cache authentication profile used in this TACACS+ server group.
Cache Authorization Profile Name	The name of the cache authentication profile used in this TACACS+ server group.
Directed Request	Specifies if only the username (and not the entire string) is sent to an AAA TACACS+ server.
Directed Request <Restricted>	Specifies that queries are restricted to directed request servers only.
Directed Request <No-Truncate>	Specifies '@hostname' is not truncated from the username.
Domain Stripping	
Right-to-Left	Specifies that the stripping configuration at the first delimiter found when parsing the full username from right to left will be applied.
Prefix Delimiter	Specifies that the prefix stripping is enabled and the specified character(s) are to be recognized as a prefix delimiter(s).
Suffix Delimiter	Specifies the character(s) that are to be recognized as a suffix delimiter.
Strip Suffix	Specifies the suffix to strip from the username.
VRF	Specifies the VRF that the domain stripping configuration is applicable to.

Viewing TACACS+ Servers Configuration Details

To view the TACACS+ Servers configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory > AAA > TACACS+ Servers**. The configuration details for each TACACS+ server are displayed in the content pane. (The attributes that are displayed depend on the device type.)

Table 15-7 describes the fields that are displayed in the TACACS+ Servers configuration content pane.

Table 15-7 TACACS+ Servers Configuration Details

Field Name	Description
Server Address	The IP address or host name of the TACACS+ server.
Port	The TCP port used to communicate with the TACACS+ server.
Server Name	The name of the TACACS+ server.
Status	Specifies the operational state of the interface with the TACACS+ server.
Visibility	Specifies whether a TACACS+ server is public or private within the scope of an AAA group server.
Timeout	Specifies the time to wait for the TACACS+ server to reply in seconds.
Single Connection	Specifies whether all requests to a TACACS+ server are multiplexed over a single TCP connection to server (for CiscoSecure).
Send NAT Address	Specifies whether a client's post NAT address is sent to the TACACS+ server.

Viewing AAA Group Configuration Details

For certain devices, the Vision client allows you to view the following configurations for an AAA group:

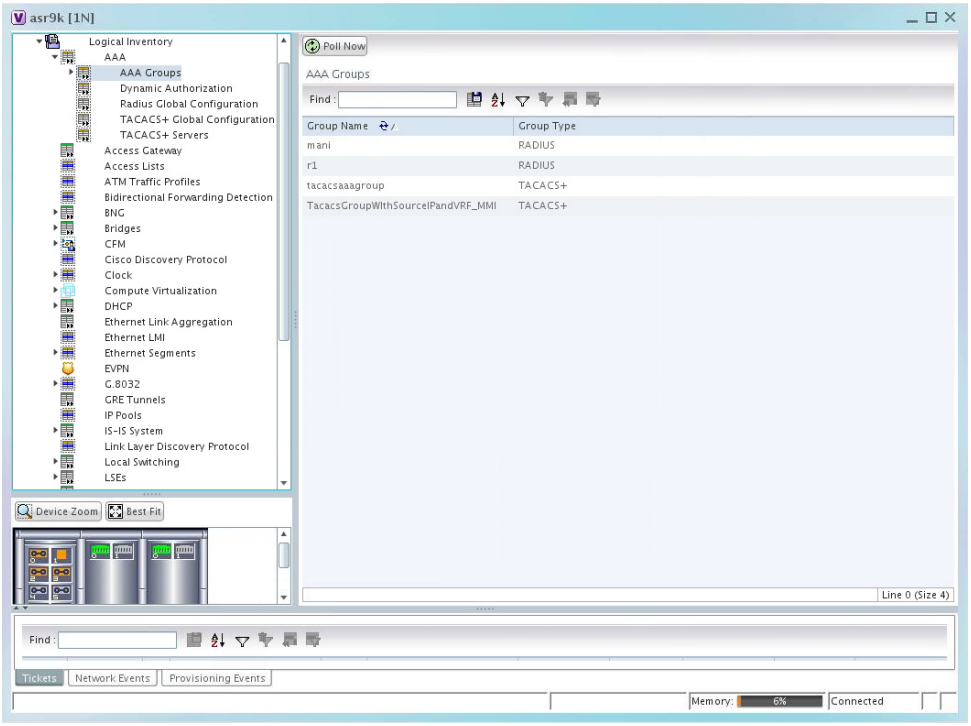
- Diameter Configuration
  - Accounting Configuration
  - Authentication Configuration
- Radius Configuration
  - Accounting Configuration
  - Accounting Keepalive and Detect Dead Server Configuration
  - Authentication Configuration
  - Authentication Keepalive and Detect Dead Server Configuration
  - Charging Configuration

  - Charging Triggers
- TACACS+ Configuration

(Refer to *Cisco Prime Network 5.0 Supported VNEs* for more information.)

The Vision client displays the AAA configuration details under the AAA container as shown in Figure 15-1. You can view the individual AAA group details by choosing **Logical Inventory** > *Context* > **AAA** > **AAA Groups**.

Figure 15-1 AAA Groups in Logical Inventory



Viewing Diameter Configuration Details for an AAA Group

To view the diameter configuration details for a AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Groups**.

You can view the AAA groups on the content pane.

Step 3 Choose **Diameter Configuration** under a specific AAA group node. The diameter configurations made for accounting servers and authentication servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 15-8 describes the diameter configuration details for accounting and authentication servers.

Table 15-8 Diameter Configuration

Field Name	Description
Accounting Servers/Authentication Servers	
Server Host	Host name of the diameter authentication/accounting server.
Priority	Relative priority of the diameter authentication/accounting server.
Number of Instances in Up State	Number of instances between the diameter authentication/accounting server and the AAA manager that are in UP status.
Number of Instances in Down State	Number of instances between the diameter authentication/accounting server and the AAA manager that are in DOWN status.

Step 4 In the **Inventory** window, choose **Accounting Configuration** or **Authentication Configuration** under the **Diameter Configuration** node. The configuration details are displayed on the content pane.

Table 15-9 describes the accounting/authentication diameter configuration details.

Table 15-9 Accounting/Authentication Diameter Configuration

Field Name	Description
Dictionary	Diameter dictionary used for accounting/authentication.
Endpoint Name	Diameter endpoint used for accounting/authentication.
Maximum Transmissions	Maximum number of transmission attempts for diameter accounting/authentication.
Maximum Retries	Number of retry attempts for diameter accounting/authentication requests.
Request Timeout	Diameter accounting/authentication request timeout period.
Redirect Host AVP	Indicates whether to use: • one returned AVP • the first returned AVP as the primary host and the second returned AVP as the secondary host. This field is applicable only for Authentication configuration.
Upgrade -dict-avps	Sets the release version to 3GPP Rel.8 for upgrading diameter accounting dictionary in the current AAA group.

Table 15-9 Accounting/Authentication Diameter Configuration

Field Name	Description
HD-mode	Sends records to the Diameter server. If all Diameter servers are down or unreachable, then periodically retries the diameter service.
HD-Policy	Associates a specific HD storage policy with a AAA group.
Supported Features	Disables the CLI command and does not send supported features AVP.
Active Start Trigger	Enables an R-P event when an active start trigger is received from the PCF and there is a parameter change.
Active Stop Trigger	Enables an R-P event when an active stop trigger is received from the PCF.
AirlinkUsage Counter Rollover	The AirlinkUsage RADIUS accounting policy for R-P.
Stop Start Trigger	Indicates that a stop or start RADIUS accounting pair is sent to the RADIUS server at the time of R-P event occurrence.
Active Handoff Trigger	Enables a single R-P event when an active PCF-to-PCF handoff occurs.
Trigger Policy	Designates to use a custom RADIUS accounting policy for R-P. You can specify parameters to form custom accounting policy. By default, all optional parameters are disabled
Handoff Policy	Specifies the behavior of generating accounting STOP when handoff occurs.
MIP HA Policy	The RADIUS accounting policy for Mobile IP HA calls.
TOD Values	
TOD Minutes/Hours	A time of day at which an R-P event should occur. **Note** Up to four time of day events are displayed,

Viewing Radius Configuration Details for an AAA Group

To view the radius configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration**. The configurations made for accounting, authentication, charging, and charging accounting servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 15-10 describes the radius configuration details for accounting, authentication, charging, and charging accounting servers.

Table 15-10 Radius Configuration

Field Name	Description
Dictionary	The radius dictionary.
Strip Domain	Indicates whether the domain must be stripped from the user name prior to authentication or accounting.
Authenticator Validation	Indicates whether the MD5 authentication of the user is enabled or disabled.
Allow Server Down Authentication	Indicates whether subscriber sessions are allowed when RADIUS authentication is unavailable.
Allow Server Down Accounting	Indicates whether subscriber sessions are allowed when RADIUS accounting is unavailable.
Accounting Servers/Authentication Servers/Charging Servers/Charging Accounting Servers	
Server Name	IP address of the RADIUS server.
Server Port	Port used to communicate with the RADIUS server.
Preference	Preference of the RADIUS server.
Operational State	Status of the RADIUS server.
Administrative Status	Administrative status of the RADIUS server.
Retain Administrative Status after Reboot	Indicates whether the administrative status must be retained when the system reboots.
Keepalive Representative Group	Name of the Keepalive representative group.

Viewing Radius Client Configuration Details for an AAA Group

To view the radius configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Default** > **AAA Radius Client Configuration**. The configurations made for accounting, authentication, charging, and charging accounting servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 15-11 describes the radius client configuration details for accounting, authentication, charging, and charging accounting servers.

Table 15-11 Radius Client Configuration

Field Name	Description
Radius Client Status	The status of the RADIUS client: Up or Down.
Active NAS IP Address	The NAS IP address configured to the client that is currently active.
Configured Primary NAS IP Address	The NAS IP address configured as the primary IP address to the RADIUS client.
Primary IP Address Interface State	The status of the interface to which the primary NAS IP address is configured: Up or down.
Configured Backup NAS IP Address	The NAS IP address configured as the secondary or backup IP address to the RADIUS client.
Secondary IP Address Interface State	The status of the interface to which the secondary or backup NAS IP address is configured: Up or down.

Viewing Radius Accounting Configuration Details for an AAA Group

To view the radius accounting configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Accounting Configuration**. The accounting configuration details are displayed in the content pane.

Table 15-12 describes the radius accounting configuration details.

Table 15-12 Radius Accounting Configuration

Field Name	Description
Server Selection Algorithm	The algorithm to select the RADIUS accounting server(s) to which accounting data must be sent. Values are: • first-n n Default • first-server • round-robin
Billing Version	The billing system version of RADIUS accounting servers.
Server Deadtime	The number of minutes after which communication must be attempted with a server that is not reachable.
Maximum Outstanding Messages	The maximum number of outstanding messages that can be queued with the AAA manager.
Fire and Forget	Indicates whether RADIUS Fire-and-Forget accounting is enabled for the AAA group.
Maximum Transmissions	The maximum number of transmissions attempted for a RADIUS accounting message, before it is declared FAILED.
Maximum Retries	The maximum number of attempts with the AAA server, before it is declared Not Responding and the detected dead server's consecutive failures count is incremented.
Maximum PDU Size (Bytes)	The maximum packet data unit size, in bytes, that can be accepted or generated.
Response Timeout	The time period, in seconds, to wait for a response from the RADIUS server, before resending the message.
Remote Address	Indicates whether the remote IP address lists are configured and the collection of accounting data for the addresses in these lists are enabled.
Archive Messages	Indicates whether archiving of the RADIUS accounting messages in the system (after retries to all available RADIUS accounting servers) is enabled.
APN To Be Included	The Access Point Name (APN) associated with the RADIUS accounting.
Interim Interval	The time interval (in seconds) between sending interim accounting records.
GTP Trigger Policy	The downlink volume that triggers interim RADIUS accounting.

Viewing the Radius Keepalive and Detect Dead Server Configuration Details for an AAA Group

To view the radius accounting/authentication Keepalive and Detect Dead Server Configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Accounting Keepalive and Detect Dead Server Configuration** or **Authentication Keepalive and Detect Dead Server Configuration**. The configuration details are displayed in the content pane.

Table 15-13 describes the radius accounting keepalive and detect dead server configuration details.

Table 15-13 Radius Accounting Keepalive and Detect Dead Server Configuration details

Field Name	Description
Keepalive Interval	The time interval (in seconds) between two keepalive access requests.
Keepalive Timeout	The time period to wait for a response from the RADIUS server, before resending the message. This value is displayed in seconds.
KeepAlive Maximum Retries	The maximum number of keepalive access requests to be sent, before the server is declared as not reachable.
Keepalive Consecutive Response	The number of consecutive accounting responses after which the server is declared as reachable.
Username	The accounting user name.
Calling Station ID	The calling station ID to be used for keepalive accounting.
Keepalive Password	The password to be used for authentication. This field is available only for authentication configuration.
Keepalive Allow Access Reject	Indicates the valid response for authentication request. This field is available only for authentication configuration.
Detect Dead Server Consecutive Failures	The number of consecutive failures for an AAA manager, before the status of an accounting server is changed from Active to Down.
Detect Dead Server KeepAlive	The number of seconds to wait for a response to any message, before the status of an accounting server is changed from Active to Down.

Viewing the RADIUS Attributes Configuration Details for an AAA Group

To view the radius attributes configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Attributes Configuration**. The configuration details are displayed in the content pane.

Table 15-14 describes the attributes configuration details.

Table 15-14 Radius Attributes Configuration details

Field Name	Description
NAS identifier	The AAA interface IP address used to identify the system.
Next HOP	Attribute name by which the system is identified in access request messages.
Backup NAS IP Address	The NAS IP address configured as the secondary or backup IP address to the RADIUS client.
Next HOP	The next hop IP address for the NAS IP address.
Input MPLS Label	Specifies the System's AAA MPLS input label.
Output MPLS Label	Specifies the system's AAA MPLS output label.

Viewing the RADIUS Accounting Attributes Configuration Details for an AAA Group

To view the RADIUS accounting attributes configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Accounting Attributes Configuration**. The configuration details are displayed in the content pane.

Table 15-15 describes the attributes configuration details.

Table 15-15 RADIUS Accounting Attributes Configuration details

Field Name	Description
NAS IP Address	Indicates whether RADIUS accounting attribute for NAS IP Address is enabled.
NAS Identifier	Indicates whether RADIUS accounting attribute for NAS Identifier is enabled.
IMSI	Indicates whether RADIUS accounting attribute for IMSI is enabled.
Service Type	Indicates whether RADIUS accounting attribute for service type is enabled.
Framed IP Address	Indicates whether RADIUS accounting attribute for Framed IP Address is enabled.
Framed IPv6 Prefix	Indicates whether RADIUS accounting attribute for Framed IPv6 Prefix is enabled.
Called Station ID	Indicates whether RADIUS authentication attribute for called station id is enabled.
Calling Station ID	Indicates whether RADIUS authentication attribute for calling station id is enabled.
User Name	Indicates enabled status for - name of the user being authenticated by the RADIUS server.
Class	Indicates whether RADIUS accounting attribute for class is enabled.
NAS Port ID	Indicates whether RADIUS accounting attribute for NAS Port ID is enabled.
Nas Port Type	Indicates whether RADIUS accounting attribute for NAS Port Type is enabled.
3GPP PDP Type	Indicates whether RADIUS accounting attribute for 3GPP PDP type is enabled.
3GPP CG Address	Indicates whether RADIUS accounting attribute for 3GPP CG address is enabled.
3GPP GPRS QoS Negotiated Profile	Indicates whether RADIUS accounting attribute for 3GPP GPRS QoS negotiated profile is enabled.
3GPP SGSN Address	Indicates whether RADIUS accounting attribute for 3GPP SGSN address is enabled.
3GPP GGSN Address	Indicates whether RADIUS accounting attribute for 3GPP GGSN address is enabled.
3GPP GGSN MCC MNC	Indicates whether RADIUS accounting attribute for 3GPP GGSN MCC MNC is enabled.
3GPP IMSI MCC MNC	Indicates whether RADIUS accounting attribute for 3GPP select mode is enabled.
3GPP Select Mode	Indicates whether RADIUS accounting attribute for 3GPP NSAPI is enabled.
3GPP NSAPI	Indicates whether RADIUS accounting attribute for 3GPP NSAPI is enabled.

Table 15-15 RADIUS Accounting Attributes Configuration details

Field Name	Description
3GPP SGSN MCC MNC	Indicates whether RADIUS accounting attribute for 3GPP SGSN MCC MNC is enabled.
3GPP Charging Characteristics	Indicates whether RADIUS accounting attribute for 3GPP charging characteristics is enabled.
3GPP Rat Type	Indicates whether RADIUS accounting attribute for 3GPP RAT type is enabled.
3GPP IMEISV	Indicates whether RADIUS accounting attribute for 3GPP imeisv is enabled.
3GPP MS Timezone	Indicates whether RADIUS accounting attribute for 3GPP ms timezone is enabled.
3GPP User Location Information	Indicates whether RADIUS accounting attribute for 3GPP user location information is enabled.
3GPP Session Stop Indicator	Indicates whether RADIUS accounting attribute for 3GPP Session Stop Indicator is enabled.
3GPP Charging ID	Indicates whether RADIUS accounting attribute for 3GPP charging ID is enabled.
Input Octets	Indicates whether RADIUS accounting attribute for accounting input octets is enabled.
Output Octets	Indicates whether RADIUS accounting attribute for accounting output octets is enabled.
Session Time	Indicates whether RADIUS accounting attribute for accounting session time is enabled.
Input Packets	Indicates whether RADIUS accounting attribute for accounting input packets is enabled.
Output Packets	Indicates whether RADIUS accounting attribute for accounting output packets is enabled.
Event Timestamp	Indicates whether RADIUS accounting attribute for event timestamp is enabled.
Session ID	Indicates whether RADIUS accounting attribute for session id is enabled.
Status Type	Indicates whether RADIUS accounting attribute for status type is enabled.
Authentication	Indicates whether RADIUS accounting attribute for authentication is enabled.
Delay Time	Indicates whether RADIUS accounting attribute for delay time is enabled.

Viewing the RADIUS Authentication Attributes Configuration Details for an AAA Group

To view the radius authentication attributes configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Authentication Attributes Configuration**. The configuration details are displayed in the content pane.

Table 15-16 describes the attributes configuration details.

Table 15-16 RADIUS Authentication Attributes Configuration details

Field Name	Description
NAS IP Address	Indicates whether RADIUS authentication attribute for NAS IP Address is enabled.
NAS Identifier	Indicates whether RADIUS authentication attribute for NAS Identifier is enabled.
IMSI	Indicates whether RADIUS authentication attribute for IMSI is enabled.
Service Type	Indicates whether RADIUS authentication attribute for service type is enabled.
Framed IP Address	Indicates whether RADIUS authentication attribute for Framed IP Address is enabled.
Framed IPv6 Prefix	Indicates whether RADIUS authentication attribute for Framed IPv6 Prefix is enabled.
Called Station ID	Indicates whether RADIUS authentication attribute for called station id is enabled.
Calling Station ID	Indicates whether RADIUS authentication attribute for calling station id is enabled.
Chap Challenge	Indicates if the Challenge Handshake Authentication Protocol challenge sent by the network access server to a PPP CHAP user, is enabled.
Nas Port Type	NAS-Port-Type (RADIUS IETF attribute 61) indicates the type of physical port the network access server (NAS) is using to authenticate the user.
NAS Port ID	NAS-Port-ID (RADIUS IEFT attribute 87) contains a text string that identifies the NAS port that is authenticating the user.
User Name	Indicates enabled status for - name of the user being authenticated by the RADIUS server.
3GPP PDP Type	Indicates whether RADIUS authentication attribute for 3GPP PDP type is enabled.
3GPP CG Address	Indicates whether RADIUS authentication attribute for 3GPP CG address is enabled.
3GPP GPRS QoS Negotiated Profile	Indicates whether RADIUS authentication attribute for 3GPP GPRS QoS negotiated profile is enabled.
3GPP SGSN Address	Indicates whether RADIUS authentication attribute for 3GPP SGSN address is enabled.

Table 15-16 RADIUS Authentication Attributes Configuration details

Field Name	Description
3GPP GGSN Address	Indicates whether RADIUS authentication attribute for 3GPP GGSN address is enabled.
3GPP GGSN MCC MNC	Indicates whether RADIUS authentication attribute for 3GPP GGSN MCC MNC is enabled.
3GPP IMSI MCC MNC	Indicates whether RADIUS authentication attribute for 3GPP select mode is enabled.
3GPP Select Mode	Indicates whether RADIUS authentication attribute for 3GPP NSAPI is enabled.
3GPP NSAPI	Indicates whether RADIUS authentication attribute for 3GPP NSAPI is enabled.
3GPP SGSN MCC MNC	Indicates whether RADIUS authentication attribute for 3GPP SGSN MCC MNC is enabled.
3GPP Charging Characteristics	Indicates whether RADIUS authentication attribute for 3GPP charging characteristics is enabled.
3GPP Rat Type	Indicates whether RADIUS authentication attribute for 3GPP RAT type is enabled.
3GPP IMEISV	Indicates whether RADIUS authentication attribute for 3GPP imeisv is enabled.
3GPP MS Timezone	Indicates whether RADIUS authentication attribute for 3GPP ms timezone is enabled.
3GPP User Location Information	Indicates whether RADIUS authentication attribute for 3GPP user location information is enabled.

Viewing the Radius Authentication Configuration Details for an AAA Group

To view the radius authentication configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Authentication Configuration**. The authentication configuration details are displayed in the content pane.

Table 15-17 describes the radius authentication configuration details.

Table 15-17 Radius Authentication Configuration

Field Name	Description
Server Selection Algorithm	The algorithm to select the RADIUS accounting server(s) to which accounting data must be sent. Values are: • first-server • round-robin
Server Deadtime	The time period after which the status of the authentication server must be changed from Down to Active.
Maximum Outstanding Messages	The maximum number of outstanding messages that can be queued with the AAA manager.
Authentication Maximum Retries	The maximum number of attempts with the AAA server, before it is declared Not Responding and the detected dead server's consecutive failures count is incremented.
Authentication Maximum Transmissions	The maximum number of transmissions attempted for a RADIUS authentication message, before it is declared FAILED.
Authentication Response Timeout	The time period to wait for a response from the RADIUS server, before resending the message. This value is displayed in seconds.
APN To Be Included	The APN associated with the RADIUS authentication.
Authenticate Null User Name	Indicates whether the authentication of user names that are blank or empty is enabled.
Modify NAS IP	Indicates whether the RADIUS authentication is attempted after NAS IP is modified.
Probe Interval	The time interval (in seconds) before sending another probe authentication request to a RADIUS server.
Probe Timeout	The time period (in seconds) to wait for a response from a RADIUS server before resending the authentication probe.
Probe Maximum Retries	The number of retries for RADIUS authentication probe response before the authentication is declared as failed.

Viewing the Charging Configuration Details for an AAA Group

To view the radius charging configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Charging Configuration**. The charging configuration details are displayed in the content pane.

Table 15-18 describes the charging configuration details.

Table 15-18 Radius Charging Configuration

Field Name	Description
Authentication Server Selection Algorithm	The algorithm to select the RADIUS server(s) for active charging service to ensure proper load distribution amongst the available servers used for authentication requests. Value could be one of the following: • first-server • round-robin
Accounting Server Selection Algorithm	The algorithm to select the RADIUS server(s) for active charging service to ensure proper load distribution amongst the available servers for accounting requests. Value could be one of the following: • first-n n Default • first-server • round-robin
Server Deadtime	The time period after which the status of the RADIUS server must be changed from Down to Active.
Maximum Outstanding Messages	The maximum number of outstanding messages that can be queued with the AAA manager.
Maximum Retries	The maximum number of attempts with the AAA server, before it is declared Not Responding and the detected dead server's consecutive failures count is incremented.
Response Timeout	The maximum number of retransmissions for RADIUS authentication requests.
Detect Dead Server Consecutive Retries	The number of consecutive failures for an AAA manager, before the status of an charging server is changed from Active to Down.

Viewing the Charging Trigger Configuration Details for an AAA Group

To view the radius charging trigger configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Charging Trigger**. The charging configuration details are displayed in the content pane.

Table 15-19 describes the charging trigger configuration details.

Table 15-19 Radius Charging Triggers Configuration

Field Name	Description
Serving Node Change	Indicates whether RADIUS trigger for serving node is enabled.
Radio Access Technology Change	Indicates whether RADIUS trigger for radio access technology change is enabled.
User Location Information Change	Indicates whether RADIUS trigger for user location information change is enabled.
Routing Area Information Change	Indicates whether RADIUS trigger for routing area information change is enabled.
Quality of Service Change	Indicates whether RADIUS trigger for quality of service change is enabled.
Mobile Station Timezone Change	Indicates whether RADIUS trigger for mobile station time zone change is enabled.

Viewing TACACS+ Group Configuration Details for an AAA Group

To view the TACACS+ group configuration details for a AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the **Inventory** window, choose **Logical Inventory > AAA > AAA Groups**.The configuration details are displayed on the content pane. (The attributes that are displayed depend on the device type.)

Step 3 Expand a specific **TACACS+ Group** node and then **choose TACACS+ Configuration** under a specific AAA group node.

Table 15-20 describes the TACACS+ group configuration details and its associated TACACS+ Servers details.

Table 15-20 TACACS+ group Configuration

Field Name	Description
Group Name	The AAA group name.
Group Type	The AAA group type.
Source Interface	Specifies that the IP address of this specified interface is used for all outgoing TACACS+ packets.
VRF	The VRF used in this TACACS+ server group.
Acknowledge Broadcast Accounting	Specifies if accounting information can be broadcast to one or more AAA servers simultaneously.
Cache Expiry Time	Specifies the length of time, in hours, for a cache database profile entry to expire.
Cache Expiry Rule	Specifies how the expired cached database profile entries in this TACACS+ server group are to be used: • Enforce—Indicates not to use expired entries. • Failover—Indicates to use an expired entry if all other methods fail.
Cache Authentication Profile Name	The name of the cache authentication profile used in this TACACS+ server group.
Cache Authorization Profile Name	The name of the cache authorization profile used in this TACACS+ server group.
Associated TACACS+ Servers	
Server Address	The IP address or hostname of the TACACS+ server.
Port	The TCP port used to communicate with the TACACS+ server.
Server Name	The name of the associated TACACS+ Server.
Status	Specifies the operational state of the interface with the TACACS+ server.

Configuring AAA Groups

The following commands can be launched from the inventory by right-clicking and AAA group and choosing **Commands > Configuration**. Your permissions determine whether you can run these commands (see Permissions for Vision Client NE-Related Operations, page B-4). To find out if a device supports these commands, see the *Cisco Prime Network 5.1 Supported Cisco VNEs*.

Command	Navigation	Description
Create Diameter Accounting Server	Right-click the *AA group* > **Commands** > **group dialog box, select a group name** and then choose **Commands > Configuration > Create Diameter Accounting Server**	Use this command to create a new diameter accounting server.
Create Diameter Authentication Server	Right-click the *AA group* > **Commands** > **group dialog box, select a group name** and then choose **Commands > Configuration > Create Diameter Authentication Server**	Use this command to create a new diameter authentication server.
Delete AAA Group	Right-click the *AA group* > **Commands** > **group dialog box, select a group name** and then choose **Commands > Configuration > Delete AAA Group**	Use this command to delete an AAA group.
Modify AAA Group	Right-click the *AA group* > **Commands** > **group dialog box, select a group name** and then choose **Commands > Configuration > Modify AAA Group**	Use this command to modify the attributes of an AAA group.