



WiNG 4.X / WiNG 5.X RADIUS Attributes

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office.

Symbol is a registered trademark of Symbol Technologies, Inc. All other product or service names are the property of their respective owners.

© 2011 Motorola Solutions, Inc. All rights reserved.

Table of Contents:

1. Overview	4
1.1 IETF Standard Attributes.....	5
1.2 Motorola Vendor-Specific Attributes	7
2. RADIUS Accounting Attributes	14
3. Dynamic Authorization Extensions	18
4. RADIUS Dictionary Files	19
4.1 Cisco Secure Access Control Server.....	19
4.2 FreeRADIUS	21
4.3 Radiator	22
4.4 Steel Belted RADIUS	23
5. Microsoft RADIUS Servers	25
5.1 Microsoft Internet Authentication Service	26
5.2 Microsoft Network Policy Server	36

1. Overview

The RADIUS protocol follows client-server architecture and uses the User Datagram Protocol (UDP) as described in RFC 2865. A Wireless Controller or Access Point sends user information to the RADIUS server in an Access-Request message and after receiving a reply from the server acts according to the returned information.

The RADIUS server receives user requests for access from the client, attempts to authenticate the user, and returns the configuration information and policies to the client. The RADIUS server may be configured to authenticate an Access-Request locally or against an external user store such as SQL, Kerberos, LDAP or Active Directory.

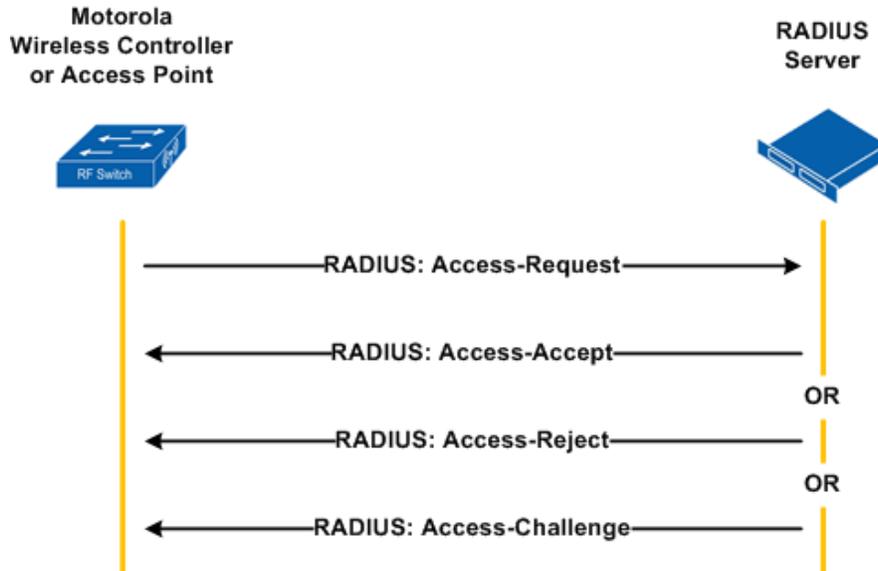


Figure 1.0 – RADIUS Authentication & Authorization

During authentication the RADIUS server then returns one of three responses to the Wireless Controller or Access Point:

- 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 Wireless Controller or Access Point 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 optionally enabled for MAC based authentication.

1.1 IETF Standard Attributes

The following table outlines the standard authentication attributes that have been implemented in WiNG 4.X and WiNG 5.X in accordance to RFC 2865. Additional extensions have also been implemented following the recommendations in RFC 2868 and RFC 2869.

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	The <i>User-Name</i> attribute is forwarded in the <i>Access-Request</i> and indicates the name of the user to be authenticated.
User-Password	2	RFC 2865	The <i>User-Password</i> attribute is forwarded in the <i>Access-Request</i> and indicates the password of the user to be authenticated, or the user's input following an <i>Access-Challenge</i> .
CHAP-Password	3	RFC 2865	The <i>CHAP-Password</i> attribute is forwarded in the <i>Access-Request</i> and indicates the PPP Challenge-Handshake Authentication Protocol (CHAP) response to a challenge.
NAS-IP-Address	4	RFC 2865	The <i>NAS-IP-Address</i> attribute is forwarded in the <i>Access-Request</i> and indicates the IP Address of the Wireless Controller or Access Point requesting user authentication.
NAS-Port	5	RFC 2865	The <i>NAS-Port</i> attribute is forwarded in the <i>Access-Request</i> and indicates the association index of the user on the Wireless Controller or Access Point.
Service-Type	6	RFC 2865	The <i>Service-Type</i> attribute is forwarded in the <i>Access-Request</i> and indicates the type of service the user has requested, or the type of service to be provided. The attribute value is always set to <i>Framed-User</i> by the Wireless Controller or Access Point.
Framed-MTU	12	RFC 2865	The <i>Framed-MTU</i> attribute is forwarded in the <i>Access-Request</i> and indicates the Maximum Transmission Unit (MTU) to be configured for the user. The attribute value is always set to <i>1400</i> by the Wireless Controller or Access Point.
State	24	RFC 2865	The <i>State</i> attribute is available to be forwarded in the <i>Access-Challenge</i> and must be sent unmodified from the client to the server in the <i>Access-Request</i> reply to that challenge, if any.
Called-Station-Id	30	RFC 2865	The <i>Called-Station-Id</i> attribute is forwarded in the <i>Access-Request</i> and indicates the BSSID and ESSID that the authenticating user is associated with. The Wireless Controller or Access Point will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX:ESSID</i> .
Calling-Station-Id	31	RFC 2865	The <i>Calling-Station-Id</i> attribute is forwarded in the <i>Access-Request</i> and indicates the MAC address of the authenticating user. It is only used in <i>Access-Request</i> packets. The Wireless Controller or Access Point will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX</i> .
NAS-Identifier	32	RFC 2865	The <i>NAS-Identifier</i> attribute is forwarded in the <i>Access-Request</i> and indicates the hostname or user defined identifier of the Wireless Controller or Access Point.

CHAP-Challenge	60	RFC 2865	The <i>CHAP-Challenge</i> attribute is forwarded in the <i>Access-Request</i> and indicates the CHAP Challenge sent by the Wireless Controller or Access Point to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.
NAS-Port-Type	61	RFC 2865	The <i>NAS-Port-Type</i> attribute is forwarded in the <i>Access-Request</i> and indicates the type of physical connection for the authenticating the user. The attribute value is always set to <i>Wireless-802.11</i> by the Wireless Controller or Access Point.
Connection-Info	77	RFC 2869	The <i>Connection-Info</i> attribute is forwarded in the <i>Access-Request</i> and indicates the data-rate and radio type of the authenticating user. The Wireless Controller or Access Point will forward the attribute value using the following formatting: <i>CONNECT XXMbps 802.11X</i> .
NAS-Port-Id	87	RFC 2869	The <i>NAS-Port-Id</i> attribute is forwarded in the <i>Access-Request</i> and indicates the ESSID that the authenticating user is associated with.
CHAP-Challenge	60	RFC 2865	The <i>CHAP-Challenge</i> attribute is forwarded in the <i>Access-Request</i> and contains the CHAP Challenge sent by the Wireless Controller or Access Point to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.
EAP-Message	79	RFC 2869	The <i>EAP-Message</i> attribute is forwarded in the <i>Access-Request</i> , <i>Access-Challenge</i> , <i>Access-Accept</i> and <i>Access-Reject</i> and encapsulates Extended Access Protocol (EAP) packets.
Message-Authenticator	80	RFC 2869	The <i>Message-Authenticator</i> attribute is forwarded in the <i>Access-Request</i> and may be used to prevent spoofing of CHAP, ARAP or EAP Access-Request packets.
Tunnel-Private-Group-ID	81	RFC 2868	The <i>Tunnel-Private-Group-ID</i> attribute is forwarded in the <i>Access-Accept</i> and indicates the numerical VLAN ID to be assigned to the authenticating user. The attribute value must be set to a numerical value between 1 and 4094.

Table 1.1 – IETF Standard Authentication Attributes

1.1.1 Tunnel-Private-Group-ID

The *Tunnel-Private-Group-ID* attribute maybe forwarded in the *Access-Accept* to indicate the dynamic VLAN membership of an 802.1X or RADIUS MAC authenticated user.

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

Table 1.1.1 – Attribute Details



Note – The VLAN value returned from the RADIUS server will override any static VLAN(s) defined in a WLAN profile.

1.2 Motorola Vendor-Specific Attributes

The following table outlines the Motorola vendor-specific attributes (VSAs) authentication attributes that have been implemented in WiNG 4.X and WiNG 5.X in accordance to RFC 2865.

Attribute Name	Type	Vendor ID	Attribute Number	Formatting
Symbol-Admin-Role	26	388	1	Integer
Symbol-Current-ESSID	26	388	2	String
Symbol-Allowed-ESSID	26	388	3	String
Symbol-WLAN-Index	26	388	4	Integer
Symbol-QoS-Profile	26	388	5	Integer
Symbol-Allowed-Radio	26	388	6	String
Symbol-Expiry-Date-Time	26	388	7	String
Symbol-Start-Date-Time	26	388	8	String
Symbol-Posture-Status	26	388	9	String
Symbol-Downlink-Limit	26	388	10	String
Symbol-Uplink-Limit	26	388	11	Integer
Symbol-User-Group	26	388	12	String
Symbol-Login-Source	26	388	100	Integer

Table 1.2 – Motorola Vendor Specific Attributes

1.2.1 Symbol-Admin-Role

The *Symbol-Admin-Role* attribute maybe forwarded in a *Access-Accept* and indicates the permissions a remote access user is granted on an Wireless Controller or Access Point when RADIUS management user authentication is enabled.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Admin-Role	388	1	Integer
Integer Value	Associated Roles	Description	
1	Monitor	The Monitor role is assigned to personnel requiring read-only access to a Wireless Controller or Access Point.	
2	Help Desk	The Help Desk role is assigned to personnel responsible for troubleshooting tasks. The Help Desk role can clear statistics, reboot devices and create or copy tech support files when working with Motorola Solutions technical support.	
4	Network	The Network role is assigned to personnel responsible for configuration of wired and wireless parameters such as Layer 2, Layer 3, Wireless, RADIUS, DHCP and Smart-RF.	
8	System	The System role is assigned to personnel responsible for configuring general switch settings such as upgrading images, changing boot partitions, time and administrative access.	
16	Web User	The Web User role is assigned to non-skilled personnel responsible for adding guest user accounts for Captive Portal authentication.	
32	Security	The Security role is assigned to personnel responsible for changing Wireless LAN keys.	
32768	Superuser	The Superuser role is assigned to personnel requiring full administrative privileges.	

Table 1.2.1 – Symbol-Admin-Role Attribute Details



Note – The Security role is only available in WiNG 5.1 and above.



Note – The Symbol-Admin-Role attribute can be used to assign one or more management roles to a user. When multiple roles are assigned, multiple Symbol-Admin-Role attributes and values must be returned to the Wireless Controller or Access Point.

1.2.2 Symbol-Current-ESSID

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

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Current-ESSID	388	2	String
Format: <i>ESSID-Name</i>			
Example: <i>Hotspot</i>			

Table 1.2.2 – Attribute Details

1.2.3 Symbol-Allowed-ESSID

The *Symbol-Allowed-ESSID* attribute maybe forwarded in the *Access-Accept* and indicates one or more ESSIDs that the user is permitted to associate with.

During authorization the Wireless Controller or Access Point will check the returned ESSID(s) against the current ESSID the authenticating user is associated with. If the returned ESSID(s) match the user is permitted access. If the returned ESSID(s) do not match the user will be denied access.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Allowed-ESSID	388	3	String
Format: <i>ESSID-Name</i>			
Example: <i>Sales</i>			

Table 1.2.3 – Attribute Details



Note – The *Symbol-Allowed-ESSID* attribute can be used to permit access to one or more ESSIDs. When multiple ESSIDs are permitted multiple *Symbol-Allowed-ESSID* attributes and values must be returned to the Wireless Controller or Access Point.

1.2.4 Symbol-WLAN-Index

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

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-WLAN-Index	388	4	Integer
Format: <i>Index-Number</i>			
Example: 2			

Table 1.2.4 – Attribute Details



Note – The *Symbol-WLAN-Index* has been depreciated in WiNG 5.X. Restricting users to specific ESSIDs can be achieved using the *Symbol-Allowed-ESSID* attribute.

1.2.5 Symbol-QoS-Profile

The *Symbol-QoS-Profile* attribute maybe 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 Name	Vendor ID	Attribute Number	Attribute Format
Symbol-QoS-Profile	388	5	Integer
Supported Values: 4 (<i>Voice</i>), 3 (<i>Video</i>), 2 (<i>Background</i>), 1 (<i>Best Effort</i>)			
Example: 1			

Table 1.2.5 – Attribute Details

1.2.6 Symbol-Allowed-Radio

The *Symbol-Allowed-Radio* attribute maybe forwarded in the *Access-Accept* and indicates one or more radios that the authenticating user is permitted to associate with.

The *Symbol-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 Wireless Controller or Access Point will only permit access to radios with *1st-Floor* defined in the description field such as *1st-Floor-Conference-Room*, *1st-Floor-Cafateria* etc. The user in this example would be denied access to radios with the description *2nd-Floor-Conference-Room* or *AP650-1*.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Allowed-Radio	388	6	String
Format: <i>Radio-Description-Filter</i>			
Example: <i>1st-Floor</i>			

Table 1.2.6 – Attribute Details

1.2.7 Symbol-Expiry-Date-Time

The *Symbol-Expiry-Date-Time* attribute maybe forwarded in the *Access-Accept* and indicates the date and time the authenticating user is no longer authorized to access the network.

During authorization the Wireless Controller or Access Point will check the returned date and time values against the current date and time on the Wireless Controller or Access Point. If the returned date and time is before the current date and time on the Wireless Controller or Access Point the user will be permitted access. If the returned date and time is after the current date and time on the Wireless Controller or Access Point the user will be denied access.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Expiry-Date-Time	388	7	String
Format: <i>MMDD/YYYY-HH:MM</i>			
Example: <i>01/02/2009-17:00</i>			

Table 1.2.7 – Attribute Details

1.2.8 Symbol-Start-Date-Time

The *Symbol-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 Wireless Controller or Access Point will check the returned date and time values against the current date and time on the Wireless Controller or Access Point. If the returned date and time is after the current date and time on the Wireless Controller or Access Point the user will be permitted access. If the returned date and time is before than the current date and time on the Wireless Controller or Access Point the user will be denied access.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Start-Date-Time	388	8	String
Format: <i>MM/DD/YYYY-HH:MM</i>			
Example: <i>01/01/2009-08:00</i>			

Table 1.2.8 – Attribute Details

1.2.9 Symbol-Posture-Status

The *Symbol-Posture-Status* attribute maybe 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 Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Posture-Status	388	9	String

Table 1.2.9 – Attribute Details

1.2.10 Symbol-Downlink-Limit

The *Symbol-Downlink-Limit* attribute maybe forwarded in the *Access-Accept* and indicates the amount of bandwidth in Kbps that the authenticating user is permitted to receive from the AP. Traffic that exceeds the defined value will be dropped by the Wireless Controller or Access Point.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Downlink-Limit	388	10	Integer
Format: <i>0, 100-10,000 (0 = Disabled)</i>			
Example: <i>768</i>			

Table 1.2.10 – Attribute Details

1.2.11 Symbol-Uplink-Limit

The *Symbol-Uplink-Limit* attribute maybe forwarded in the *Access-Accept* and indicates the amount of bandwidth in Kbps that the authenticating user is permitted to transmit to the AP. Traffic that exceeds the defined value will be dropped by the Wireless Controller or Access Point.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Uplink-Limit	388	11	Integer
Format: 0, 100-10,000 (0 = Disabled)			
Example: 512			

Table 1.2.11 – Attribute Details

1.2.12 Symbol-User-Group

The *Symbol-User-Group* attribute maybe forwarded in the *Access-Accept* and indicates the group on the Wireless Controller or Access Point that the authenticating user is to be associated with. The *Symbol-User-Group* attribute is used by the role base firewall to dynamically assign firewall policies to users based on group membership.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-User-Group	388	12	String
Format: <i>Group-Name</i>			
Example: <i>Sales</i>			

Table 1.2.12 – Attribute Details

1.2.13 Symbol-Login-Source

The *Symbol-Login-Source* attribute maybe forwarded in the *Access-Accept* and indicates the management interfaces the user is permitted to access on the Wireless Controller or Access Point when RADIUS management user authentication is enabled.

During authorization the Wireless Controller or Access Point will check the returned list of permitted interfaces against the current interface the user is authenticating through. If the interface is permitted the user will be permitted access to the Wireless Controller or Access Point. If the interface is not permitted the user will be denied access to the Wireless Controller or Access Point.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Login-Source	388	100	Integer

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

Table 1.2.13 – Attribute Details



Note – The *Symbol-Login-Source* attribute can be used to permit access to one or more management interfaces or all management interfaces. When multiple interfaces are assigned, multiple *Symbol-Login-Source* attributes and values must be returned to the Wireless Controller or Access Point.

2. 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 statistic for general network monitoring.

When network access is granted to the user by the Wireless Controller or Access Point, an Accounting-Request message with the Acct-Status-Type field set to Start is forwarded by the Wireless Controller or Access Point to the RADIUS server to signal the start of the user's network access. Start records typically contain the user's identification, network address, point of attachment and a unique session identifier.

Optionally periodic Accounting-Request messages with the Acct-Status-Type field set to Interim Update may be sent by the Wireless Controller or Access Point to the RADIUS server to update it on the status of an active session. Interim records typically convey the current session duration and information on current data usage.

When the user's session is closed, the Wireless Controller or Access Point forwards an Accounting-Request message with the Acct-Status-Type field set to Stop. This provides information on the final usage in terms of time, packets transferred, data transferred and reason for disconnect and other information related to the user's network access.

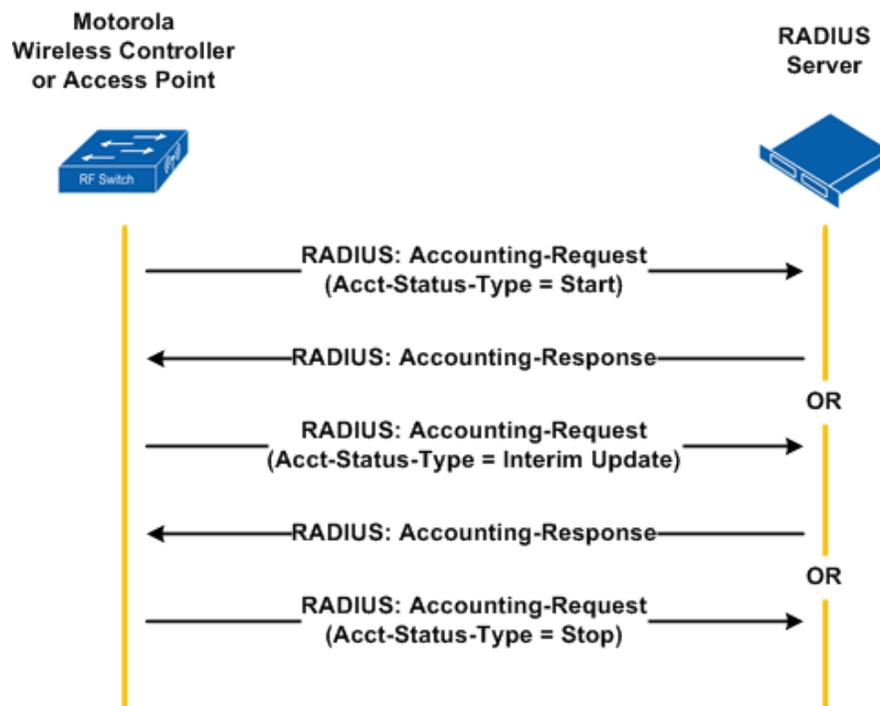


Figure 2.0 – RADIUS Accounting

RADIUS Accounting can be enabled / disabled on the Wireless Controller or Access Point for each WLAN profile and administrators can select how the Wireless Controller or Access Point forwards accounting information to the RADIUS server. For each WLAN profile the following accounting configuration is supported:

- 1) Start-Stop – The Wireless Controller or Access Point will forward Accounting-Requests at the start and end of the user sessions.
- 2) Stop-Only – The Wireless Controller or Access Point will forward Accounting-Requests at the end of the user sessions.
- 3) Start-Interim-Stop – The Wireless Controller or Access Point will forward Accounting-Requests at the start and end of the user sessions as well as periodically during the lifetime of the sessions.

The following table outlines the standard RADIUS accounting attributes that have been implemented in WiNG 4.X and WiNG 5.X in accordance to RFC 2866:

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	The <i>User-Name</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the name of the user.
NAS-IP-Address	4	RFC 2865	The <i>NAS-IP-Address</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the IP Address of the Wireless Controller or Access Point.
NAS-Port	5	RFC 2865	The <i>NAS-Port</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the association index of the user on the Wireless Controller or Access Point.
Class	25	RFC 2865	The <i>Class</i> attribute is optionally forwarded in the <i>Access-Accept</i> and should be sent unmodified by the client to the accounting server as part of the <i>Accounting-Request</i> packet if accounting is supported.
Called-Station-Id	30	RFC 2865	The <i>Called-Station-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the BSSID and ESSID that the user is associated with. The Wireless Controller or Access Point will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX:ESSID</i> .
Calling-Station-Id	31	RFC 2865	The <i>Calling-Station-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the MAC address of the user. The Wireless Controller or Access Point will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX</i> .
NAS-Identifier	32	RFC 2865	The <i>NAS-Identifier</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the hostname or user defined identifier of the Wireless Controller or Access Point.
Acct-Status-Type	40	RFC 2866	The <i>Acct-Status-Type</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates whether the <i>Accounting-Request</i> marks the status of the accounting update. Supported values include <i>Start</i> , <i>Stop</i> and <i>Interim-Update</i> .
Acct-Delay-Time	41	RFC 2866	The <i>Acct-Delay-Time</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many seconds the Wireless Controller or Access Point 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 <i>Accounting-Request</i> .

Acct-Input-Octets	42	RFC 2866	The <i>Acct-Input-Octets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many octets have been received from the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Output-Octets	43	RFC 2866	The <i>Acct-Output-Octets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many octets have been forwarded to the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Session-Id	44	RFC 2866	The <i>Acct-Session-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and provides a unique identifier to make it easy to match <i>start</i> , <i>stop</i> and <i>interim</i> records in an accounting log file.
Account-Authentic	45	RFC 2866	The <i>Account-Authentic</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how the user was authenticated. When RADIUS accounting is enabled the Wireless Controller or Access Point will set this value to <i>RADIUS</i> .
Acct-Session-Time	46	RFC 2866	The <i>Acct-Session-Time</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many seconds the user has received service for. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Input-Packets	47	RFC 2866	The <i>Acct-Input-Packets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many packets have been received from the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Output-Packets	48	RFC 2866	The <i>Acct-Output-Packets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many packets have been forwarded to the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Terminate-Cause	49	RFC 2866	The <i>Acct-Terminate-Cause</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how the session was terminated. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Event-Timestamp	55	RFC 2869	The <i>Event-Timestamp</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the time that the accounting event occurred on the Wireless Controller or Access Point.
NAS-Port-Type	61	RFC 2865	The <i>NAS-Port-Type</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the type of physical connection for the user. This attribute value is always set to <i>Wireless-802.11</i> by the Wireless Controller or Access Point.

Tunnel-Type	64	RFC 2868	The <i>Tunnel-Type attribute</i> is forwarded in the <i>Accounting-Request</i> indicates the tunneling protocol(s) used by the user. This attribute value is always set to type 13 (<i>Virtual LANs</i>).
Tunnel-Medium-Type	65	RFC 2868	The <i>Tunnel-Medium-Type attribute</i> is forwarded in the <i>Accounting-Request</i> and indicates which transport medium used by the user. This attribute value is always set to type 6 (<i>802 includes all 802 media plus Ethernet "canonical format"</i>).
Tunnel-Private-Group-ID	81	RFC 2868	The <i>Tunnel-Private-Group-ID attribute</i> is forwarded in the <i>Accounting-Request</i> and 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	The <i>NAS-Port-Id attribute</i> is forwarded in the <i>Accounting-Request</i> and indicates the ESSID that the user is associated with.

Table 2.0 – IETF Standard Accounting Attributes

3. Dynamic Authorization Extensions

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

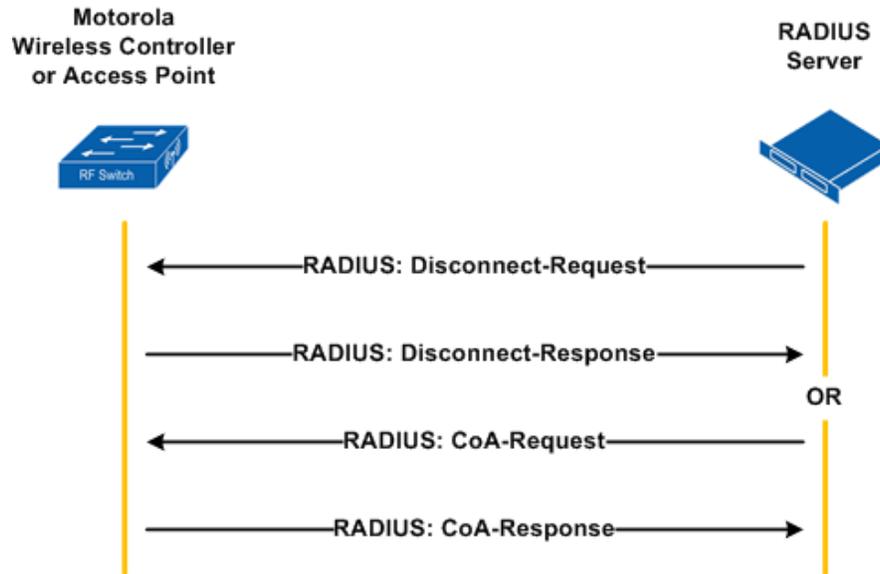


Figure 3.0 – Dynamic Authorization Extensions

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

Disconnect-Request – Causes a user session to be terminated. The Disconnect-Request packet identifies the NAS as well as the user session to be terminated by inclusion of the identification attributes shown in table 3.0.

CoA-Request – Causes session information to be dynamically updated on the Wireless Controller or Access Point. Currently a CoA-Request packet may only be used to change the session-timeout and the idle-timeout of a user.

The following table outlines the dynamic authorization extension attributes that have been implemented in WiNG 4.X and WiNG 5.X in accordance to RFC 3576.

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.

Table 3.0 – Dynamic Authorisation Extensions



Note – The Called-Station-Id, NAS-Identifier, NAS-IP-Address and Service-Type attributes are also evaluated by the Wireless Controller or Access Point if present.

4. RADIUS Dictionary Files

4.1 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.

```
;
; Motorola WiNG 4.X / WiNG 5.X File for Cisco Secure ACS
; Last Updated: August 2011
; Created By: kmarshall@motorolasolutions.com
;

[User Defined Vendor]
Name=SYMBOL
IETF Code=388
RadiusExtensionPoints=EAP

VSA 1=Symbol-Admin-Role
VSA 2=Symbol-Current-ESSID
VSA 3=Symbol-Allowed-ESSID
VSA 4=Symbol-WLAN-Index
VSA 5=Symbol-QoS-Profile
VSA 6=Symbol-Allowed-Radio
VSA 7=Symbol-Expiry-Date-Time
VSA 8=Symbol-Start-Date-Time
VSA 9=Symbol-Posture-Status
VSA 10=Symbol-Downlink-Limit
VSA 11=Symbol-Uplink-Limit
VSA 12=Symbol-User-Group
VSA 100=Symbol-Login-Source

[Symbol-Admin-Role]
Type=INTEGER
Profile=OUT
Enums=Admin-Role

[Admin-Role]
1=Monitor
2=Helpdesk
4=NetworkAdmin
8=SysAdmin
```

16=WebAdmin
32=Security
32768=SuperUser

[Symbol-Current-ESSID]
Type=STRING
Profile=IN

[Symbol-Allowed-ESSID]
Type=STRING
Profile=OUT

[Symbol-WLAN-Index]
Type=INTEGER
Profile=IN

[Symbol-QoS-Profile]
Type=INTEGER
Profile=IN

[Symbol-Allowed-Radio]
Type=STRING
Profile=OUT

[Symbol-Expiry-Date-Time]
Type=STRING
Profile=OUT

[Symbol-Start-Date-Time]
Type=STRING
Profile=OUT

[Symbol-Posture-Status]
Type=STRING
Profile=OUT

[Symbol-Downlink-Limit]
Type=INTEGER
Profile=OUT

[Symbol-Uplink-Limit]
Type=INTEGER

```

Profile=OUT

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

[Symbol-Login-Source]
Type=INTEGER
Profile=OUT
Enums=Login-Source

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

```

4.2 FreeRADIUS

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

```

#
# Motorola WiNG 4.X / WiNG 5.X Dictionary File for FreeRADIUS
# Last Updated: August 2011
# Created By: kmarshall@motorolasolutions.com
#

VENDOR          Symbol          388

ATTRIBUTE       Symbol-Admin-Role      1          integer      Symbol
VALUE           Symbol-Admin-Role      Monitor    1
VALUE           Symbol-Admin-Role      Helpdesk   2
VALUE           Symbol-Admin-Role      NetworkAdmin 4
VALUE           Symbol-Admin-Role      SysAdmin   8
VALUE           Symbol-Admin-Role      WebAdmin   16
VALUE           Symbol-Admin-Role      Security    32
VALUE           Symbol-Admin-Role      SuperUser  32768

ATTRIBUTE       Symbol-Current-ESSID   2          string       Symbol
ATTRIBUTE       Symbol-Allowed-ESSID   3          string       Symbol
ATTRIBUTE       Symbol-WLAN-Index      4          integer      Symbol

```

ATTRIBUTE	Symbol-QoS-Profile	5	integer	Symbol
ATTRIBUTE	Symbol-Allowed-Radio	6	string	Symbol
ATTRIBUTE	Symbol-Expiry-Date-Time	7	string	Symbol
ATTRIBUTE	Symbol-Start-Date-Time	8	string	Symbol
ATTRIBUTE	Symbol-Posture-Status	9	string	Symbol
ATTRIBUTE	Symbol-Downlink-Limit	10	integer	Symbol
ATTRIBUTE	Symbol-Uplink-Limit	11	integer	Symbol
ATTRIBUTE	Symbol-User-Group	12	string	Symbol
ATTRIBUTE	Symbol-Login-Source	100	integer	Symbol
VALUE	Symbol-Login-Source	HTTP	16	
VALUE	Symbol-Login-Source	SSH	32	
VALUE	Symbol-Login-Source	Telnet	64	
VALUE	Symbol-Login-Source	Console	128	
VALUE	Symbol-Login-Source	All	240	

4.3 Radiator

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

```
#
# Motorola WiNG 4.X / WiNG 5.X Dictionary File for Radiator
# Last Updated: August 2011
# Created By: kmarshall@motorolasolutions.com
#

VENDORATTR 388 Symbol-Admin-Role 1 integer
VALUE Symbol-Admin-Role Monitor 1
VALUE Symbol-Admin-Role HelpDesk 2
VALUE Symbol-Admin-Role NetworkAdmin 4
VALUE Symbol-Admin-Role SystemAdmin 8
VALUE Symbol-Admin-Role WebAdmin 16
VALUE Symbol-Admin-Role Security 32
VALUE Symbol-Admin-Role SuperUser 32768

VENDORATTR 388 Symbol-Current-ESSID 2 string
VENDORATTR 388 Symbol-Allowed-ESSID 3 string
VENDORATTR 388 Symbol-WLAN-Index 4 integer
VENDORATTR 388 Symbol-QoS-Profile 5 integer
VENDORATTR 388 Symbol-Allowed-Radio 6 string
VENDORATTR 388 Symbol-Expiry-Date-Time 7 string
VENDORATTR 388 Symbol-Start-Date-Time 8 string
```

VENDORATTR	388	Symbol-Posture-Status	9	string
VENDORATTR	388	Symbol-Downlink-Limit	10	integer
VENDORATTR	388	Symbol-Uplink-Limit	11	integer
VENDORATTR	388	Symbol-User-Group	12	string
VENDORATTR	388	Symbol-Login-Source	100	integer
VALUE		Symbol-Login-Source	HTTP	16
VALUE		Symbol-Login-Source	SSH	32
VALUE		Symbol-Login-Source	Telnet	64
VALUE		Symbol-Login-Source	Console	128
VALUE		Symbol-Login-Source	All	240

4.4 Steel Belted RADIUS

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

```
#
# Motorola WiNG 4.X / WiNG 5.X Dictionary File for Steel Belted RADIUS
# Last Updated: August 2011
# Created By: kmarshall@motorolasolutions.com
#
@radius.dct

MACRO    Symbol-VSA(type, syntax)          26    [vid=388 type1=%type% len1=+2 data=%syntax%]

ATTRIBUTE Symbol-Admin-Role              Symbol-VSA(1, integer) R
VALUE     Symbol-Admin-Role              Monitor          1
VALUE     Symbol-Admin-Role              Helpdesk        2
VALUE     Symbol-Admin-Role              NetworkAdmin    4
VALUE     Symbol-Admin-Role              SystemAdmin     8
VALUE     Symbol-Admin-Role              WebAdmin        16
VALUE     Symbol-Admin-Role              Security        32
VALUE     Symbol-Admin-Role              SuperUser       32768

ATTRIBUTE Symbol-Current-ESSID            Symbol-VSA(2, string) C
ATTRIBUTE Symbol-Allowed-ESSID           Symbol-VSA(3, string) R
ATTRIBUTE Symbol-WLAN-Index              Symbol-VSA(4, integer) C
ATTRIBUTE Symbol-QoS-Profile              Symbol-VSA(5, integer) C
ATTRIBUTE Symbol-Allowed-Radio            Symbol-VSA(6, string) R
ATTRIBUTE Symbol-Expiry-Date-Time         Symbol-VSA(7, string) R
ATTRIBUTE Symbol-Start-Date-Time         Symbol-VSA(8, string) R
ATTRIBUTE Symbol-Posture-Status           Symbol-VSA(9, string) R
```

ATTRIBUTE	Symbol-Downlink-Limit	Symbol-VSA(10, integer)	R
ATTRIBUTE	Symbol-Uplink-Limit	Symbol-VSA(11, integer)	R
ATTRIBUTE	Symbol-User-Group	Symbol-VSA(12, string)	R
ATTRIBUTE	Symbol-Login-Source	Symbol-VSA(100, integer)	R
VALUE	Symbol-Login-Source	HTTP	16
VALUE	Symbol-Login-Source	SSH	32
VALUE	Symbol-Login-Source	Telnet	64
VALUE	Symbol-Login-Source	Console	128
VALUE	Symbol-Login-Source	All	240

5. Microsoft RADIUS Servers

Microsoft Internet Authentication Service (IAS) and Network Policy Server (NPS) do not support dictionary files and require standard and vendor-specific return attributes to be manually added to policy. Standard and vendor-specific return attributes are assigned to users using Remote Access Policies in IAS and Network Policies in NPS.

Vendor ID	Attribute Name	Attribute Number	Attribute Format
388	Symbol-Admin-Role	1	Decimal
388	Symbol-Allowed-ESSID	3	String
388	Symbol-QoS-Profile	5	Decimal
388	Symbol-Allowed-Radio	6	String
388	Symbol-Expiry-Date-Time	7	String
388	Symbol-Start-Date-Time	8	String
388	Symbol-Downlink-Limit	10	Decimal
388	Symbol-Uplink-Limit	11	Decimal
388	Symbol-User-Group	12	String
388	Symbol-Login-Source	100	Decimal

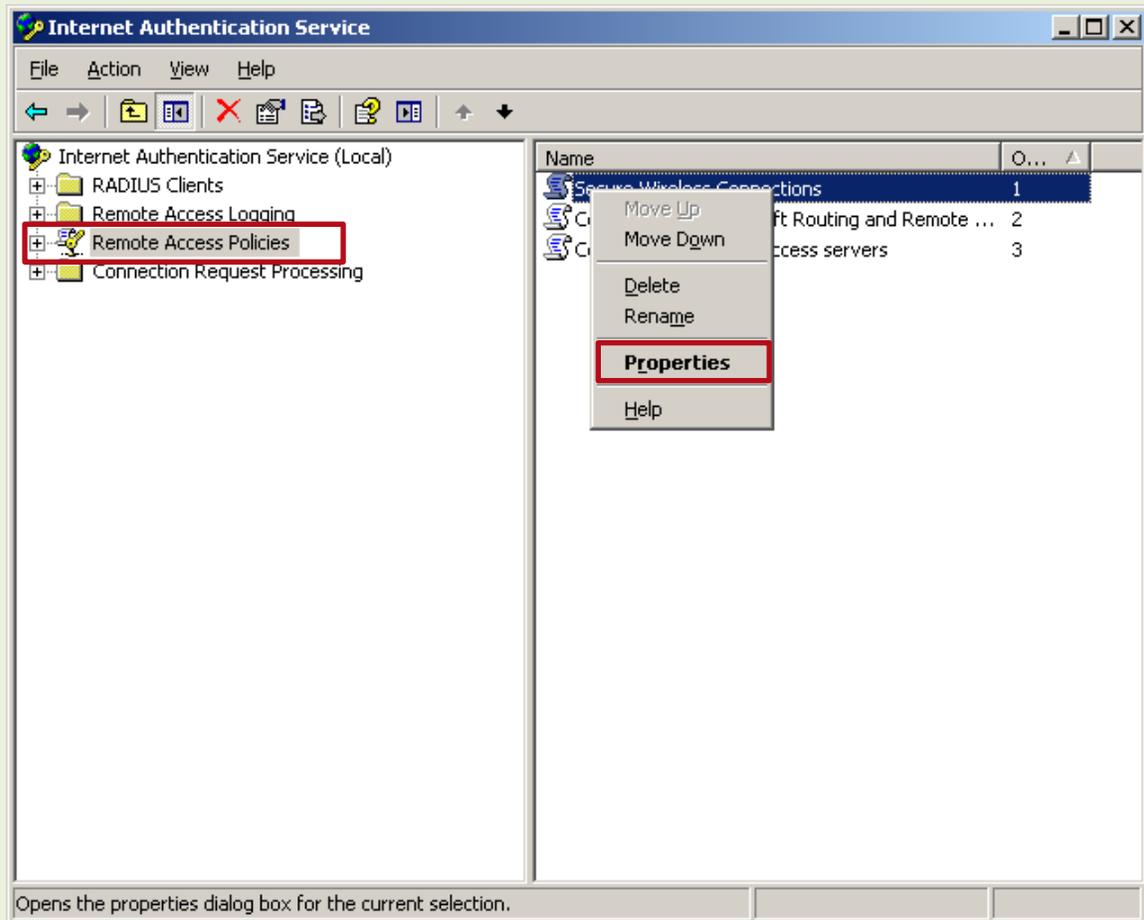
Table 5.0 – Motorola Attribute Formatting

5.1 Microsoft Internet Authentication Service

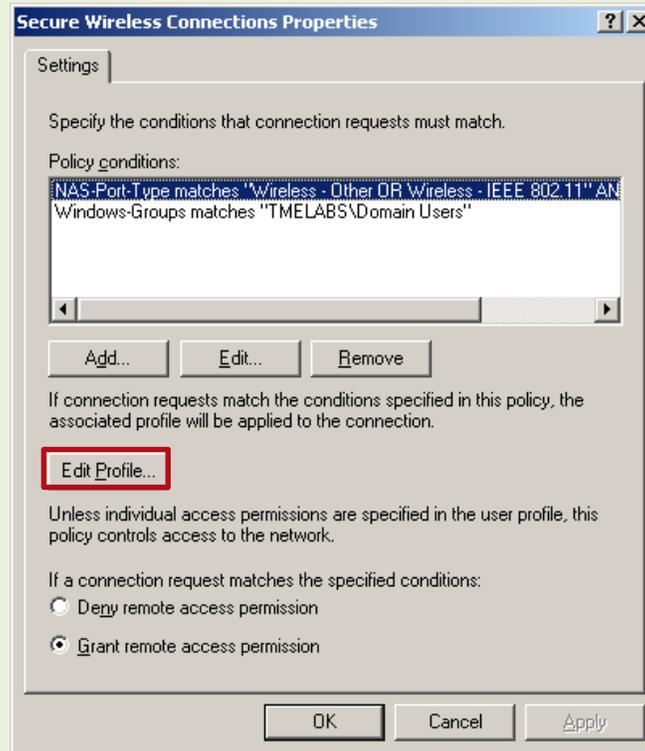
Use the following procedure to assign one or more Motorola vendor specific return attributes to a Remote Access Policy on Microsoft Internet Authentication Service.

5.1.1 Tunnel-Private-Group-ID Attribute (Dynamic VLANs)

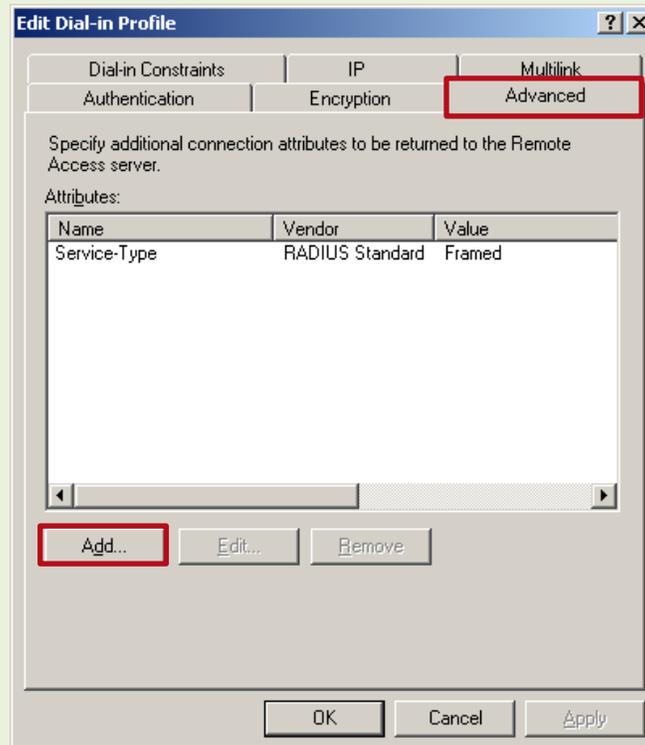
- 1 Open the *Internet Authentication Service* snap-in and select *Remote Access Policies*. Select the *Remote Access Policy* name to modify then right-click and select *Properties*:



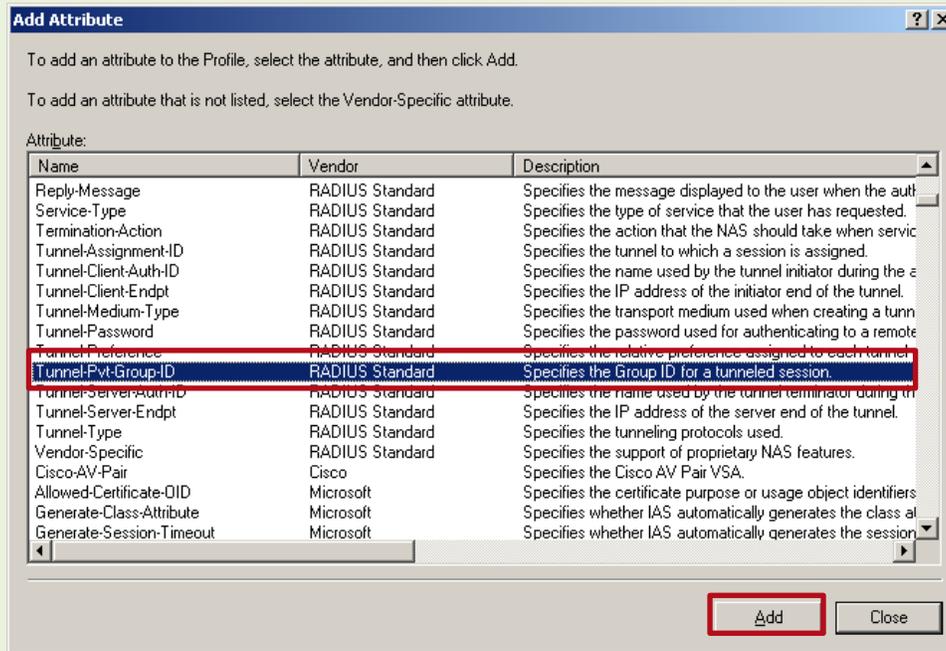
2 Select *Edit Profile*:



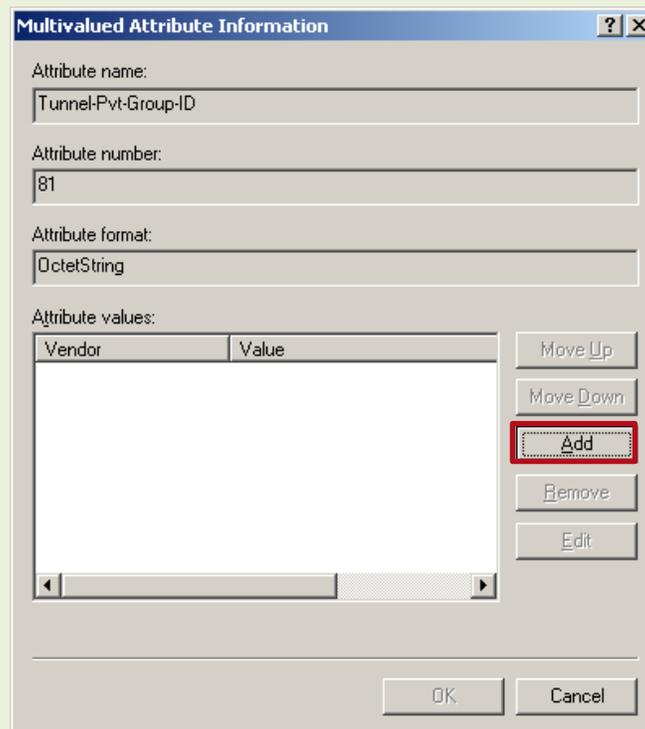
3 Select the *Advanced* tab then click *Add*:



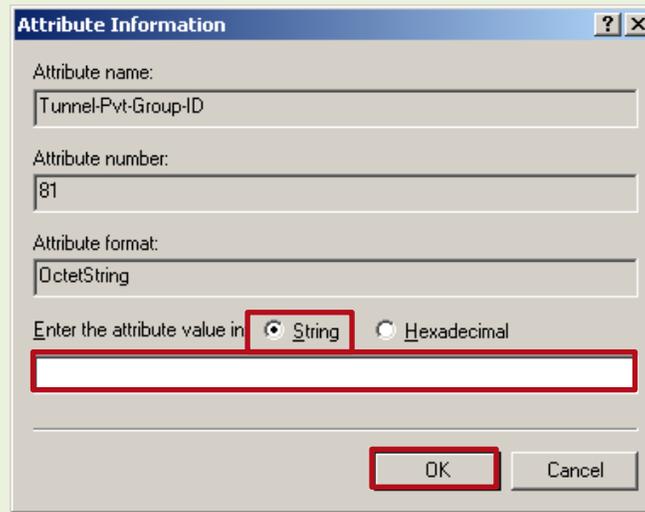
4 In the *Attribute* list select *Tunnel-Pvt-Group-Id* then click *Add*:



5 Click *Add*:



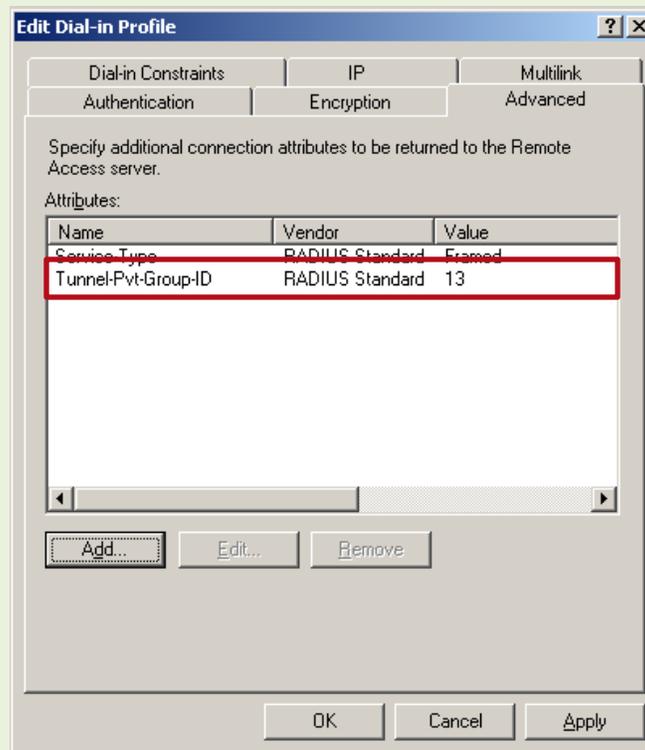
- 6 Select *String* then in the provided field enter the numerical *VLAN ID* (1 – 4094) to assign to users in the Remote Access Policy. Click *OK*:



The dialog box titled "Attribute Information" contains the following fields and options:

- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Enter the attribute value in: String Hexadecimal
- A text input field for the attribute value, currently empty.
- Buttons: OK, Cancel

- 7 In the following example the Remote Access Policy named *Secure Wireless Connections* will assign the VLAN ID 13 to authenticated and authorized users:



The dialog box titled "Edit Dial-in Profile" shows the "Advanced" tab with the following configuration:

- Specify additional connection attributes to be returned to the Remote Access server.
- Attributes table:

Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Tunnel-Pvt-Group-ID	RADIUS Standard	13

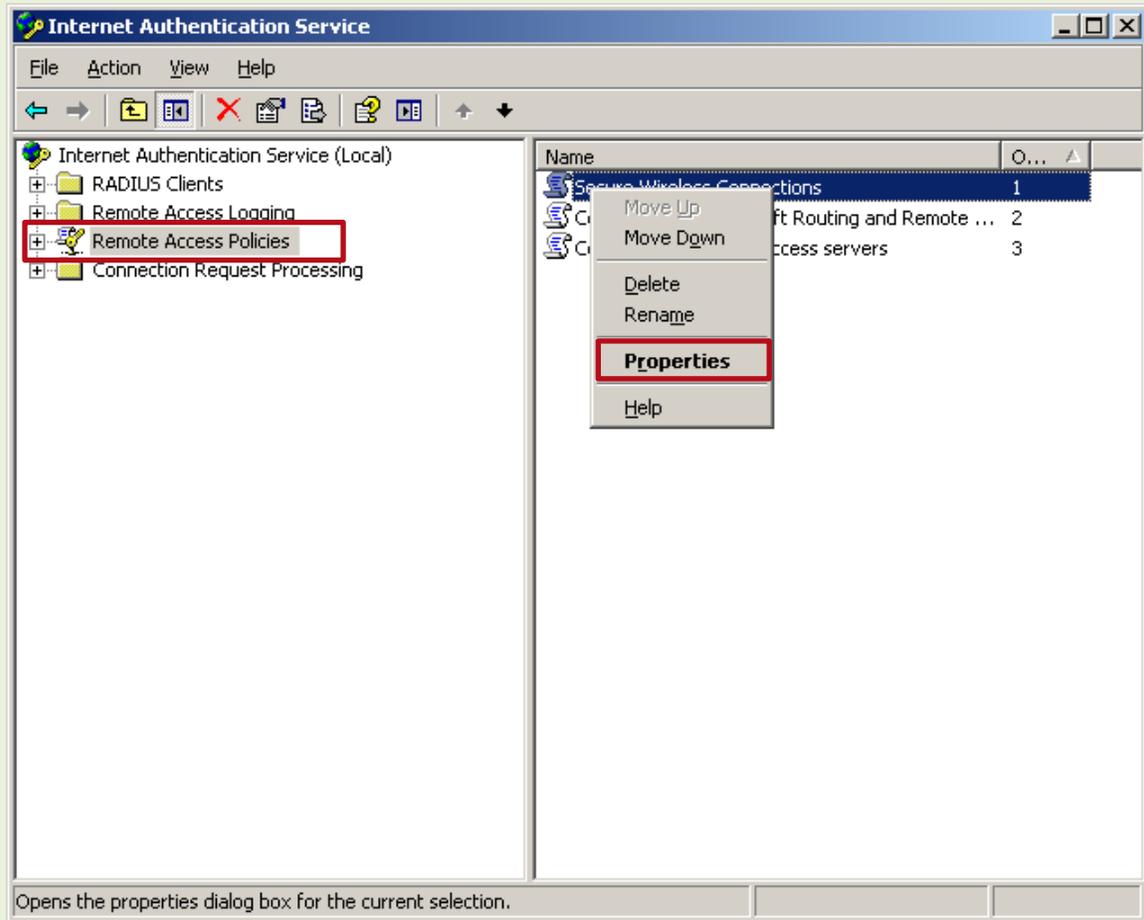
Buttons: Add..., Edit..., Remove, OK, Cancel, Apply



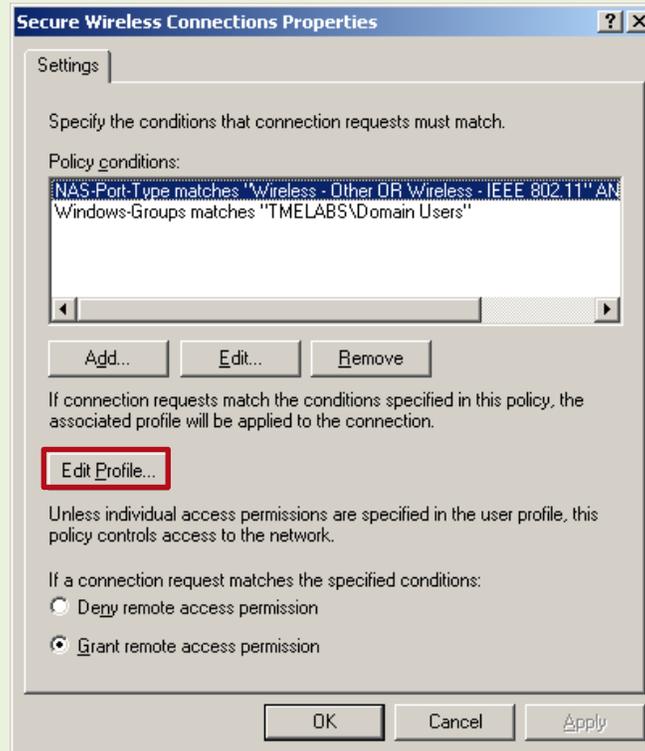
Note – Only one Tunnel-Private-Group-ID attribute and value is supported per Remote Access Policy.

5.1.2 Motorola Vendor-Specific Attributes

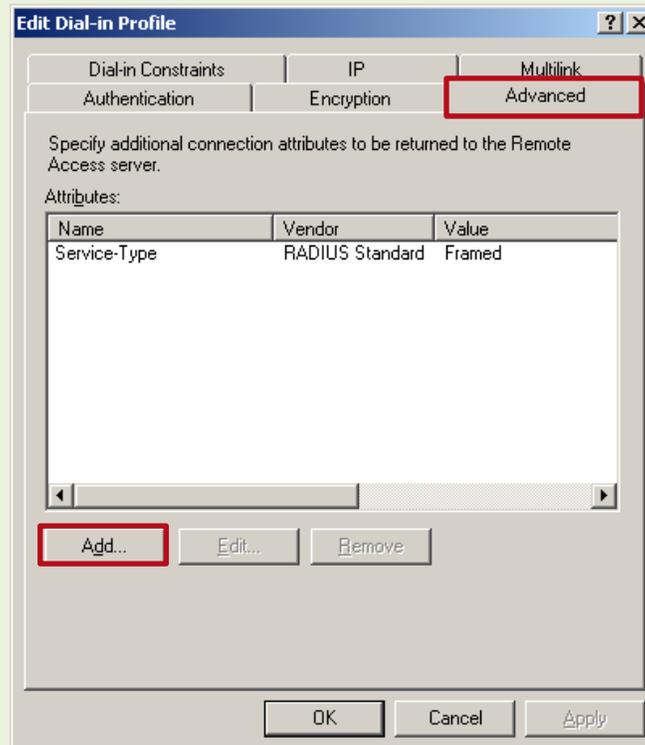
- 1 Open the *Internet Authentication Service* snap-in and select *Remote Access Policies*. Select the *Remote Access Policy* name to modify then right-click and select *Properties*:



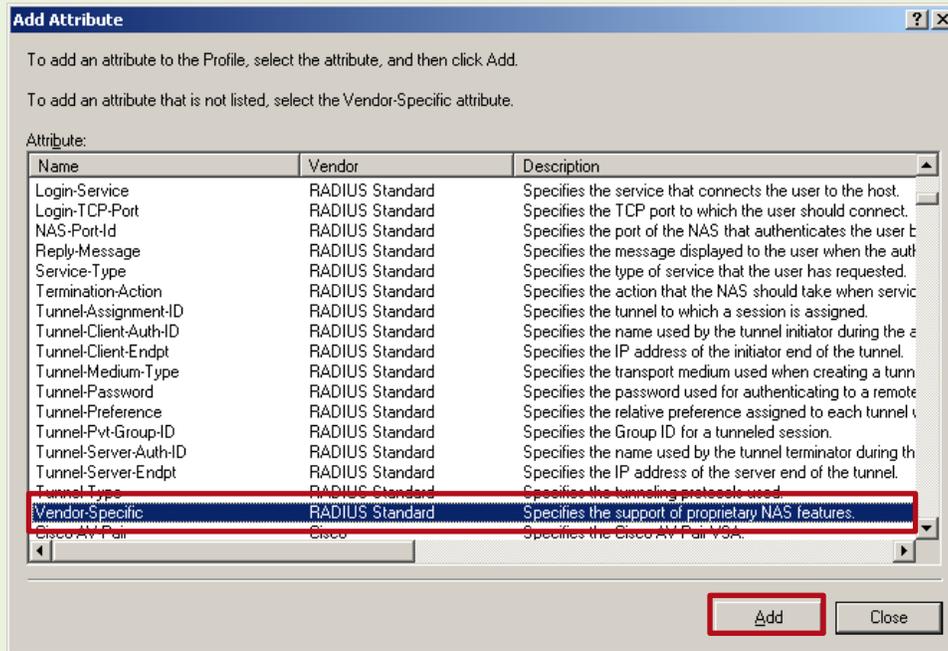
2 Select *Edit Profile*:



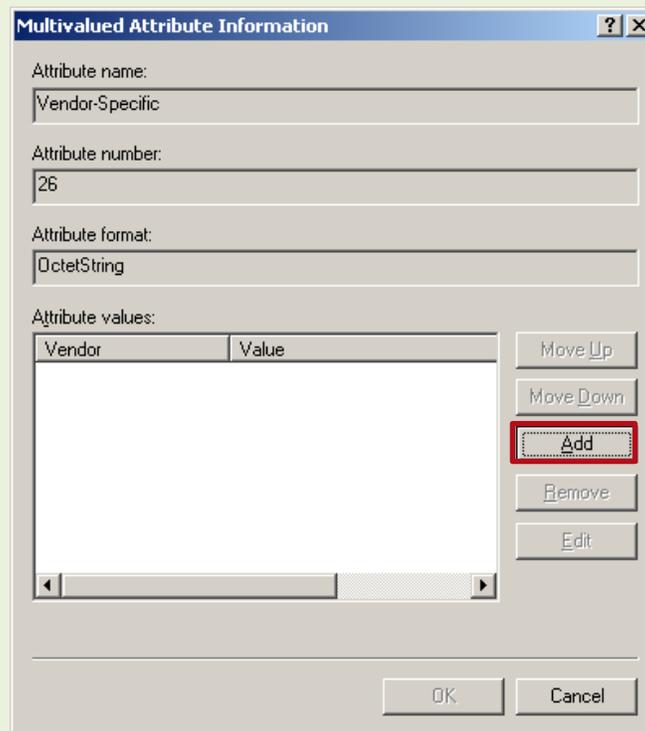
3 Select the *Advanced* tab then click *Add*:



4 In the *Attribute* list select *Vendor-Specific* then click *Add*:



5 Click *Add*:



6 In the *Enter Vendor Code* field type *388*. Select *Yes It conforms* then click *Configure Attribute*:

Vendor-Specific Attribute Information

Attribute name:
Vendor-Specific

Specify network access server vendor.

Select from list: RADIUS Standard

Enter Vendor Code: 388

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

Yes. It conforms.

No. It does not conform.

Configure Attribute...

OK Cancel

7 Using the provided examples below for each Motorola vendor specific return attribute, enter the desired *Vendor-assigned attribute number*, correct *Attribute format* and desired *Attribute value* then click *OK*:

Configure YSA (RFC compliant)

Vendor-assigned attribute number:
1

Attribute format:
Decimal

Attribute value:

OK Cancel

Attribute Example - Symbol-Admin-Role

Configure YSA (RFC compliant)

Vendor-assigned attribute number:
3

Attribute format:
String

Attribute value:

OK Cancel

Attribute Example - Symbol-Allowed-SSID

Configure VSA (RFC compliant) [?] [X]

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-QoS-Profile

Configure VSA (RFC compliant) [?] [X]

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Allowed-Radio

Configure VSA (RFC compliant) [?] [X]

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Expiry-Date-Time

Configure VSA (RFC compliant) [?] [X]

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Start-Date-Time

Configure VSA (RFC compliant) [?] [X]

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Downlink-Limit

Configure VSA (RFC compliant) [?] [X]

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Uplink-Limit

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
12

Attribute format:
String

Attribute value:
[Empty text box]

OK Cancel

Attribute Example - Symbol-User-Group

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
100

Attribute format:
Decimal

Attribute value:
[Empty text box]

OK Cancel

Attribute Example - Symbol-Login-Source

- 8 In the following example the Remote Access Policy named *Secure Wireless Connections* will restrict authenticated and authorized users to the ESSID named *MOTO-DOT1X* and will assign the users to a group called *Engineering*:

Edit Dial-in Profile

Dial-in Constraints | IP | Multilink
Authentication | Encryption | Advanced

Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Vendor-Specific	RADIUS Standard	MOTO-DOT1X, Engine

Add... Edit... Remove

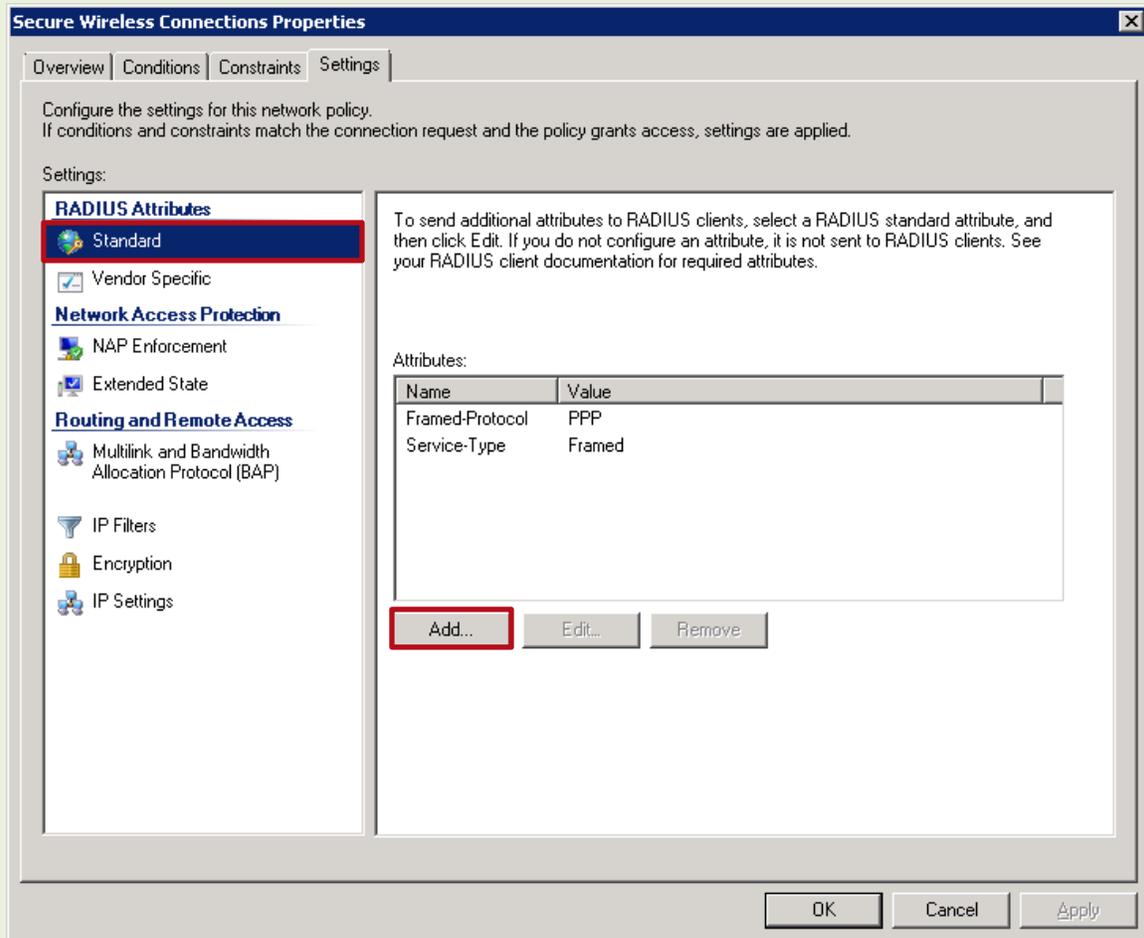
OK Cancel Apply

5.2 Microsoft Network Policy Server

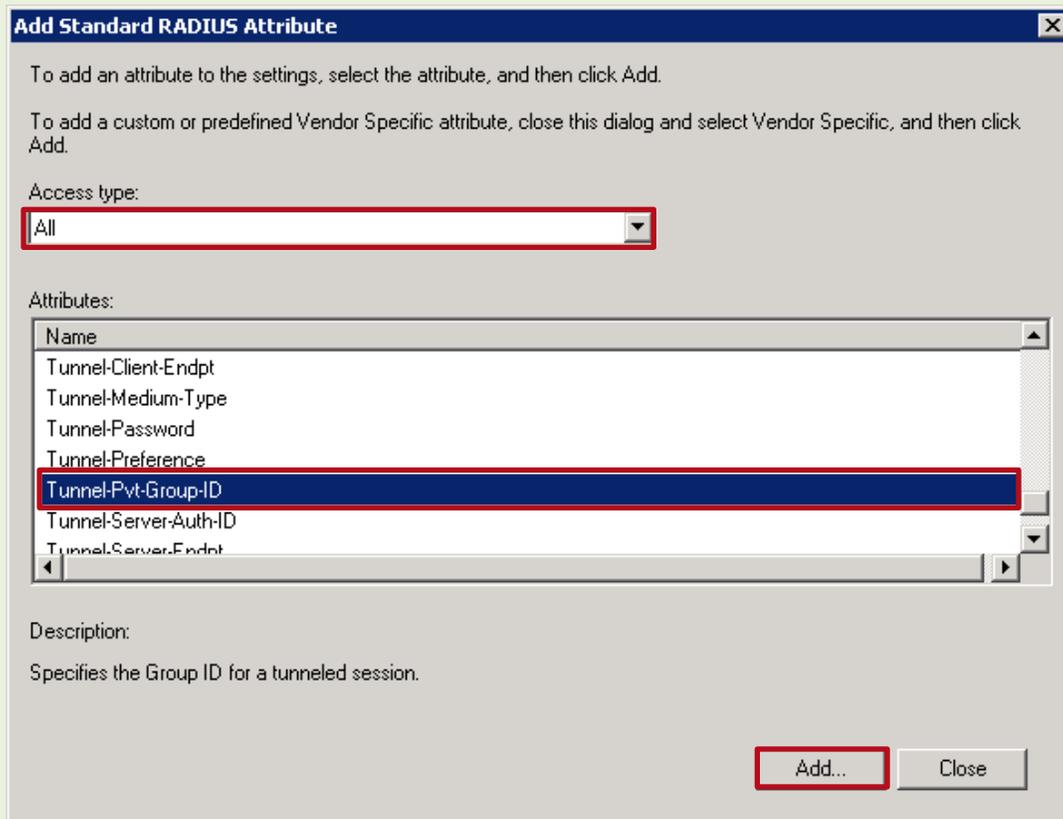
Use the following procedure to assign standard and Motorola vendor specific return attributes to a Network Policy on a Microsoft Network Policy Server.

5.2.1 Tunnel-Private-Group-ID Attribute (Dynamic VLANs)

- 1 Open the *Network Policy Server* snap-in and select *Policies* → *Network Policies*. Select the *Network Policy* name to modify then right-click and select *Properties*. Select the *Settings* → *Standard* then click *Add*:



- 2 Set the *Access type* option to *All* then in the *Attribute* list select *Tunnel-Pvt-Group-ID*. Click *Add*:



Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:
All

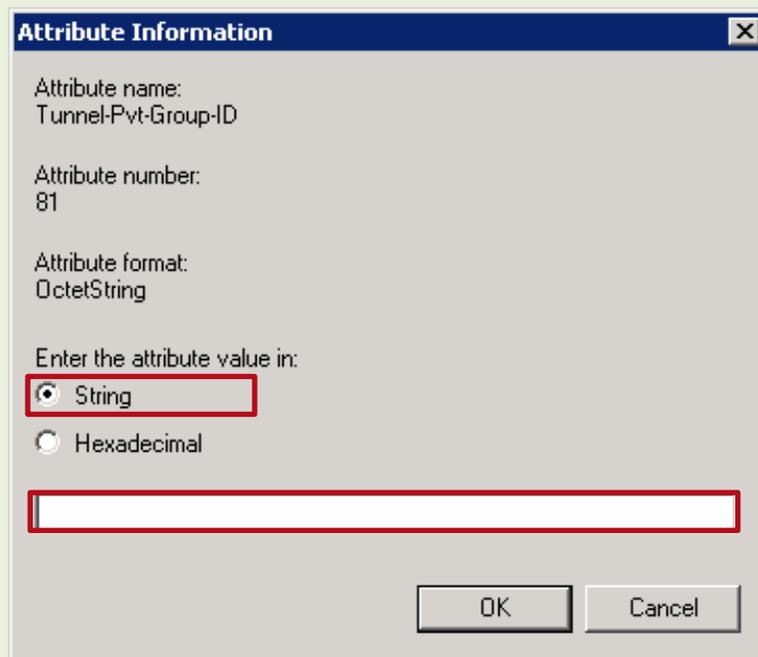
Attributes:

Name
Tunnel-Client-Endpt
Tunnel-Medium-Type
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt

Description:
Specifies the Group ID for a tunneled session.

Add... Close

- 3 Select *String* then in the provided field enter the numerical *VLAN ID* (1 – 4094) to assign to users in the Network Policy. Click *OK*:



Attribute Information

Attribute name:
Tunnel-Pvt-Group-ID

Attribute number:
81

Attribute format:
OctetString

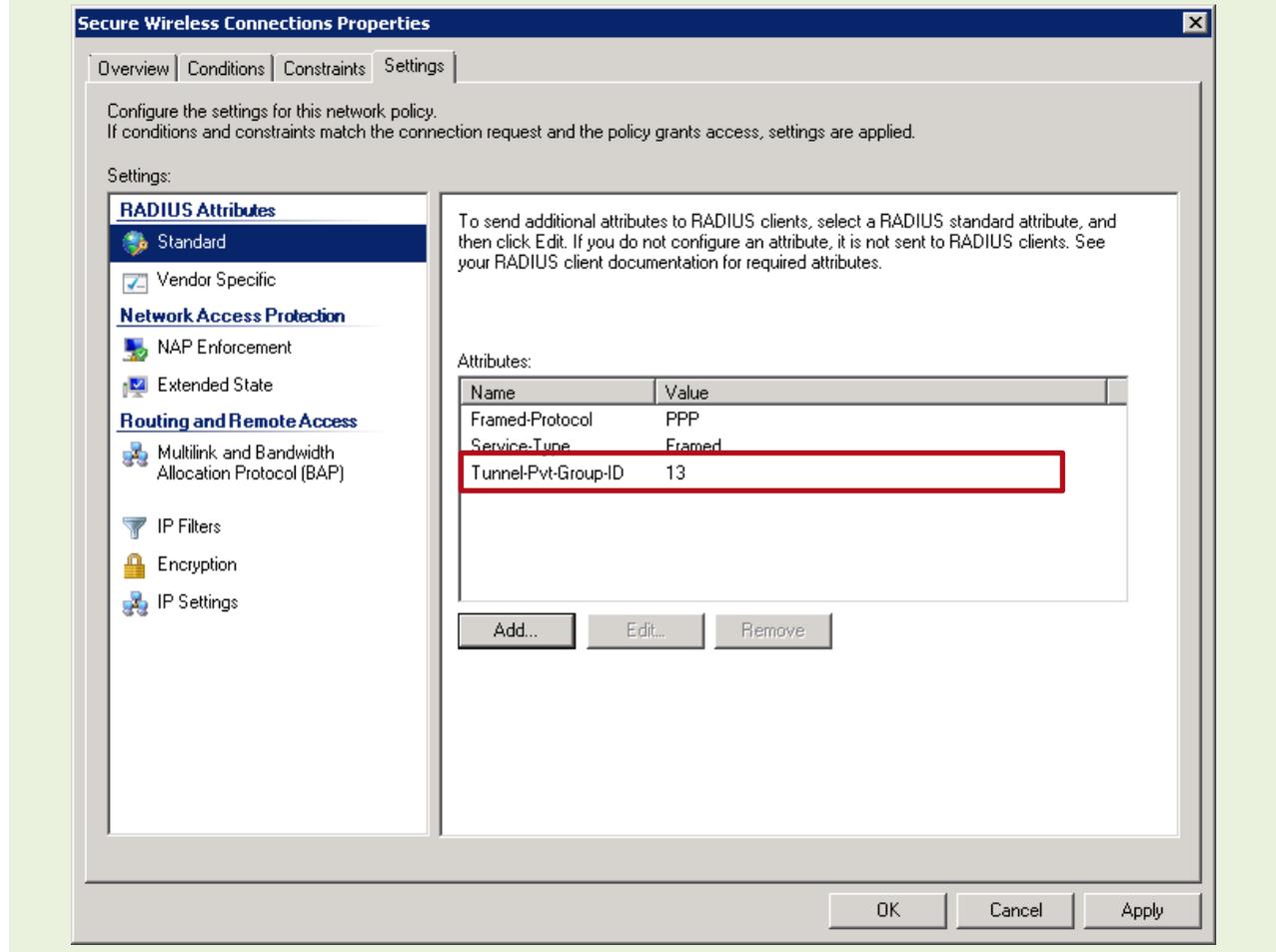
Enter the attribute value in:

String

Hexadecimal

OK Cancel

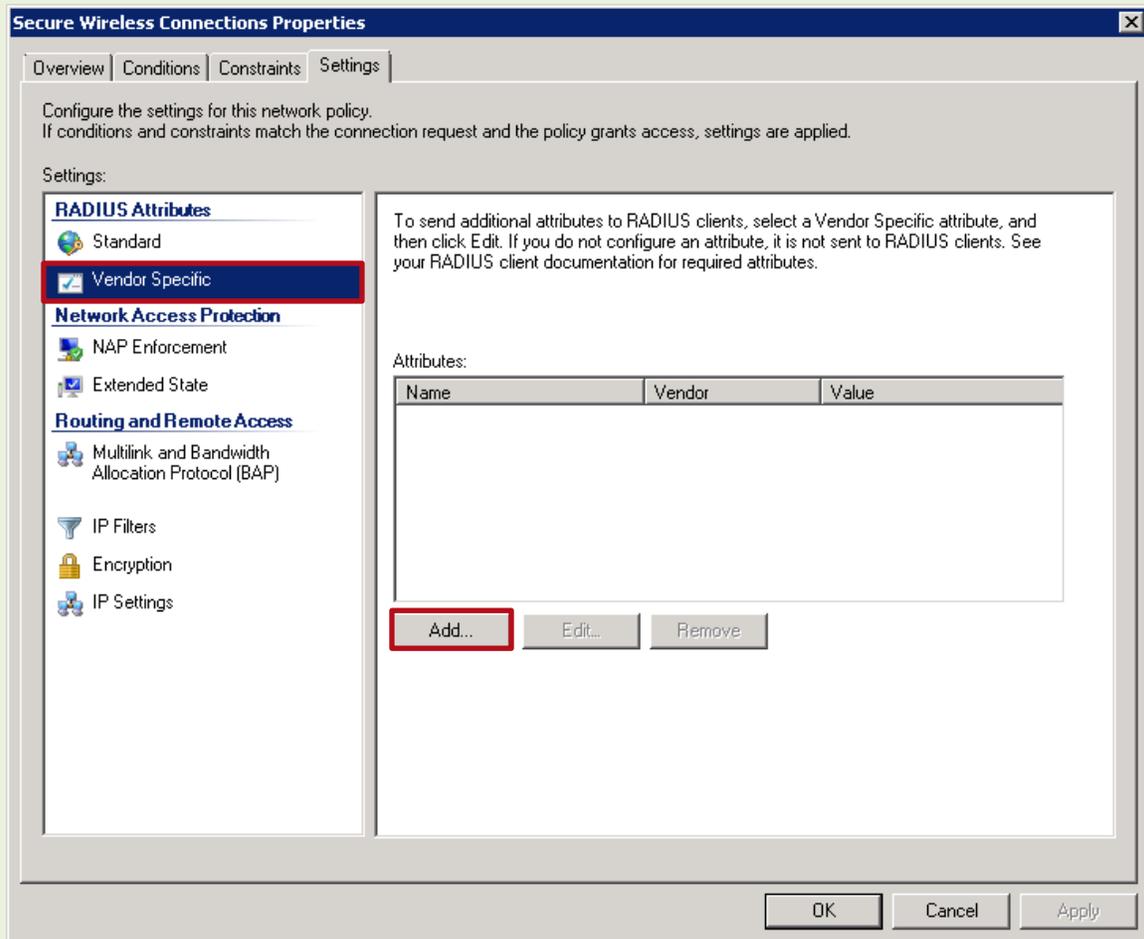
- 4 In the following example the Network Policy named *Secure Wireless Connections* will assign the VLAN ID 13 to authenticated and authorized users:



Note – Only one Tunnel-Private-Group-ID attribute and value is supported per Network Policy.

5.2.2 Motorola Vendor-Specific Attributes

- 1 Open the *Network Policy Server* snap-in and select *Policies* → *Network Policies*. Select the *Network Policy* name to modify then right-click and select *Properties*. Select the *Settings* → *Vendor Specific* then click *Add*:



2 Set the *Vendor* option to *All* then in the *Attribute* list select *Vendor-Specific*. Click *Add*:

Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.
To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:
All

Attributes:

Name	Vendor
USR-Tunnel-Switch-Endpoint	U.S. Robotics, Inc.
USR-Unauthenticated-Time	U.S. Robotics, Inc.
USR-VPN-Encryptor	U.S. Robotics, Inc.
USR-VPN-GW-Location-Id	U.S. Robotics, Inc.
USR-VTS-Session-Key	U.S. Robotics, Inc.
Vendor-Specific	RADIUS Standard

Description:
Specifies the support of proprietary NAS features.

Add... Close

3 In the *Enter Vendor Code* field type *388*. Select *Yes It conforms* then click *Configure Attribute*:

Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Specify network access server vendor.

Select from list: RADIUS Standard

Enter Vendor Code: 388

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

Yes. It conforms

No. It does not conform

Configure Attribute...

OK Cancel

4 Using the provided examples below for each Motorola vendor specific return attribute, enter the desired *Vendor-assigned attribute number*, correct *Attribute format* and desired *Attribute value* then click **OK**:

Configure VSA (RFC Compliant)

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Admin-Role

Configure VSA (RFC Compliant)

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Allowed-SSID

Configure VSA (RFC Compliant)

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-QoS-Profile

Configure VSA (RFC Compliant)

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Allowed-Radio

Configure VSA (RFC Compliant)

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Expiry-Date-Time

Configure VSA (RFC Compliant)

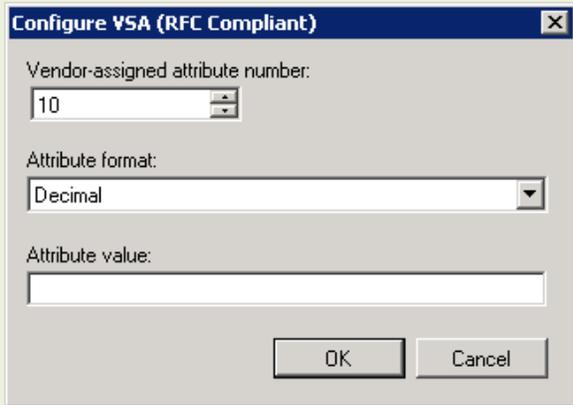
Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

Attribute Example - Symbol-Start-Date-Time



Configure VSA (RFC Compliant)

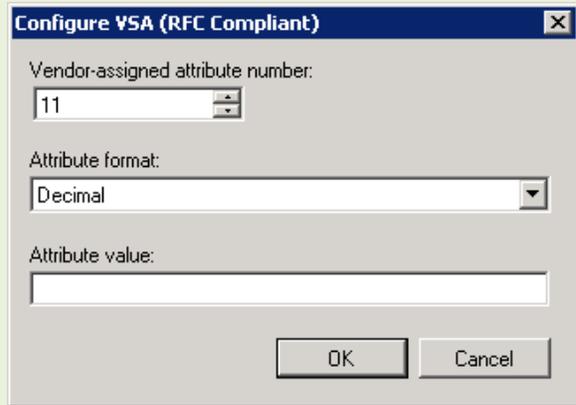
Vendor-assigned attribute number:
10

Attribute format:
Decimal

Attribute value:
[Empty text box]

OK Cancel

Attribute Example - Symbol-Downlink-Limit



Configure VSA (RFC Compliant)

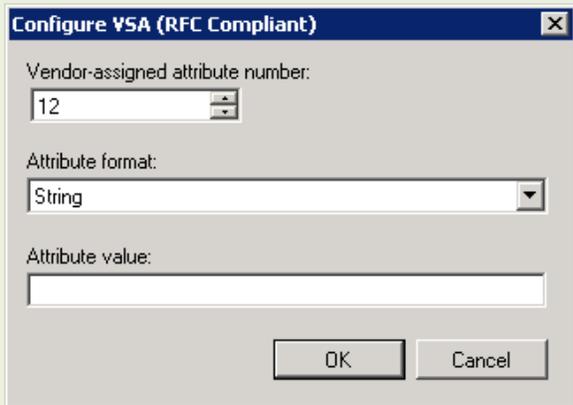
Vendor-assigned attribute number:
11

Attribute format:
Decimal

Attribute value:
[Empty text box]

OK Cancel

Attribute Example - Symbol-Uplink-Limit



Configure VSA (RFC Compliant)

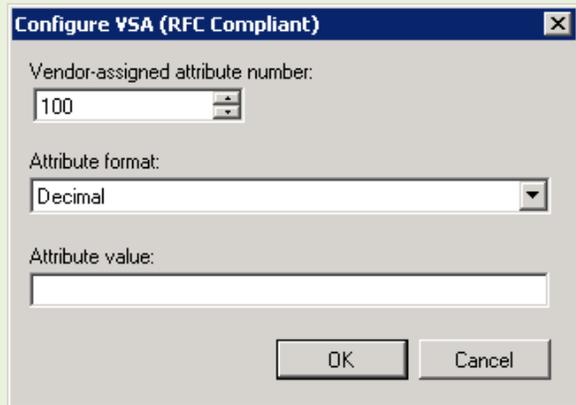
Vendor-assigned attribute number:
12

Attribute format:
String

Attribute value:
[Empty text box]

OK Cancel

Attribute Example - Symbol-User-Group



Configure VSA (RFC Compliant)

Vendor-assigned attribute number:
100

Attribute format:
Decimal

Attribute value:
[Empty text box]

OK Cancel

Attribute Example - Symbol-Login-Source

- 5 In the following example the Network Policy named *Secure Wireless Connections* will restrict authenticated and authorized users to the ESSID named *MOTO-DOT1X* and will assign the users to a group called *Engineering*:

