RADIUS Authentication Attributes

Abstract: Remote Authentication Dial In User Service (RADIUS) is an IETF-standard Internet protocol that supports client-server architecture and uses the User Datagram Protocol (UDP) as described in IETF specification RFC 2865 RADIUS. RADIUS enables network administrators to control who has access to the network, what systems or resources can be accessed, if users have configuration control and how much bandwidth is available, among other polices. RADIUS can also be configured to limit access to specific individuals and/or groups, time/day and hardware addresses.

When user requests login access, the wireless controller sends an Access-Request to the RADIUS server, which uses IETF-standard or vendor specific attributes to grant, deny or challenge user access to the network. The RADIUS server may be configured to authenticate locally or against SQL, Kerberos, LDAP, or Microsoft Active Directory.

This How-To-Guide describes how to deploy RADIUS authentication in a WLAN configured using Extreme Networks® Summit® WM3000 series controllers and Altitude™ access points.

Table of Contents

RADIUS Authentication Attributes

The IETF standard, Remote Authentication Dial In User Service (RADIUS) is an network protocol that supports client-server architecture and User Datagram Protocol (UDP) as described in IETF specification RFC 2865 RADIUS. When a wireless user requests login access, the Summit WM3000 series controller sends an Access-Request to the RADIUS server for authentication. The RADIUS server may be configured to authenticate locally or against SQL, Kerberos, LDAP, or Microsoft Active Directory. The RADIUS server processes the request according to its preconfigured authentication attributes, which may be standards-based or vendor-specific. The RADIUS server then sends this information to the Summit WM3000 series controller, which uses the returned information to either grant or deny wireless access.

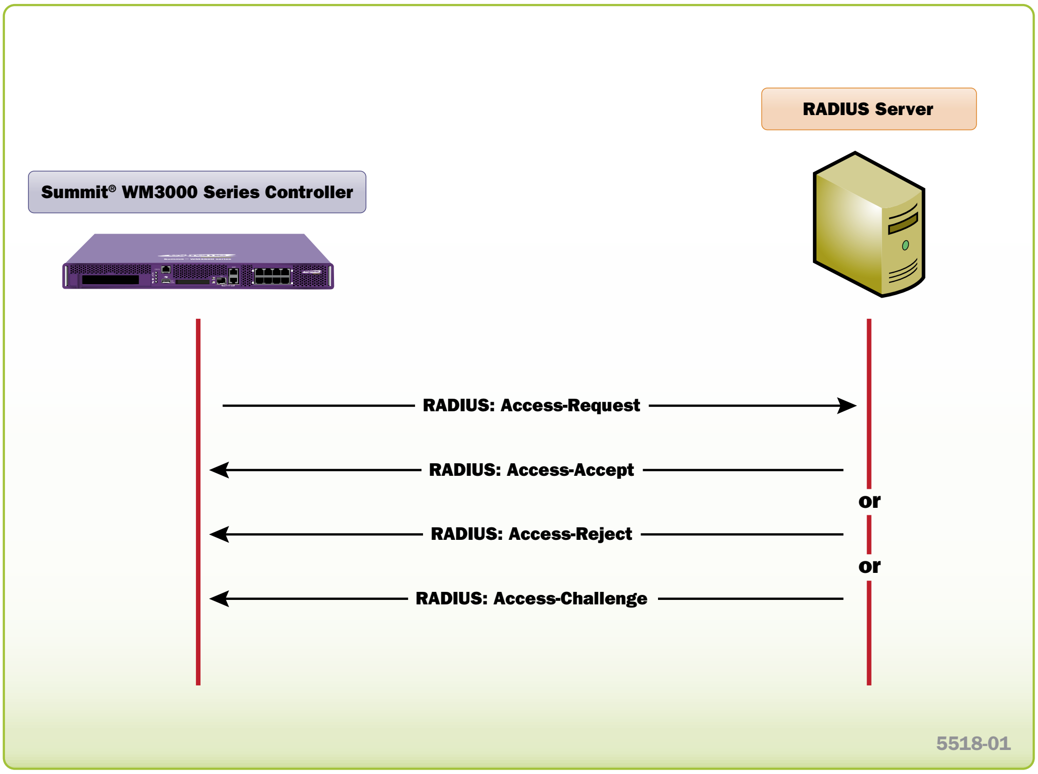

Figure 1: RADIUS Authentication and Authorization

During authentication, the RADIUS server returns one of three responses to the Summit WM3000 series controller's integrated network access server(NAS):

1. **Access-Reject –** The user is unconditionally denied access to the requested network resource. Failure reasons may include an invalid credentials or an inactive account.

2. **Access-Challenge –** Requests additional information from the user such as a secondary password, PIN, token or card. Access-Challenge is also used in more complex authentication when a secure tunnel is established between the user and the Radius Server such as authentication using Extensible Authentication Protocol (EAP).

3. **Access-Accept –** The user is permitted access. The Access-Request often includes additional configuration information for the user using return attributes.

RADIUS services can be enabled on the Summit WM3000 series controller for management user authentication as well as WLAN user authentication. RADIUS services are required for WLANs implementing 802.1X/EAP and hotspot services but may also be enabled for MAC-based authentication.

IETF Standard Attributes

The following table summarizes the IETF standard attributes supported by the Summit WM3000 series controller, in compliance with IETF standard, RFC 2865 RADIUS. Additional extensions—following the IETF recommendations for RFC 2868/RFC 2869 RADIUS—are also supported.

IETF Standard Attributes

Attribute Name	Type	RFC	Forwarded In	Description
User-Name	1	RFC 2865	Access-Request	Indicates the name of the user to be authenticated.
User-Password	2	RFC 2865	Access-Request	Indicates 1) password of the user to be authenticated, or 2) user's input following an **Access-Challenge**.
CHAP-Password	3	RFC 2865	Access-Request	Indicates a PPP Challenge-Handshake Authentication Protocol (CHAP) response to an **Access-Challenge**.
NAS-IP-Address	4	RFC 2865	Access-Request	Indicates the IP Address of the Summit WM3000 series controller requesting user authentication.
NAS-Port	5	RFC 2865	Access-Request	Indicates the association index of the user on the Summit WM3000 series controller.
Service-Type	6	RFC 2865	Access-Request	Indicates 1) type of service requested by the user, or 2) type of service to be provided. This attribute value is always set to **Framed-User** by the Summit WM3000 series controller.
Framed-MTU	12	RFC 2865	Access-Request	Indicates the Maximum Transmission Unit (MTU) to be configured for the user. This attribute value is always set to **1400** by the Summit WM3000 series controller.
State	24	RFC 2865	Access-Request	This attribute is available for forwarding and must be sent unmodified from the client to the server in the reply to **Access-Challenge**, if any.
Called-Station-Id	30	RFC 2865	Access-Request	Indicates which **BSSID** and **ESSID** are associated with the authenticating user. This attribute value is configured using the syntax: **XX-XX-XX-XX-XX-XX:ESSID**.
Calling-Station-Id	31	RFC 2865	Access-Request	Indicates the MAC address of the authenticating user. It is only used in **Access-Request** packets. This attribute value is configured using the syntax: **XX-XX-XX-XX-XX-XX**.
NAS-Identifier	32	RFC 2865	Access-Request	Indicates the hostname or user defined identifier of the Summit WM3000 series controller.
CHAP-Challenge	60	RFC 2865	Access-Request	Indicates the CHAP Challenge sent by the Summit WM3000 series controller to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.
NAS-Port-Type	61	RFC 2865	Access-Request	Indicates the type of physical network connection. This attribute value is always set to **Wireless-802.11** by the Summit WM3000 series controller.
Connection-Info	77	RFC 2869	Access-Request	Indicates the data-rate and radio-type of the authenticating user. This attribute value is configured using the following syntax: **CONNECT XXMbps 802.11X**.
NAS-Port-Id	87	RFC 2869	Access-Request	Indicates which ESSID is associated with the authenticating user.
CHAP-Challenge	60	RFC 2865	Access-Request	Contains the CHAP Challenge sent by the Summit WM3000 series controller to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.
EAP-Message	79	RFC 2869	Access-Request Access-Challenge Access-Accept Access-Reject	Encapsulates Extended Access Protocol (EAP) packets.
Message-Authenticator	80	RFC 2869	Access-Request	Used to prevent spoofing of CHAP, ARAP or EAP **Access-Request** packets.
Tunnel-Private-Group-ID	81	RFC 2868	Access-Accept	Indicates the numerical VLAN ID assigned to the authenticating user. This attribute must be set to a numerical value between **1** and **4094**.

Tunnel-Private-Group-ID

The **Tunnel-Private-Group-ID** attribute may be forwarded in the **Access-Accept** to indicate the dynamic VLAN membership of an 802.1X- or RADIUS MAC-authenticated user. The VLAN value returned from the RADIUS server will override any static VLANs defined in the WLAN profile.

Attribute Details

Attribute Name	Attribute Number	Attribute Value
Tunnel-Private-Group-ID	81	1 – 4094 (Assigned VLAN-ID)

Vendor-Specific Attributes

The following table summarizes the Extreme Networks Vendor-Specific Attributes (VSAs) supported by the Summit WM3000 series controller in compliance with IETF standard RFC 2865 RADIUS.

Extreme Networks Vendor-Specific Attributes

Attribute Name	Type	Vendor ID	Attribute Number	Formatting
Extreme-Service-Type	26	1916	1	Integer
Extreme-Current-SSID	26	1916	2	String
Extr_Wlan_Allowed_SSID	26	1916	3	String
Extreme-Wlan-Index	26	1916	4	Integer
Extr_Wlan_QoS_Profile	26	1916	5	Integer
Extr_Wlan_Allowed_Radio	26	1916	6	String
Guest-User-Expiry-Date-Time	26	1916	7	String
Guest-User-Start-Date-Time	26	1916	8	String
Extr_MU_Posture_Status	26	1916	9	String
Extreme-Downlink-Limit-Kbps	26	1916	10	String
Extreme-Uplink-Limit-Kbps	26	1916	11	Integer
Extreme-User-Group	26	1916	12	Integer
Extreme-Login-Service	26	1916	100	Integer

Extreme-Admin-Type

The **Extreme-Admin-Type** attribute may be forwarded in an **Access-Accept** request and indicates which management user permissions are granted by the Summit WM3000 series controller, when RADIUS management user authentication is enabled. The **Extreme-Admin-Type** attribute can be used to assign one or more management roles to a user. When multiple roles are assigned, multiple **Extreme-Admin-Type** attributes and values must be returned to the Summit WM3000 series controller.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extreme-Admin-Type	1916	1	Integer

Integer Value	Associated Roles	Description
1	Monitor	This role is assigned to personnel requiring read-only access to the Summit WM3000 series controller.
2	Help Desk Manager	This role is assigned to personnel responsible for troubleshooting and debugging problems. It provides access to troubleshooting utilities, execution of service commands, logs and rebooting of the switch.
4	Network Administrator	This role is assigned to personnel responsible for configuration of wired and wireless parameters such as IP configuration, VLANs, firewalls, WLANs, access points, IDS and hotspots.
8	System Administrator	This role is assigned to personnel responsible for configuring general switch settings such as NTP, boot parameters, licenses, images, auto install, clustering and access control.
16	Web User Administrator	This role is assigned to non-technical personnel and supports adding guest-user accounts for hotspot authentication.
32768	Super User	This role is assigned to personnel requiring full administrative privileges.

Extreme-Current-SSID

The **Extreme-Current-SSID** attribute is forwarded in the **Access-Request** and indicates with which ESSID the authenticating user is associated.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extreme-Current-SSID	1916	2	String
Format: **ESSID-Name**			
Example: **Hotspot**			

Extr_Wlan_Allowed_SSID

The **Extr_Wlan_Allowed_SSID** attribute may be forwarded in the **Access-Accept** and indicates which ESSIDs are associated with a user. The **Extr_Wlan_Allowed_SSID** attribute can be used to permit access to one or more ESSIDs. When multiple ESSIDs are permitted, multiple **Extr_Wlan_Allowed_SSID** attributes and values must be returned to the Summit WM3000 series controller. During authorization, the Summit WM3000 series controller will check the returned ESSIDs against the ESSID already associated with the authenticating user. The user is permitted access to any of the ESSIDs that match. The user will be denied any ESSIDs that do not match.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extr_Wlan_Allowed_SSID	1916	3	String
Format: **ESSID-Name**			
Example: **Sales**			

Extreme-Wlan-Index

The **Extreme-WLAN-Index** attribute is forwarded in the **Access-Request** and indicates which WLAN index number is associated with the authenticating user.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extreme-Wlan-Index	1916	4	Integer
Format: **Index-Number**			
Example: **2**			

Extr_Wlan_QoS_Profile

The **Extr_Wlan_QoS_Profile** attribute may be forwarded in the **Access-Accept** and indicates the static WMM Access Category (AC) to be assigned to the authenticating user. Once assigned, traffic forwarded from the AP to the user will be prioritized using the assigned QoS value.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extr_Wlan_QoS_Profile	1916	5	Integer
Supported Values: **4 (Voice), 3 (Video), 2 (Background), 1 (Best Effort)**			
Example: **1**			

Extr_Wlan_Allowed_Radio

The **Extr_Wlan_Allowed_Radio** attribute may be forwarded in the **Access-Accept** and indicates one or more radios with which the authenticating user is permitted to associate. The **Extr_Wlan_Allowed_Radio** returned value must match one or more key words defined in the radio description fields for the user to be permitted access.

For example, if the RADIUS server returns the string **1st-Floor**, the Summit WM3000 series controller will only permit access to radios configured with 1st-Floor defined in the description field, such as **1st-Floor-Conference-Room** or **1st-Floor-Cafateria**, while blocking access to radios with the description **2nd-Floor-Conference-Room**.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extr_Wlan_Allowed_Radio	1916	6	String
Format: **Radio-Index-Number**			
Example: **1st-Floor**			

Guest-User-Expiry-Date-Time

The **Guest-User-Expiry-Date-Time** attribute may be forwarded in the **Access-Accept** and indicates the date and time during which an authenticating user is no longer authorized to access the network. During authorization, the Summit WM3000 series controller will check the returned date and time values against the current date and time on the controller. If the returned date and time is before the current date and time on the controller, the user will be permitted access. If the returned date and time is after the current date and time on the controller, the user will be denied access.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Guest-User-Expiry-Date-Time	1916	7	String
Format: **MM/DD/YYYY-HH:MM**			
Example: **01/02/2009-17:00**			

Guest-User-Start-Date-Time

The **Guest-User-Start-Date-Time** attribute maybe forwarded in the **Access-Accept** and indicates the date and time the authenticating user is initially permitted to access the network.

During authorization, the Summit WM3000 series controller will compare the date and time values included with the request against the internal clock of the Summit WM3000 series controller. If the requested date/time falls **after** the clock date/time, the user will be permitted access. If the requested date/time falls **before** the clock date/time, the user will be denied access.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Guest-User-Start-Date-Time	1916	8	String
Format: **MM/DD/YYYY-HH:MM**			
Example: **01/01/2009-08:00**			

Extr_MU_Posture_Status

The **Extr_MU_Posture_Status** attribute may be forwarded in the **Access-Accept** and indicates the NAP compliance state of the authenticating user. This attribute is used with the Symantec LAN Enforcer endpoint inspection solution.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extr_MU_Posture_Status	1916	9	String

Extreme-Downlink-Limit-Kbps

The **Extreme-Downlink-Limit-Kbps** attribute may be forwarded in the **Access-Accept** and indicates the access point bandwidth (in Kbps) the authenticating user is permitted to receive. Traffic loads that exceed the defined value will be dropped by the Summit WM3000 series controller.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extreme-Downlink-Limit-Kbps	1916	10	Integer
Format: **0, 100-10,000 (0 = Disabled)**			
Example: **768**			

Symbol-Uplink-Limit

The **Symbol-Uplink-Limit** attribute may be forwarded in the **Access-Accept** and indicates the access point bandwidth (in Kbps) the authenticating user is permitted to transmit. Traffic loads that exceed the defined value will be dropped by the Summit WM3000 series controller.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Uplink-Limit	1916	11	Integer
Format: **0, 100-10,000 (0 = Disabled)**			
Example: **512**			

Extreme-User-Group

The **Extreme-User-Group** attribute may be forwarded in the **Access-Accept** and indicates which group on the Summit WM3000 series controller is associated with the authenticating user. Groups may be assigned to users to apply policies such as defining VLAN membership, time of day restrictions and bandwidth limits. Groups can also be used to assign dynamic firewall policies using the role-based firewall.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extreme-User-Group	1916	12	String
Format: **Group-Name**			
Example: **Sales**			

Extreme-Login-Service

The **Extreme-Login-Service** attribute may be forwarded in the **Access-Accept** and indicates which management interfaces the user is permitted to access on the Summit WM3000 series controller, when RADIUS management user authentication is enabled.

During authorization the controller will check the returned list of permitted interfaces against the current interface through which the user is authenticating. If the interface is permitted the user will be permitted access to the controller. If the interface is not permitted the user will be denied access to the controller.

The **Extreme-Login-Service** attribute can be used to permit access to one or more management interfaces, or all management interfaces. When multiple interfaces are assigned, multiple **Extreme-Login-Service** attributes and values must be returned to the controller.

Attribute Details

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Extreme-Login-Service	1916	100	Integer

Integer Value	Login Source	Description
16	HTTP	Permits management access using the Web-UI.
32	SSH	Permits management access using SSH.
64	Telnet	Permits management access using Telnet.
128	Console	Permits management access using serial console.
240	All	Permits management access using all management interfaces.

RADIUS Accounting Attributes

RADIUS accounting is used to send accounting information about an authenticated session to the RADIUS accounting server. Accounting information is sent to the server when a user connects and disconnects from a WLAN and may also be periodically forwarded during the session. RADIUS accounting information can be used to track individual user's network usage for billing purposes as well as be used as a tool for gathering statistics for general network monitoring.

When the Summit WM3000 series controller grants network access to a user, it forwards an Accounting-Request message, with the Acct-Status-Type field set to Start, to the RADIUS server. This signals the initiation of network access by the user. Start records typically contain user identification, network address, point of attachment and a unique session identifier.

Optionally, the Summit WM3000 series controller may send periodic Accounting-Request messages, with the Acct-Status-Type field set to Interim Update, to the RADIUS server, in order to update the status of an active session. Interim records typically convey the current session duration and information on current data usage.

When the user session is closed, the Summit WM3000 series controller forwards an Accounting-Request message, with the Acct-Status-Type field set to Stop. This provides usage information such as length of session, time of access packets transferred, data transferred and reason for disconnect, and other information related to the user access.

RADIUS Accounting can be enabled/disabled in the Summit WM3000 series controller for each WLAN profile. Also, administrators can select how the Summit WM3000 series controller forwards accounting information to the RADIUS server. For each WLAN profile, the following accounting configuration parameters are supported:

1. **Start-Stop –** Forwards **Accounting-Requests** at the start and end of user sessions.
2. **Stop-Only –** Forwards **Accounting-Requests** at the end of user sessions.
3. **Start-Interim-Stop –** Forwards **Accounting-Requests** at the start and end of user sessions, as well as periodically during the sessions.

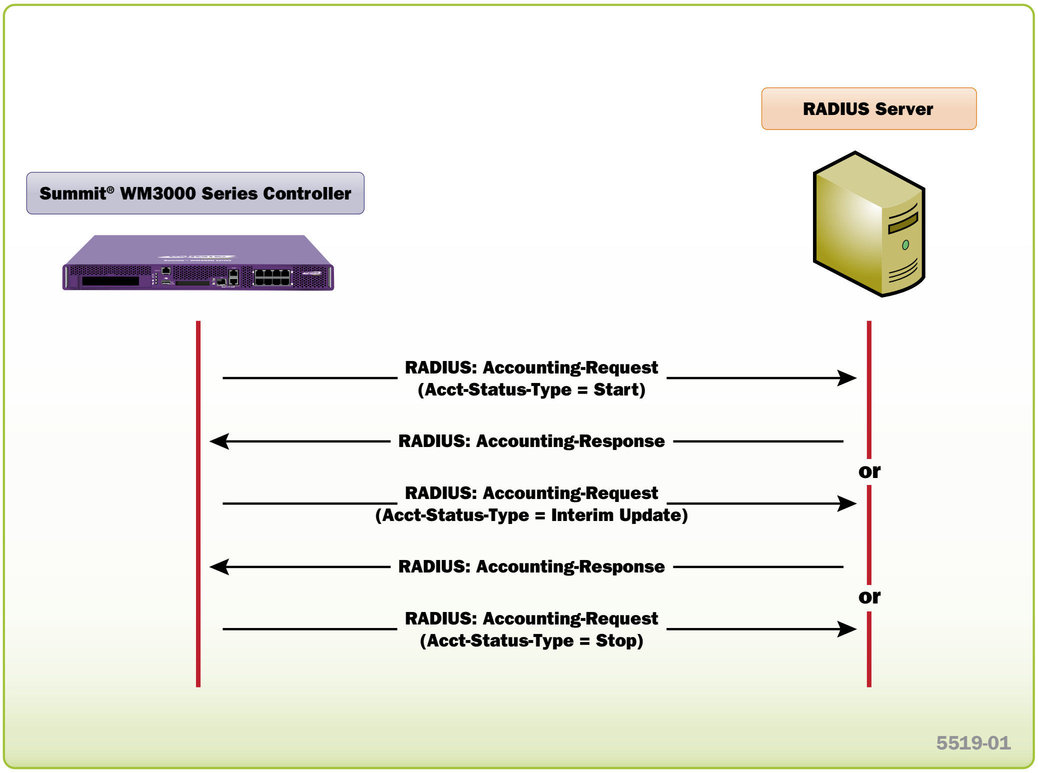
RADIUS Server
Summit® WM3000 Series Controller
RADIUS: Accounting-Request
(Acct-Status-Type = Start)
RADIUS: Accounting-Response
or
RADIUS: Accounting-Request
(Acct-Status-Type = Interim Update)
RADIUS: Accounting-Response
or
RADIUS: Accounting-Request
(Acct-Status-Type = Stop)
5519-01

Figure 2: RADIUS Accounting Attributes

The following table summarizes the standard RADIUS accounting attributes supported by the Summit WM3000 series controller in accordance to RFC 2866:

IETF Standard Attributes

Attribute Name	Type	RFC	Forwarded In	Description
User-Name	1	RFC 2865	Accounting-Request	Indicates the name of the user.
NAS-IP-Address	4	RFC 2865	Accounting-Request	Indicates the IP Address of the Summit WM3000 series controller.
NAS-Port	5	RFC 2865	Accounting-Request	Indicates the association index of the user on the Summit WM3000 series controller.
Class	25	RFC 2865	Accounting-Accept	Optionally forwarded (if accounting is supported) in the **Access-Accept** and should be sent unmodified as part of the **Accounting-Request** packet.
Called-Station-Id	30	RFC 2865	Accounting-Request	Indicates the BSSID and ESSID that the user is associated with. The Summit WM3000 series controller will forward the attribute value using the following formatting: **XX-XX-XX-XX-XX-XX:ESSID**.
Calling-Station-Id	31	RFC 2865	Accounting-Request	Indicates the MAC address of the user. The Summit WM3000 series controller will forward the attribute value using the following formatting: **XX-XX-XX-XX-XX-XX**.
NAS-Identifier	32	RFC 2865	Accounting-Request	Indicates the hostname or user defined identifier of the Summit WM3000 series controller.
Acct-Status-Type	40	RFC 2866	Accounting-Request	indicates whether the **Accounting-Request** marks the status of the accounting update. Supported values include **Start**, **Stop** and **Interim-Update**.
Acct-Delay-Time	41	RFC 2866	Accounting-Request	Indicates how many seconds the Summit WM3000 series controller has been trying to send the accounting record for. This value is subtracted from the time of arrival on the server to find the approximate time of the event generating this **Accounting-Request**.
Acct-Input-Octets	42	RFC 2866	Accounting-Request	Indicates how many octets have been received from the user over the course of the connection. This attribute may only be present in **Accounting-Request** records where the **Acct-Status-Type** is set to **Stop**.
Acct-Output-Octets	43	RFC 2866	Accounting-Request	Indicates how many octets have been forwarded to the user over the course of the connection. This attribute may only be present in **Accounting-Request** records where the **Acct-Status-Type** is set to **Stop**.
Acct-Session-Id	44	RFC 2866	Accounting-Request	Provides a unique identifier to make it easy to match start, stop and interim records in an accounting log file.
Account-Authentic	45	RFC 2866	Accounting-Request	Indicates how the user was authenticated. When RADIUS accounting is enabled the Summit WM3000 series controller will set this value to **RADIUS**.
Acct-Session-Time	46	RFC 2866	Accounting-Request	Indicates how many seconds the user has received service for. This attribute may only be present in **Accounting-Request** records where the **Acct-Status-Type** is set to **Stop**.
Acct-Input-Packets	47	RFC 2869	Accounting-Request	Indicates how many packets have been received from the user over the course of the connection. This attribute may only be present in **Accounting-Request** records where the **Acct-Status-Type** is set to **Stop**.
Acct-Output-Packets	48	RFC 2866	Accounting-Request	Indicates how many packets have been forwarded to the user over the course of the connection. This attribute may only be present in **Accounting-Request** records where the **Acct-Status-Type** is set to **Stop**.
Acct-Terminate-Cause	49	RFC 2866	Accounting-Request	Indicates how the session was terminated. This attribute may only be present in **Accounting-Request** records where the **Acct-Status-Type** is set to **Stop**.
Event-Timestamp	55	RFC 2869	Accounting-Request	Indicates the time that the accounting event occurred on the Summit WM3000 series controller.
NAS-Port-Type	61	RFC 2865	Accounting-Request	Indicates the type of physical connection for the user. This attribute value is always set to **Wireless-802.11** by the Summit WM3000 series controller.
Tunnel-Type	64	RFC 2868	Accounting-Request	Indicates the tunneling protocol(s) used by the user. This attribute value is always set to type **13 (Virtual LANs)**.
Tunnel-Medium-Type	65	RFC 2868	Accounting-Request	Indicates which transport medium used by the user. This attribute value is always set to type **6 (802 includes all 802 media plus Ethernet “canonical format”)**.
Tunnel-Private-Group-ID	81	RFC 2868	Accounting-Request	Indicates the numerical VLAN ID assigned to the user. This attribute value is always set to a numerical value between **1** and **4094**.
NAS-Port-Id	87	RFC 2869	Accounting-Request	Indicates the ESSID that the user is associated with.

Dynamic Authorization Extensions

The RADIUS authentication protocol does not support unsolicited messages sent from the RADIUS server to the Summit WM3000 series controller. However, there are many instances in which it is desirable for changes to be made to session characteristics without requiring the Summit WM3000 series controller to initiate the exchange.

To overcome these limitations, several vendors have implemented additional RADIUS extensions to support unsolicited messages sent from the RADIUS server to the Summit WM3000 series controller. These extensions support Disconnect and Change-of-Authorization (CoA) messages that can be used to change the characteristics of or terminate an active user session.

1. **Disconnect-Request –** Terminates an active user session. The **Disconnect-Request** packet identifies the NAS, as well as the user session to be terminated, by inclusion of the identification attributes shown below.
2. **CoA-Request –** Dynamically updates connection information on the Summit WM3000 series controller during an active user session. Currently a **CoA-Request** packet may only be used to change the user **session-timeout** and **idle-timeout**.

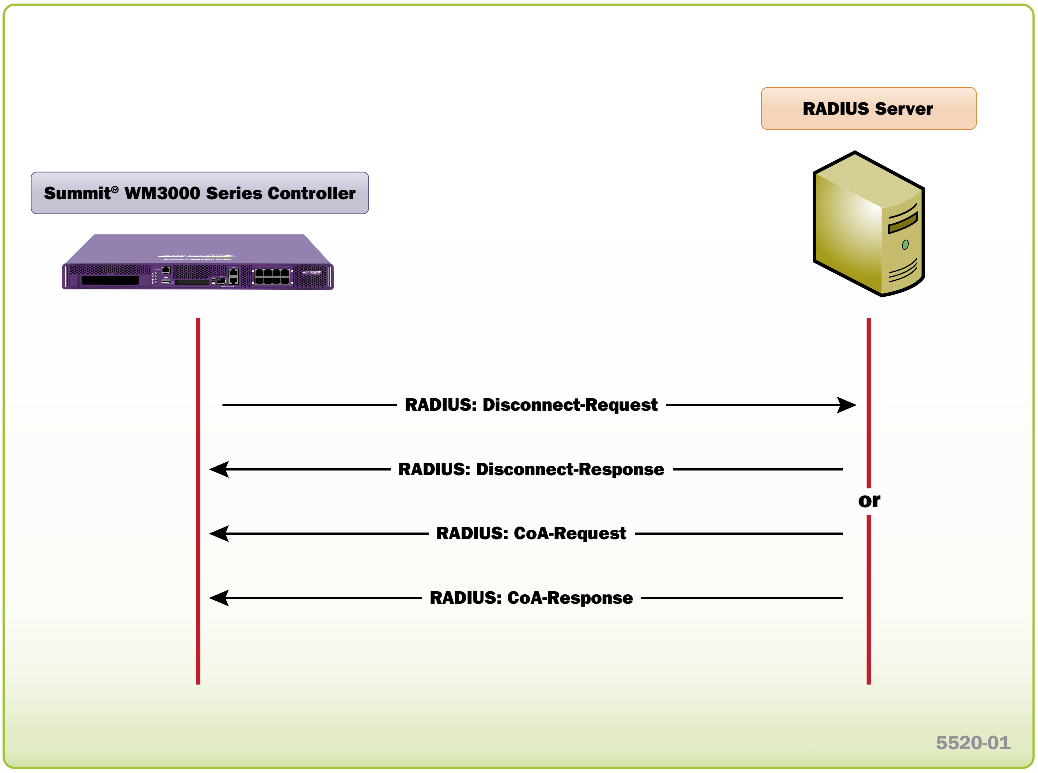
RADIUS Server
Summit® WM3000 Series Controller
RADIUS: Disconnect-Request
RADIUS: Disconnect-Response
or
RADIUS: CoA-Request
RADIUS: CoA-Response
5520-01

Figure 3: Dynamic Authorization Extensions

The following table summarizes the dynamic authorization extension attributes supported by the Summit WM3000 series controller, in accordance with RFC 3576.

Dynamic Authorization Extensions

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	Name of the user.
Calling-Station-Id	31	RFC 2865	MAC address of the user.
Acct-Session-Id	44	RFC 2866	The identifier uniquely identifying the session on the NAS.

The **Called-Station-Id**, **NAS-Identifier**, **NAS-IP-Address** and **Service-Type** attributes, if present, are also evaluated by the Summit WM3000 series controller.

RADIUS Dictionary Files

Cisco Secure Access Control Server

The following provides the necessary information to create a dictionary file that includes all the supported vendor-specific attributes for Cisco Secure Access Control Server. The provided text can be copied into a file named **symbol.ini** and imported using the provided CSUtil utility.

```
;
; Summit WM Controller Dictionary File for Cisco Secure ACS
; Last Updated: July 21st 2010
; Created By: mgutierrez@extremenetworks.com
;

[User Defined Vendor]
Name=SYMBOL
IETF Code=1916

VSA 1=Extreme-Service-Type
VSA 2=Extreme-Current-SSID
VSA 3=Extr_Wlan_Allowed_SSID
VSA 4=Extreme-Wlan-Index
VSA 5=Extr_Wlan_QoS_Profile
VSA 6=Extr_Wlan_Allowed_Radio
VSA 7=Guest-User-Expiry-Date-Time
VSA 8=Guest-User-Start-Date-Time
VSA 9=Extr_MU_Posture_Status
VSA 10=Extreme-Downlink-Limit-Kbps
VSA 11=Extreme-Uplink-Limit-Kbps
VSA 12=Extreme-User-Group
VSA 100=Extreme-Login-Service

[Extreme-Service-Type]
Type=INTEGER
Profile=OUT
Enums=Admin-Role

[Admin-Role]
1=Monitor
2=Helpdesk
4=NetworkAdmin
8=SysAdmin
16=WebAdmin
32768=SuperUser

[Extreme-Current-SSID]
Type=STRING
Profile=IN

[Extreme-Current-SSID]
Type=STRING
Profile=IN

[Extr_Wlan_Allowed_SSID]
Type=STRING
Profile=OUT
```

```
[Extreme-Wlan-Index]
Type=INTEGER
Profile=IN

[Extr_Wlan_QoS_Profile]
Type=INTEGER
Profile=IN

[Extr_Wlan_Allowed_Radio]
Type=STRING
Profile=OUT

[Guest-User-Expiry-Date-Time]
Type=STRING
Profile=OUT

[Guest-User-Start-Date-Time]
Type=STRING
Profile=OUT

[Extr_MU_Posture_Status]
Type=STRING
Profile=OUT

[Extreme-Downlink-Limit-Kbps]
Type=INTEGER
Profile=OUT

[Extreme-Uplink-Limit-Kbps]
Type=INTEGER
Profile=OUT

[Extreme-User-Group]
Type=STRING
Profile=OUT

[Extreme-Login-Service]
Type=INTEGER
Profile=OUT
Enums=Login-Source

[Login-Source]
16=HTTP
32=SSH
64=Telnet
128=Console
240=All
```

FreeRADIUS Server

The following provides the necessary information to create a dictionary file that includes all the supported vendor-specific attributes for FreeRADIUS Server. The provided text can be copied into a file named **dictionary.symbol**.

```
#
# Summit WM Controller Dictionary File for FreeRADIUS
# Last Updated: July 21st 2010
# Created By: mgutierrez@extremenetworks.com
#

VENDOR         Symbol        1916

ATTRIBUTE      Extreme-Service-Type         1              integer       Symbol
VALUE          Extreme-Service-Type         Monitor        1
VALUE          Extreme-Service-Type         Helpdesk       2
VALUE          Extreme-Service-Type         NetworkAdmin   4
VALUE          Extreme-Service-Type         SysAdmin       8
VALUE          Extreme-Service-Type         WebAdmin       16
VALUE          Extreme-Service-Type         SuperUser      32768

ATTRIBUTE      Extreme-Current-SSID         2              string        Symbol
ATTRIBUTE      Extr_Wlan_Allowed_SSID              3              string        Symbol
ATTRIBUTE      Extreme-Wlan-Index           4              integer       Symbol
ATTRIBUTE      Extr_Wlan_QoS_Profile        5              integer       Symbol
ATTRIBUTE      Extr_Wlan_Allowed_Radio             6              string        Symbol
ATTRIBUTE      Guest-User-Expiry-Date-Time  7              string        Symbol
ATTRIBUTE      Guest-User-Start-Date-Time          8              string        Symbol
ATTRIBUTE      Extr_MU_Posture_Status              9              string        Symbol
ATTRIBUTE      Extreme-Downlink-Limit-Kbps         10             integer       Symbol
ATTRIBUTE      Extreme-Uplink-Limit-Kbps           11             integer       Symbol
ATTRIBUTE      Extreme-User-Group           12             string        Symbol

ATTRIBUTE      Extreme-Login-Service        100            integer       Symbol
VALUE          Extreme-Login-Service        HTTP           16
VALUE          Extreme-Login-Service        SSH            32
VALUE          Extreme-Login-Service        Telnet         64
VALUE          Extreme-Login-Service        Console        128
VALUE          Extreme-Login-Service        All            240
```

OSC Radiator RADIUS Server

The following provides the necessary information to create a dictionary file that includes all the supported vendor specific attributes for OSC Radiator RADIUS Server. The provided text can be copied into the main Radiator dictionary file.

```
#
# Summit WM Controller Dictionary File for Radiator
# Last Updated: July 21st 2010
# Created By: mgutierrez@extremenetworks.com
#

VENDORATTR     1916   Extreme-Service-Type  1              integer
VALUE          Extreme-Service-Type                Monitor        1
VALUE          Extreme-Service-Type                HelpDesk       2
VALUE          Extreme-Service-Type                NetworkAdmin   4
VALUE          Extreme-Service-Type                SystemAdmin    8
VALUE          Extreme-Service-Type                WebAdmin       16
VALUE          Extreme-Service-Type                SuperUser      32768

VENDORATTR     1916   Extreme-Current-SSID         2        string
VENDORATTR     1916   Extr_Wlan_Allowed_SSID               3       string
VENDORATTR     1916   Extreme-Wlan-Index           4        integer
VENDORATTR     1916   Extr_Wlan_QoS_Profile        5        integer
VENDORATTR     1916   Extr_Wlan_Allowed_Radio              6       string
VENDORATTR     1916   Guest-User-Expiry-Date-Time  7        string
VENDORATTR     1916   Guest-User-Start-Date-Time           8       string
VENDORATTR     1916   Extr_MU_Posture_Status               9       string
VENDORATTR     1916   Extreme-Downlink-Limit-Kbps          10      integer
VENDORATTR     1916   Extreme-Uplink-Limit-Kbps            11      integer
VENDORATTR     1916   Extreme-User-Group           12       string

VENDORATTR     1916   Extreme-Login-Service 100            integer
VALUE          Extreme-Login-Service        HTTP           16
VALUE          Extreme-Login-Service        SSH            32
VALUE          Extreme-Login-Service        Telnet         64
VALUE          Extreme-Login-Service        Console        128
VALUE          Extreme-Login-Service        All            240
```

Juniper Networks Steel-Belted RADIUS Server

The following provides the necessary information to create a dictionary file that includes all the supported vendor specific attributes for Juniper Networks Steel-Belted RADIUS Server. The provided text can be copied into a file named **symbol.dct**.

```
#
# Summit WM Controller Dictionary File for Steel Belted RADIUS
# Last Updated: July 21st 2010
# Created By: mgutierrez@extremenetworks.com
#
@radius.dct

MACRO  Symbol-VSA(type,syntax)       26     [vid=1916 type1=%type% len1=+2 data=%syntax%]

ATTRIBUTE      Extreme-Service-Type         Symbol-VSA(1, integer) R
VALUE          Extreme-Service-Type         Monitor        1
VALUE          Extreme-Service-Type         Helpdesk       2
VALUE          Extreme-Service-Type         NetworkAdmin   4
VALUE          Extreme-Service-Type         SystemAdmin    8
VALUE          Extreme-Service-Type         WebAdmin       16
VALUE          Extreme-Service-Type         SuperUser      32768

ATTRIBUTE      Extreme-Current-SSID         Symbol-VSA(2, string) C
ATTRIBUTE      Extr_Wlan_Allowed_SSID              Symbol-VSA(3, string) R
ATTRIBUTE      Extreme-Wlan-Index           Symbol-VSA(4, integer) C
ATTRIBUTE      Extr_Wlan_QoS_Profile        Symbol-VSA(5, integer) C
ATTRIBUTE      Extr_Wlan_Allowed_Radio             Symbol-VSA(6, string) R
ATTRIBUTE      Guest-User-Expiry-Date-Time  Symbol-VSA(7, string) R
ATTRIBUTE      Guest-User-Start-Date-Time          Symbol-VSA(8, string) R
ATTRIBUTE      Extr_MU_Posture_Status              Symbol-VSA(9, string) R
ATTRIBUTE      Extreme-Downlink-Limit-Kbps         Symbol-VSA(10, integer) R
ATTRIBUTE      Extreme-Uplink-Limit-Kbps           Symbol-VSA(11, integer) R
ATTRIBUTE      Extreme-User-Group           Symbol-VSA(12, string) R

ATTRIBUTE      Extreme-Login-Service        Symbol-VSA(100, integer) R
VALUE          Extreme-Login-Service        HTTP           16
VALUE          Extreme-Login-Service        SSH            32
VALUE          Extreme-Login-Service        Telnet         64
VALUE          Extreme-Login-Service        Console        128
VALUE          Extreme-Login-Service        All            240
```

Reference Documentation

Description	Location
Summit WM3000 Series Controller System Reference Guide	http://www.extremenetworks.com/services/software-userguide.aspx
Summit WM3000 Series Controller CLI Reference Guide	http://www.extremenetworks.com/services/software-userguide.aspx

www.extremenetworks.com

Corporate
and North America
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa
and South America
Phone +31 30 800 5100

Asia Pacific
Phone +65 6836 5437

Japan
Phone +81 3 5842 4011