WiNG 4.X / WiNG 5.X

RADIUS Attributes

Part No. TME-10-2013-07 Rev. E

Table of Contents:

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 polices 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.

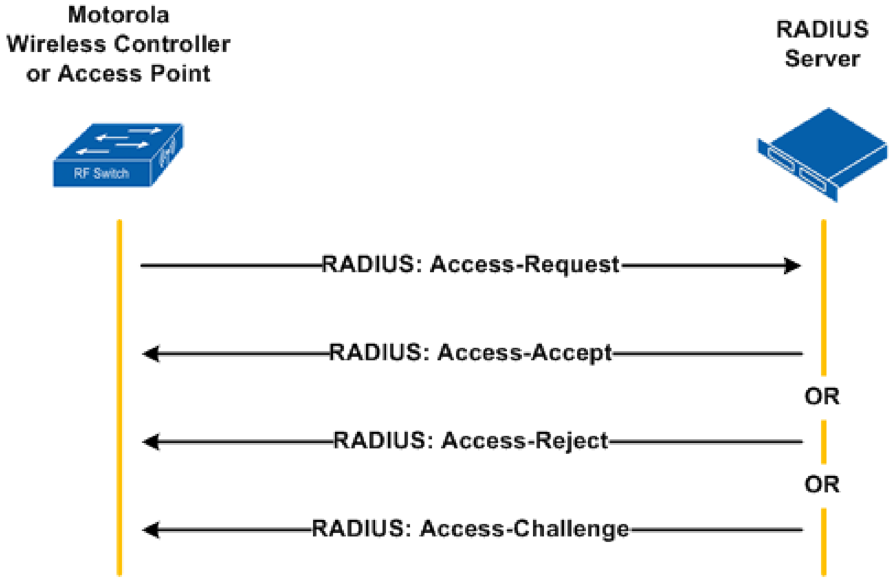


Figure 1.0 – RADIUS Authentication & Authorization

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

NAS-Identifier	32	RFC 2865	The *NAS-Identifier* attribute is forwarded in the *Access-Request* and indicates the hostname or user defined identifier of the Wireless Controller or Access Point.
CHAP-Challenge	60	RFC 2865	The *CHAP-Challenge* attribute is forwarded in the *Access-Request* 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 *NAS-Port-Type* attribute is forwarded in the *Access-Request* and indicates the type of physical connection for the authenticating the user. The attribute value is always set to *Wireless-802.11* by the Wireless Controller or Access Point.
Connection-Info	77	RFC 2869	The *Connection-Info* attribute is forwarded in the *Access-Request* 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: *CONNECT XXMbps 802.11X*.
NAS-Port-Id	87	RFC 2869	The *NAS-Port-Id* attribute is forwarded in the *Access-Request* and indicates the ESSID that the authenticating user is associated with.
CHAP-Challenge	60	RFC 2865	The *CHAP-Challenge* attribute is forwarded in the *Access-Request* 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 *EAP-Message* attribute is forwarded in *the Access-Request*, Access-Challenge, Access-Accept and Access-Reject and encapsulates Extended Access Protocol (EAP) packets.
Message-Authenticator	80	RFC 2869	The *Message-Authenticator* attribute is forwarded in the *Access-Request* and may be used to prevent spoofing of CHAP, ARAP or EAP Access-Request packets.
Tunnel-Private-Group-ID	81	RFC 2868	The *Tunnel-Private-Group-ID* attribute is forwarded in the *Access-Accept* 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 WiNG 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
WING-Admin-Role	26	388	1	Integer
WING-Current-ESSID	26	388	2	String
WING-Allowed-ESSID	26	388	3	String
WING-WLAN-Index	26	388	4	Integer
WING-QoS-Profile	26	388	5	Integer
WING-Allowed-Radio	26	388	6	String
WING-Expiry-Date-Time	26	388	7	String
WING-Start-Date-Time	26	388	8	String
WING-Posture-Status	26	388	9	String
WING-Downlink-Limit	26	388	10	String
WING-Uplink-Limit	26	388	11	Integer
WING-User-Group	26	388	12	String
WING-VLAN-Name	26	388	22	String
WING-Login-Source	26	388	100	Integer

Table 1.2 – Motorola Vendor Specific Attributes

1.2.1 WING-Admin-Role

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

Attribute Name	Vendor ID	Attribute Number	Attribute Format
WING-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 – WING-Admin-Role Attribute Details

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

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

1.2.2 WING-Current-ESSID

The *WING-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
WING-Current-ESSID	388	2	String
Format: *ESSID-Name*			
Example: *Hotspot*			

Table 1.2.2 – Attribute Details

1.2.3 WING-Allowed-ESSID

The *WING-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 retuned 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
WING-Allowed-ESSID	388	3	String
Format: *ESSID-Name*			
Example: *Sales*			

Table 1.2.3 – Attribute Details

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

1.2.4 WING-WLAN-Index

The *WING-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
WING-WLAN-Index	388	4	Integer
Format: *Index-Number*			
Example: *2*			

Table 1.2.4 – Attribute Details

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

1.2.5 WING-QoS-Profile

The *WING-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
WING-QoS-Profile	388	5	Integer
Supported Values: *4 (Voice), 3 (Video), 2 (Background), 1 (Best Effort)*			
Example: *1*			

Table 1.2.5 – Attribute Details

1.2.6 WING-Allowed-Radio

The *WING-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 *WING-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
WING-Allowed-Radio	388	6	String
Format: *Radio-Description-Filter*			
Example: *1st-Floor*			

Table 1.2.6 – Attribute Details

1.2.7 WING-Expiry-Date-Time

The *WING-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 retuned date and time values against the current date and time on the Wireless Controller or Access Point. If the retuned 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 retuned 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
WING-Expiry-Date-Time	388	7	String
Format: *DD:MM:YYYY-HH:mm*			
Example: *01:02:2013-17:00*			

Table 1.2.7 – Attribute Details

1.2.8 WING-Start-Date-Time

The *WING-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 retuned date and time values against the current date and time on the Wireless Controller or Access Point. If the retuned 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 retuned 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
WING-Start-Date-Time	388	8	String
Format: *DD:MM:YYYY-HH:mm*			
Example: 10*:02:2013-08:00*			

Table 1.2.8 – Attribute Details

1.2.9 WING-Posture-Status

The *WING-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
WING-Posture-Status	388	9	String

Table 1.2.9 – Attribute Details

1.2.10 WING-Downlink-Limit

The *WING-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
WING-Downlink-Limit	388	10	Integer
Format: *0, 100-10,000 (0 = Disabled)*			
Example: *768*			

Table 1.2.10 – Attribute Details

1.2.11 WING-Uplink-Limit

The *WING-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
WING-Uplink-Limit	388	11	Integer
Format: *0, 100-10,000 (0 = Disabled)*			
Example: *512*			

Table 1.2.11 – Attribute Details

1.2.12 WING-User-Group

The *WING-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 *WING-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
WING-User-Group	388	12	String
Format: *Group-Name*			
Example: *Sales*			

Table 1.2.12 – Attribute Details

1.2.13 WING-VLAN-Name

The *WING-VLAN-Name* attribute maybe forwarded in the *Access-Accept* and indicates the VLAN Alias the authenticating user is to be assigned. The *WING-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
WING-User-Group	388	22	String
Format: *$ALIASNAME*			
Example: *$Sales*			

Table 1.2.13 – Attribute Details

Note – The WING-VLAN-Name attribute is supported in WiNG 5.4.4 and above and requires the Alias to be defined in the global, profile, device or RF Domain contexts.

1.2.14 WING-Login-Source

The *WING-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 retuned 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
WING-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 1.2.14 – Attribute Details

Note – The WING-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 WING-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.

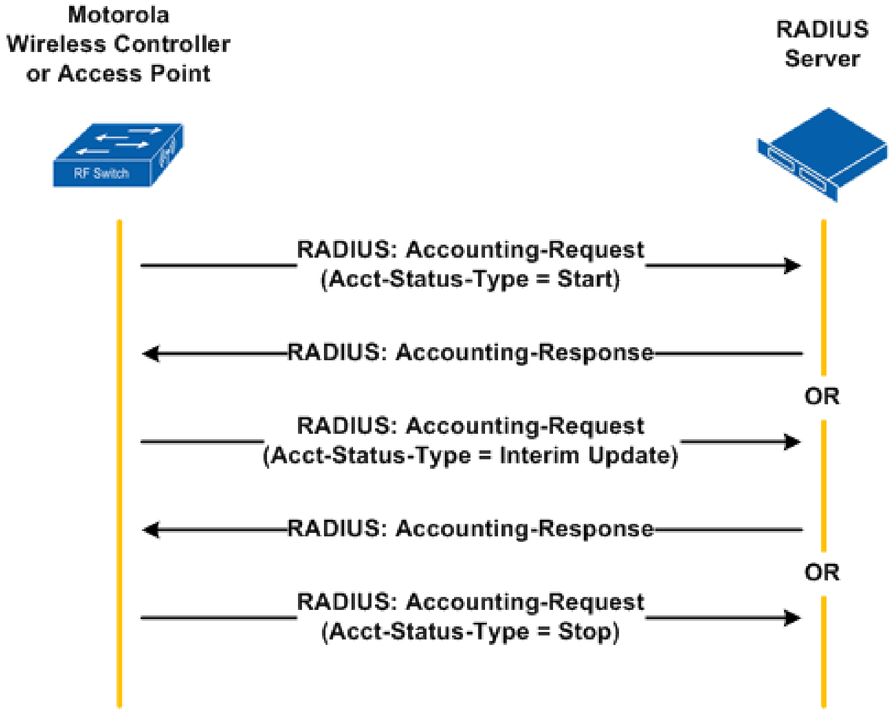

Motorola
Wireless Controller
or Access Point
RADIUS
Server
RF Switch
RADIUS: Accounting-Request
(Acct-Status-Type = Start)
RADIUS: Accounting-Response
OR
RADIUS: Accounting-Request
(Acct-Status-Type = Interim Update)
RADIUS: Accounting-Response
OR
RADIUS: Accounting-Request
(Acct-Status-Type = Stop)

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 *User-Name* attribute is forwarded in the *Accounting-Request* and indicates the name of the user.
NAS-IP-Address	4	RFC 2865	The *NAS-IP-Address* attribute is forwarded in the *Accounting-Request* and indicates the IP Address of the Wireless Controller or Access Point.
NAS-Port	5	RFC 2865	The *NAS-Port* attribute is forwarded in the *Accounting-Request* and indicates the association index of the user on the Wireless Controller or Access Point.
Class	25	RFC 2865	The *Class* attribute is optionally forwarded in the *Access-Accept* and should be sent unmodified by the client to the accounting server as part of the *Accounting-Request* packet if accounting is supported.
Called-Station-Id	30	RFC 2865	The *Called-Station-Id* attribute is forwarded in the *Accounting-Request* 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: *XX-XX-XX-XX-XX-XX:ESSID*.
Calling-Station-Id	31	RFC 2865	The *Calling-Station-Id* attribute is forwarded in the *Accounting-Request* and indicates the MAC address of the user. The Wireless Controller or Access Point will forward the attribute value using the following formatting: *XX-XX-XX-XX-XX-XX*.
NAS-Identifier	32	RFC 2865	The *NAS-Identifier* attribute is forwarded in the *Accounting-Request* and indicates the hostname or user defined identifier of the Wireless Controller or Access Point.
Acct-Status-Type	40	RFC 2866	The *Acct-Status-Type* attribute is forwarded in the *Accounting-Request* and 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	The *Acct-Delay-Time* attribute is forwarded in the *Accounting-Request* 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 *Accounting-Request*.

Acct-Input-Octets	42	RFC 2866	The *Acct-Input-Octets* attribute is forwarded in the *Accounting-Request* and 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	The *Acct-Output-Octets* attribute is forwarded in the *Accounting-Request* and 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	The *Acct-Session-Id* attribute is forwarded in the *Accounting-Request* and 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	The *Account-Authentic* attribute is forwarded in the *Accounting-Request* and indicates how the user was authenticated. When RADIUS accounting is enabled the Wireless Controller or Access Point will set this value to *RADIUS*.
Acct-Session-Time	46	RFC 2866	The *Acct-Session-Time* attribute is forwarded in the *Accounting-Request* and 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 2866	The *Acct-Input-Packets* attribute is forwarded in the *Accounting-Request* and 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	The *Acct-Output-Packets* attribute is forwarded in the *Accounting-Request* and 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	The *Acct-Terminate-Cause* attribute is forwarded in the *Accounting-Request* and 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	The *Event-Timestamp* attribute is forwarded in the *Accounting-Request* and indicates the time that the accounting event occurred on the Wireless Controller or Access Point.
NAS-Port-Type	61	RFC 2865	The *NAS-Port-Type* attribute is forwarded in the *Accounting-Request* and indicates the type of physical connection for the user. This attribute value is always set to *Wireless-802.11* by the Wireless Controller or Access Point.

Tunnel-Type	64	RFC 2868	The *Tunnel-Type attribute* is forwarded in the *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	The *Tunnel-Medium-Type* attribute is forwarded in the *Accounting-Request* and 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	The *Tunnel-Private-Group-ID* attribute is forwarded in the *Accounting-Request* 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 *NAS-Port-Id* attribute is forwarded in the *Accounting-Request* 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.

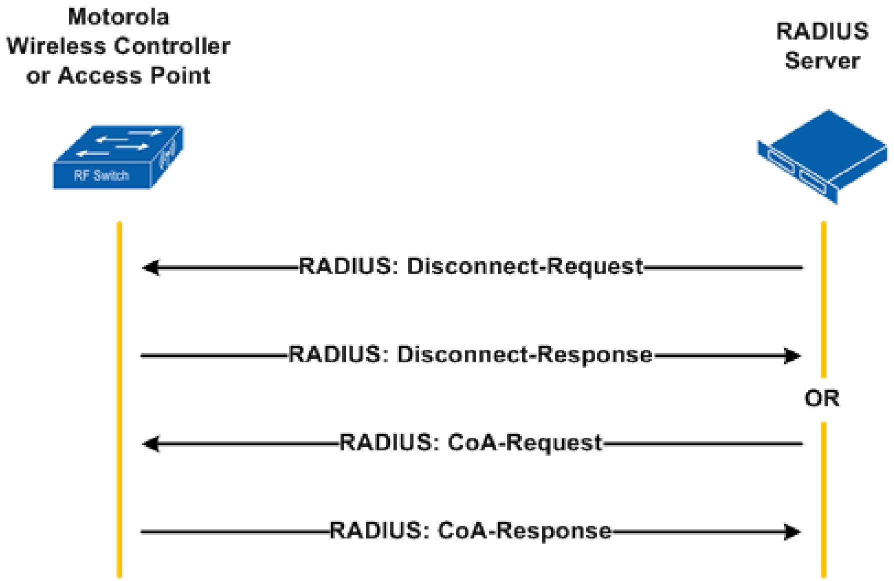


Figure 3.0 – Dynamic Authorization Extensions

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 by 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 *wing.ini* and imported using the provided CSUtil utility.

```
;
; Motorola WiNG 4.X / WiNG 5.X File for Cisco Secure ACS for Windows
; Last Updated: June 2013
; Created By: kmarshall@motorolasolutions.com
;

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

VSA 1=WING-Admin-Role
VSA 2=WING-Current-ESSID
VSA 3=WING-Allowed-ESSID
VSA 4=WING-WLAN-Index
VSA 5=WING-QoS-Profile
VSA 6=WING-Allowed-Radio
VSA 7=WING-Expiry-Date-Time
VSA 8=WING-Start-Date-Time
VSA 9=WING-Posture-Status
VSA 10=WING-Downlink-Limit
VSA 11=WING-Uplink-Limit
VSA 12=WING-User-Group
VSA 22=WING-VLAN-Name
VSA 100=WING-Login-Source

[WING-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

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

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

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

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

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

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

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

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

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

[WING-Uplink-Limit]
```

```
Type=INTEGER
Profile=OUT

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

[WING-VLAN-Name]
Type=STRING
Profile=OUT

[WING-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.wingl*.

```
#
# Motorola WiNG 4.X / WiNG 5.X Dictionary File for FreeRADIUS
# Last Updated: June 2013
# Created By: kmarshall@motorolasolutions.com
#

VENDOR         Symbol         388

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

ATTRIBUTE      WING-Current-ESSID            2              string         Symbol
ATTRIBUTE      WING-Allowed-ESSID            3              string         Symbol
ATTRIBUTE      WING-WLAN-Index               4              integer        Symbol
ATTRIBUTE      WING-QoS-Profile              5              integer        Symbol
ATTRIBUTE      WING-Allowed-Radio            6              string         Symbol
ATTRIBUTE      WING-Expiry-Date-Time  7              string         Symbol
ATTRIBUTE      WING-Start-Date-Time          8              string         Symbol
ATTRIBUTE      WING-Posture-Status           9              string         Symbol
ATTRIBUTE      WING-Downlink-Limit           10             integer        Symbol
ATTRIBUTE      WING-Uplink-Limit             11             integer        Symbol
ATTRIBUTE      WING-User-Group               12             string         Symbol
ATTRIBUTE      WING-VLAN-Name               22              string         Symbol

ATTRIBUTE      WING-Login-Source             100            integer        Symbol
VALUE          WING-Login-Source             HTTP           16
VALUE          WING-Login-Source             SSH            32
VALUE          WING-Login-Source             Telnet         64
VALUE          WING-Login-Source             Console        128
VALUE          WING-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: June 2013
# Created By: kmarshall@motorolasolutions.com
#

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

VENDORATTR     388     WING-Current-ESSID            2       string
VENDORATTR     388     WING-Allowed-ESSID            3       string
VENDORATTR     388     WING-WLAN-Index               4       integer
VENDORATTR     388     WING-QoS-Profile              5       integer
VENDORATTR     388     WING-Allowed-Radio            6       string
VENDORATTR     388     WING-Expiry-Date-Time        7        string
VENDORATTR     388     WING-Start-Date-Time          8       string
VENDORATTR     388     WING-Posture-Status           9       string
VENDORATTR     388     WING-Downlink-Limit           10      integer
VENDORATTR     388     WING-Uplink-Limit             11      integer
VENDORATTR     388     WING-User-Group               12      string
VENDORATTR     388     WING-VLAN-Name                22      string

VENDORATTR     388     WING-Login-Source     100            integer
VALUE          WING-Login-Source             HTTP           16
VALUE          WING-Login-Source             SSH            32
VALUE          WING-Login-Source             Telnet         64
VALUE          WING-Login-Source             Console        128
VALUE          WING-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 wing.*dct*.

```
#
# Motorola WiNG 4.X / WiNG 5.X Dictionary File for Steel Belted RADIUS
# Last Updated: June 2013
# Created By: kmarshall@motorolasolutions.com
#
@radius.dct

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

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

ATTRIBUTE      WING-Current-ESSID            WING-VSA(2, string) C
ATTRIBUTE      WING-Allowed-ESSID            WING-VSA(3, string) R
ATTRIBUTE      WING-WLAN-Index               WING-VSA(4, integer) C
ATTRIBUTE      WING-QoS-Profile              WING-VSA(5, integer) C
ATTRIBUTE      WING-Allowed-Radio            WING-VSA(6, string) R
ATTRIBUTE      WING-Expiry-Date-Time WING-VSA(7, string) R
ATTRIBUTE      WING-Start-Date-Time          WING-VSA(8, string) R
ATTRIBUTE      WING-Posture-Status           WING-VSA(9, string) R
ATTRIBUTE      WING-Downlink-Limit           WING-VSA(10, integer) R
ATTRIBUTE      WING-Uplink-Limit             WING-VSA(11, integer) R
ATTRIBUTE      WING-User-Group               WING-VSA(12, string) R
ATTRIBUTE      WING-VLAN-Name                WING-VSA(22, string) R

ATTRIBUTE      WING-Login-Source             WING-VSA(100, integer) R
VALUE          WING-Login-Source             HTTP           16
VALUE          WING-Login-Source             SSH            32
VALUE          WING-Login-Source             Telnet         64
VALUE          WING-Login-Source             Console        128
VALUE          WING-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	WING-Admin-Role	1	Decimal
388	WING-Allowed-ESSID	3	String
388	WING-QoS-Profile	5	Decimal
388	WING-Allowed-Radio	6	String
388	WING-Expiry-Date-Time	7	String
388	WING-Start-Date-Time	8	String
388	WING-Downlink-Limit	10	Decimal
388	WING-Uplink-Limit	11	Decimal
388	WING-User-Group	12	String
388	WING-Login-Source	100	Decimal

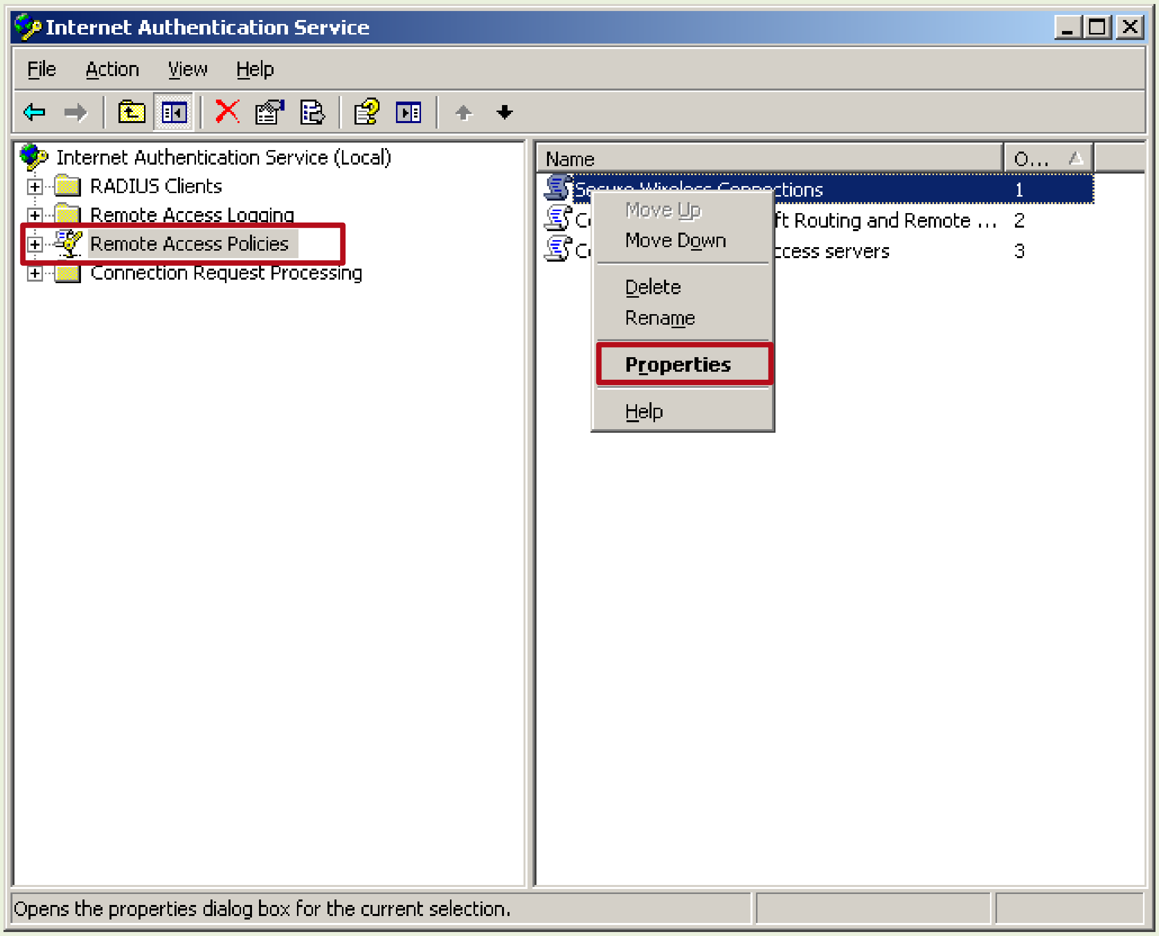
Table 5.0 – Motorola Attribute Formatting

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.

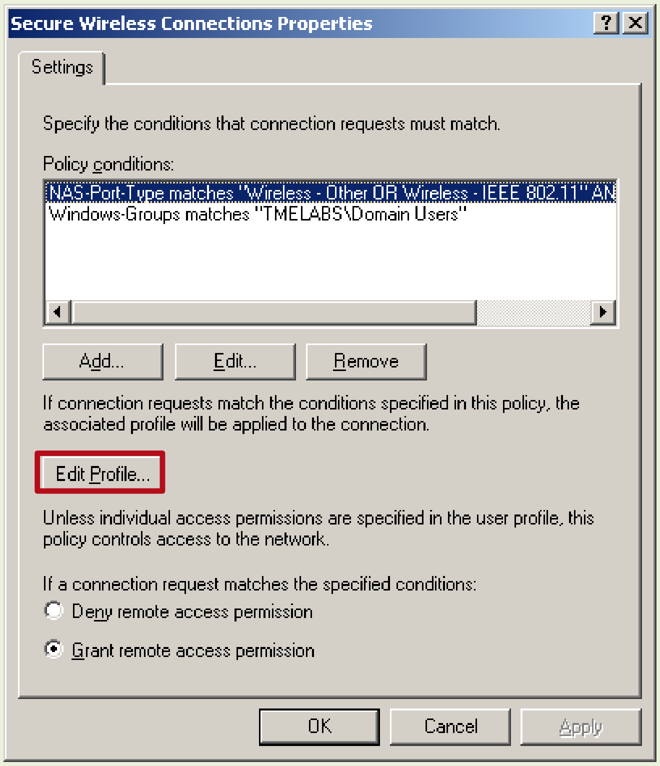
5.1.1 Tunnel-Private-Group-ID Attribute (Dynamic VLANs)

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*:**


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
Name
O...
Secure Wireless Connections
1
Ci
ft Routing and Remote ...
2
Ci
ccess servers
3
Move Up
Move Down
Delete
Rename
Properties
Help

Opens the properties dialog box for the current selection.

2 Select *Edit Profile*:



Specify the conditions that connection requests must match.

Policy conditions:

NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11" AN

Windows-Groups matches "TMELABS\Domain Users"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

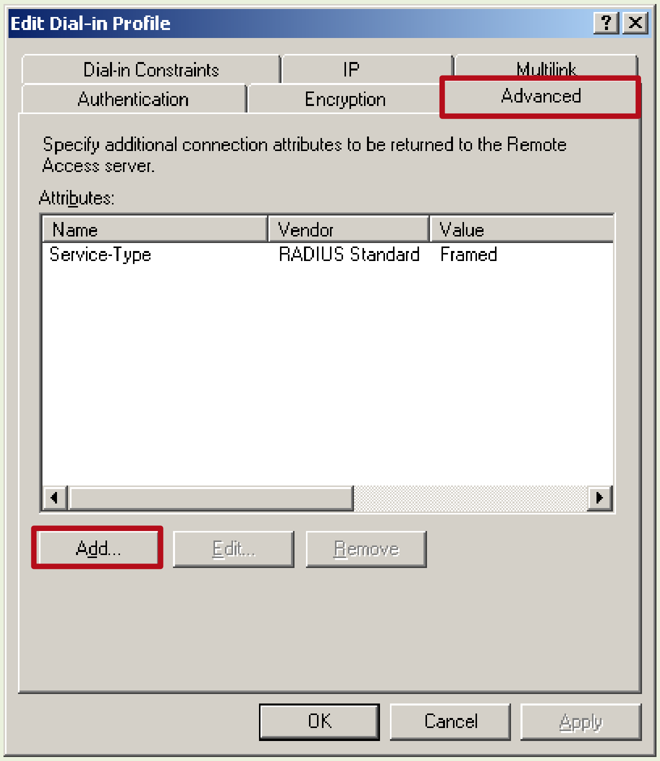
Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

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

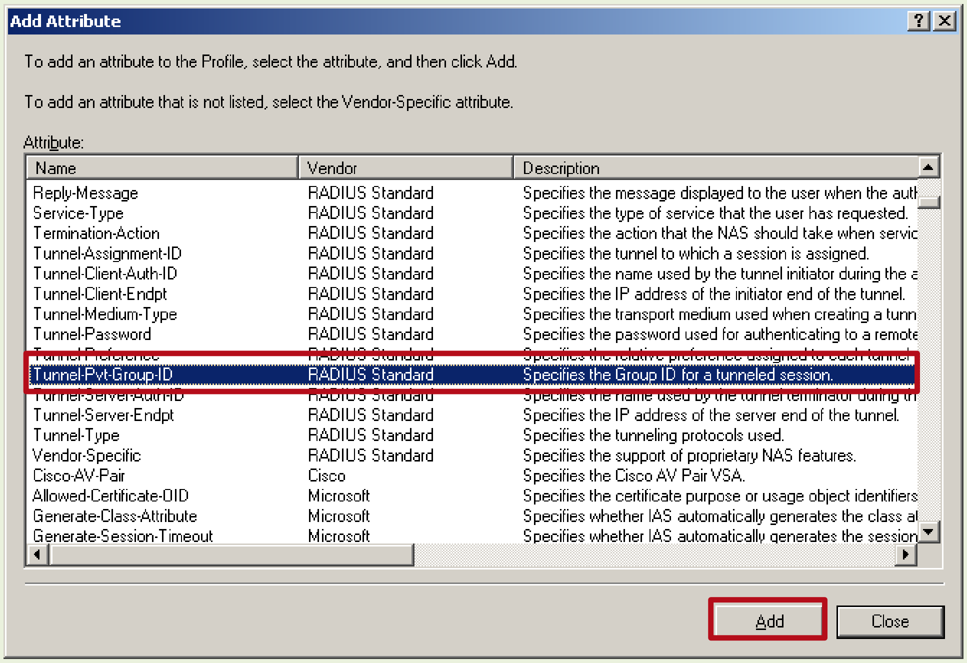


Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Service-Type	RADIUS Standard	Framed

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



Add Attribute

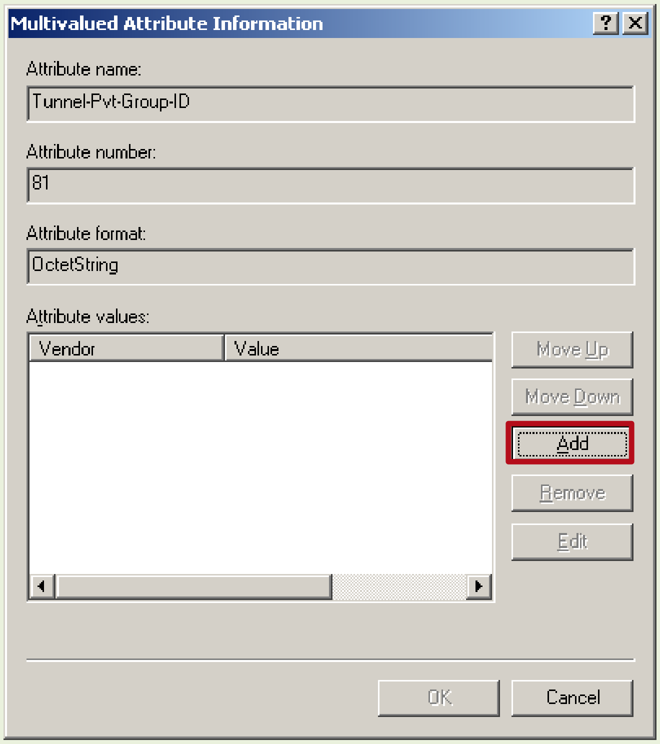
To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	Vendor	Description
Reply-Message	RADIUS Standard	Specifies the message displayed to the user when the auth
Service-Type	RADIUS Standard	Specifies the type of service that the user has requested.
Termination-Action	RADIUS Standard	Specifies the action that the NAS should take when servic
Tunnel-Assignment-ID	RADIUS Standard	Specifies the tunnel to which a session is assigned.
Tunnel-Client-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel initiator during the a
Tunnel-Client-Endpt	RADIUS Standard	Specifies the IP address of the initiator end of the tunnel.
Tunnel-Medium-Type	RADIUS Standard	Specifies the transport medium used when creating a tunn
Tunnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote
Tunnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each tunnel
Tunnel-Pvt-Group-ID	RADIUS Standard	Specifies the Group ID for a tunneled session.
Tunnel-Server-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during th
Tunnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the tunnel.
Tunnel-Type	RADIUS Standard	Specifies the tunneling protocols used.
Vendor-Specific	RADIUS Standard	Specifies the support of proprietary NAS features.
Cisco-AV-Pair	Cisco	Specifies the Cisco AV Pair VSA.
Allowed-Certificate-OID	Microsoft	Specifies the certificate purpose or usage object identifiers
Generate-Class-Attribute	Microsoft	Specifies whether IAS automatically generates the class at
Generate-Session-Timeout	Microsoft	Specifies whether IAS automatically generates the session

5 Click *Add*:



Multivalued Attribute Information

Attribute name: Tunnel-Pvt-Group-ID

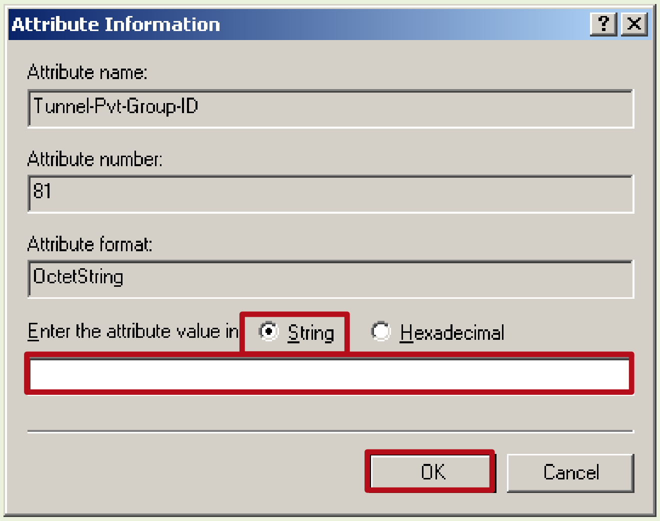
Attribute number: 81

Attribute format: OctetString

Attribute values:

Vendor	Value

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*:**



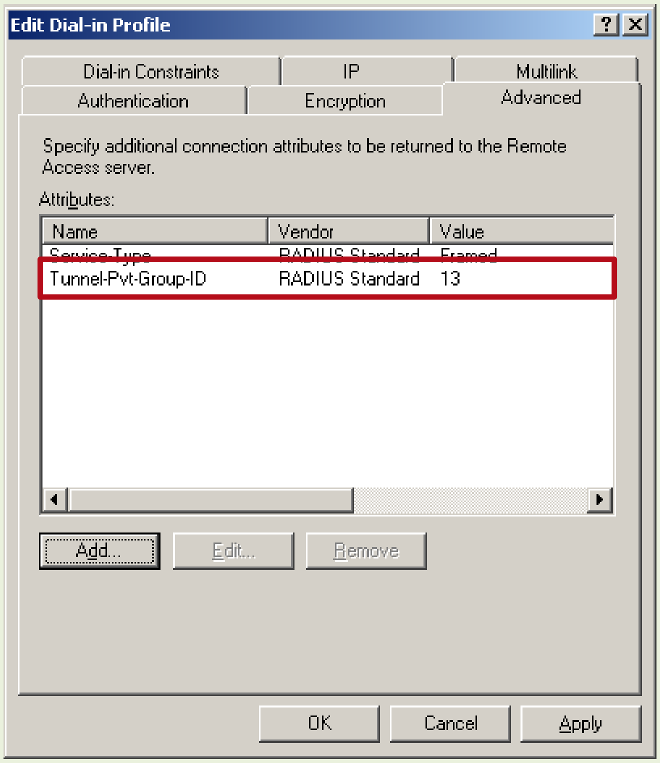
Attribute name: Tunnel-Pvt-Group-ID

Attribute number: 81

Attribute format: OctetString

Enter the attribute value in: ● String ○ Hexadecimal

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



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

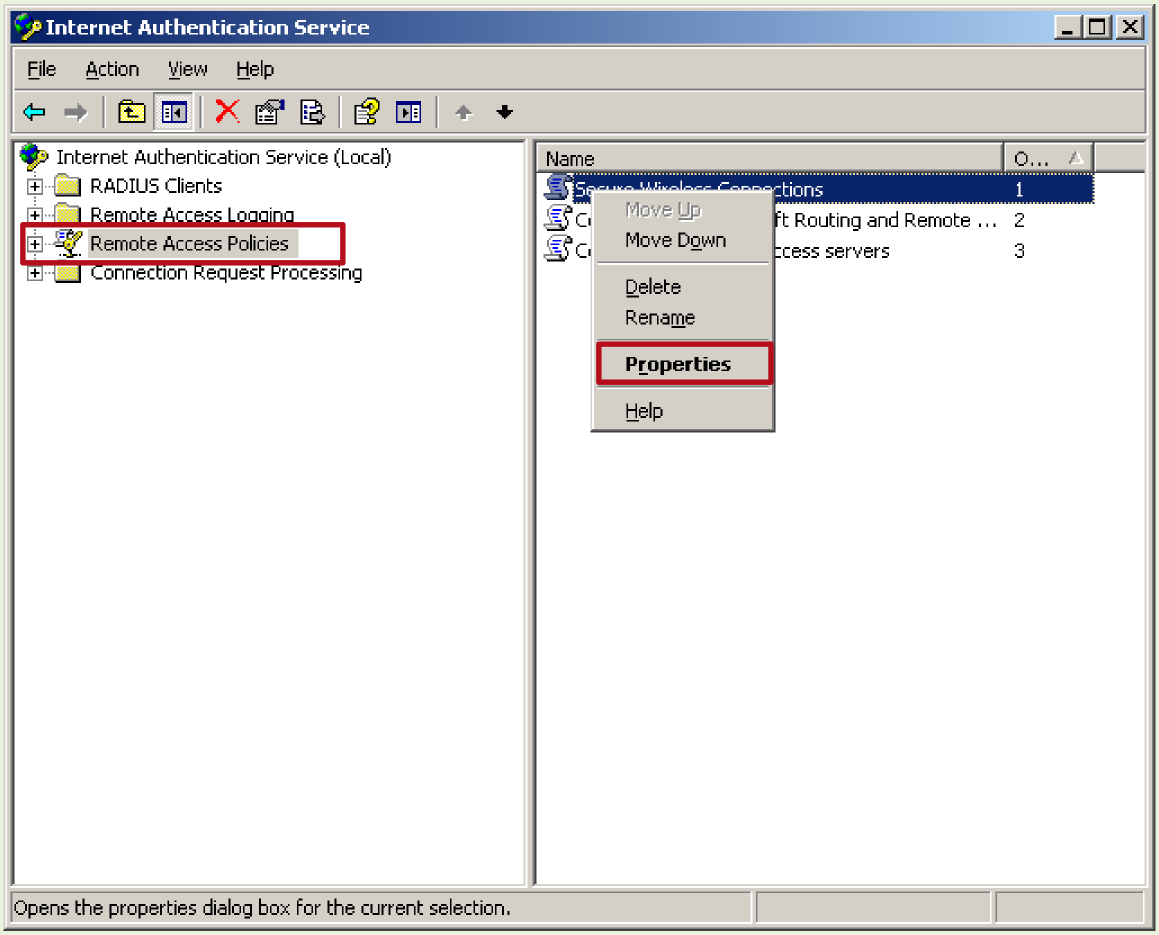
Attributes:

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

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

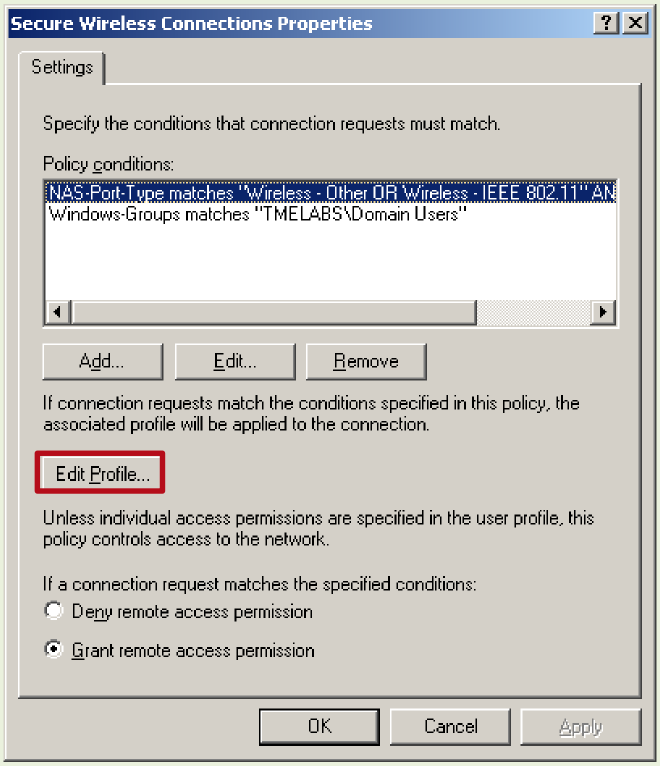
5.1.2 Motorola Vendor-Specific Attributes

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*:**


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
Name
O...
Secure Wireless Connections
1
ft Routing and Remote ...
2
ccess servers
3
Move Up
Move Down
Delete
Rename
Properties
Help

Opens the properties dialog box for the current selection.

2 Select *Edit Profile*:



Specify the conditions that connection requests must match.

Policy conditions:

NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11" AN

Windows-Groups matches "TMELABS\Domain Users"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

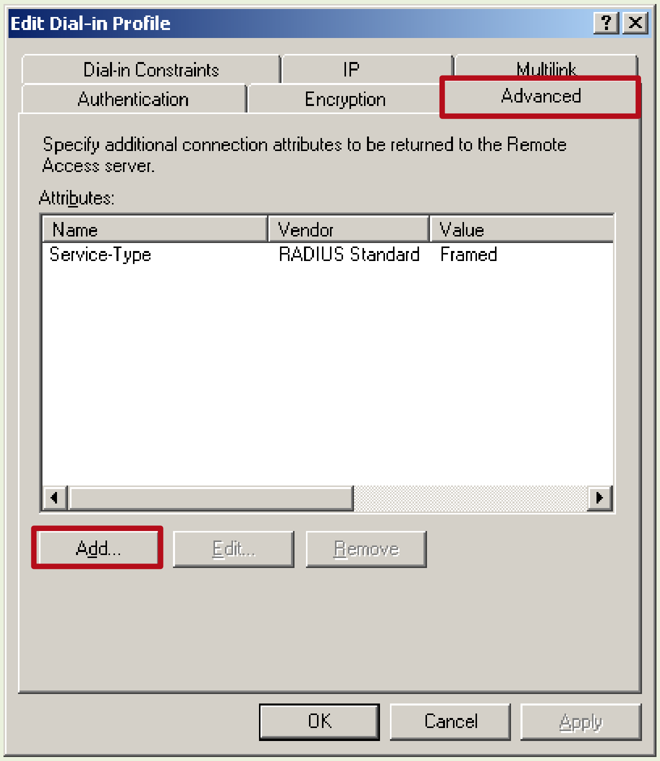
Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

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

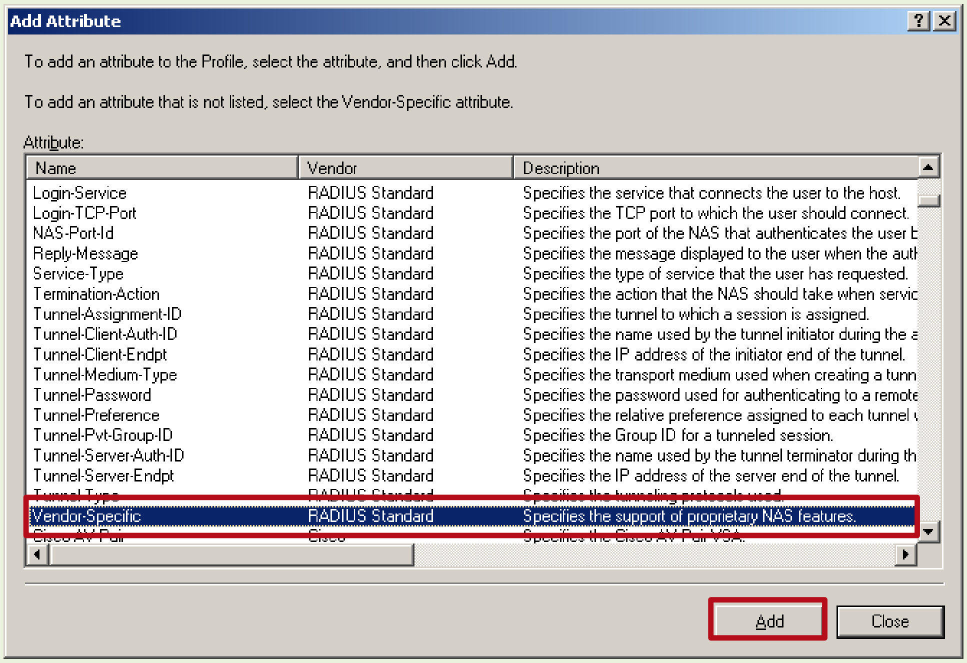


Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Service-Type	RADIUS Standard	Framed

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



Add Attribute

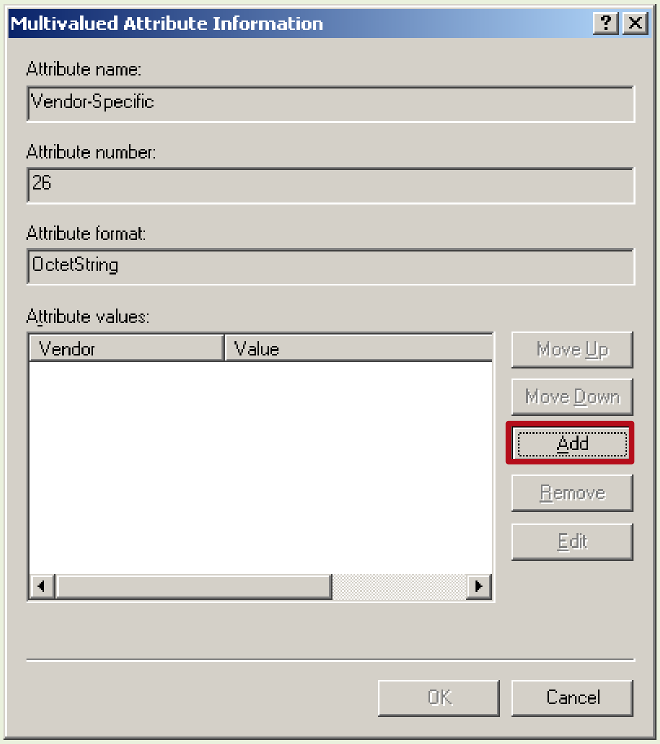
To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	Vendor	Description
Login-Service	RADIUS Standard	Specifies the service that connects the user to the host.
Login-TCP-Port	RADIUS Standard	Specifies the TCP port to which the user should connect.
NAS-Port-Id	RADIUS Standard	Specifies the port of the NAS that authenticates the user b
Reply-Message	RADIUS Standard	Specifies the message displayed to the user when the auth
Service-Type	RADIUS Standard	Specifies the type of service that the user has requested.
Termination-Action	RADIUS Standard	Specifies the action that the NAS should take when servic
Tunnel-Assignment-ID	RADIUS Standard	Specifies the tunnel to which a session is assigned.
Tunnel-Client-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel initiator during the a
Tunnel-Client-Endpt	RADIUS Standard	Specifies the IP address of the initiator end of the tunnel.
Tunnel-Medium-Type	RADIUS Standard	Specifies the transport medium used when creating a tunn
Tunnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote
Tunnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each tunnel w
Tunnel-Pvt-Group-ID	RADIUS Standard	Specifies the Group ID for a tunneled session.
Tunnel-Server-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during th
Tunnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the tunnel.
Tunnel-Type	RADIUS Standard	Specifies the tunneling protocols used.
Vendor-Specific	RADIUS Standard	Specifies the support of proprietary NAS features.
Cisco-AV-Pair	Cisco	Specifies the Cisco AV Pair VSA.

5 Click *Add*:



Multivalued Attribute Information

Attribute name:
Vendor-Specific

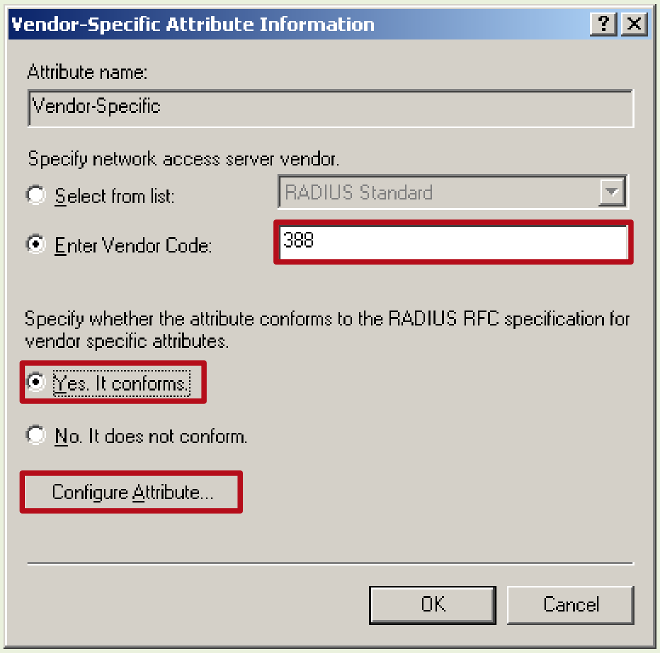
Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value

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

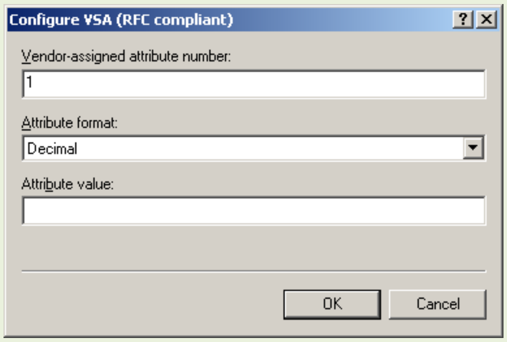
● Enter Vendor Code: 388

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

● Yes. It conforms.

○ No. It does not conform.

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*:



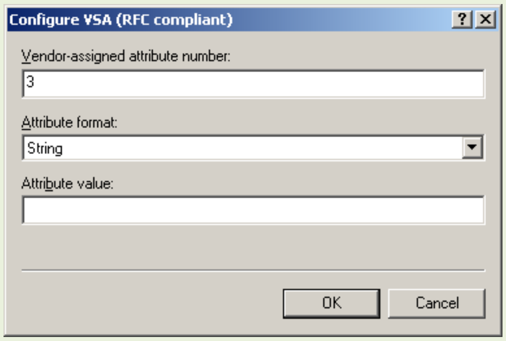
Configure VSA (RFC compliant)

Vendor-assigned attribute number: 1

Attribute format: Decimal

Attribute value:

Attribute Example - WING-Admin-Role



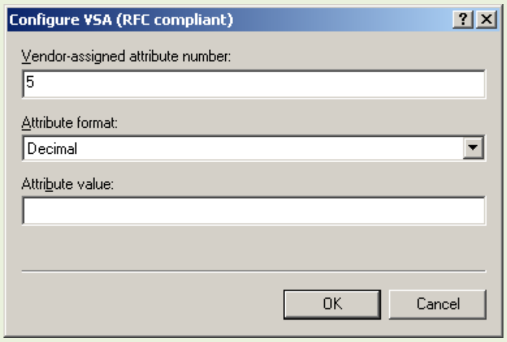
Configure VSA (RFC compliant)

Vendor-assigned attribute number: 3

Attribute format: String

Attribute value:

Attribute Example - WING-Allowed-SSID



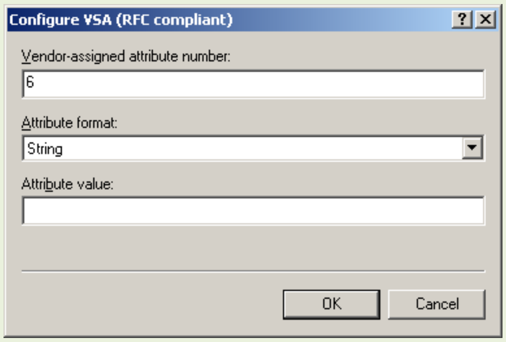
Configure VSA (RFC compliant)

Vendor-assigned attribute number: 5

Attribute format: Decimal

Attribute value:

Attribute Example - WING-QoS-Profile



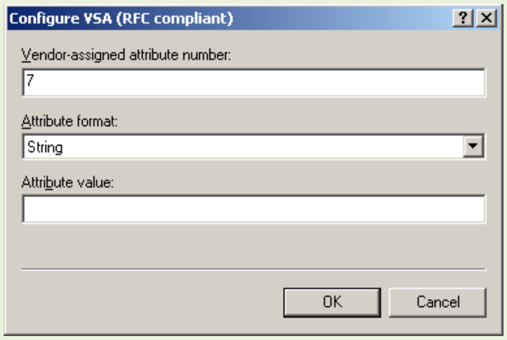
Configure VSA (RFC compliant)

Vendor-assigned attribute number: 6

Attribute format: String

Attribute value:

Attribute Example - WING-Allowed-Radio

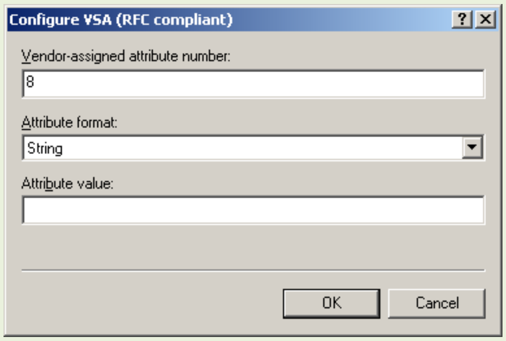

Configure VSA (RFC compliant)

Vendor-assigned attribute number: 7

Attribute format: String

Attribute value:

Attribute Example - WING-Expiry-Date-Time

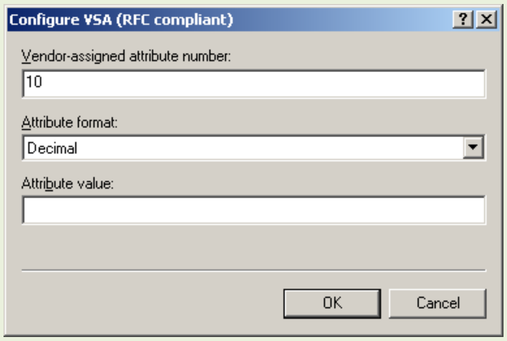

Configure VSA (RFC compliant)

Vendor-assigned attribute number: 8

Attribute format: String

Attribute value:

Attribute Example - WING-Start-Date-Time

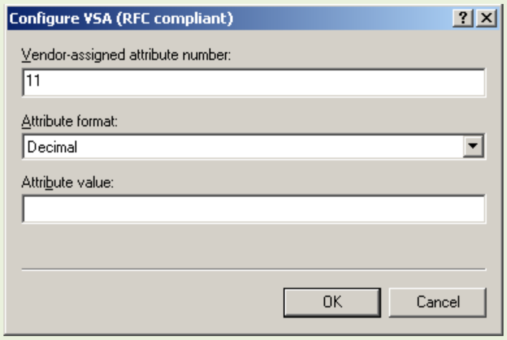

Configure VSA (RFC compliant)

Vendor-assigned attribute number: 10

Attribute format: Decimal

Attribute value:

Attribute Example - WING-Downlink-Limit

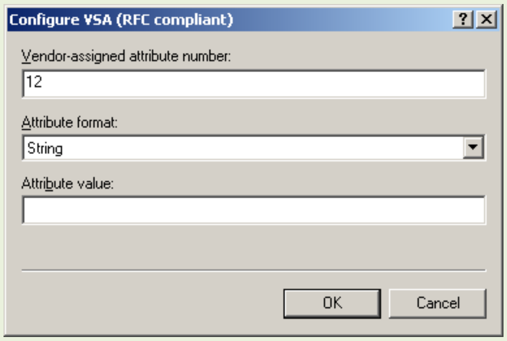

Configure VSA (RFC compliant)

Vendor-assigned attribute number: 11

Attribute format: Decimal

Attribute value:

Attribute Example - WING-Uplink-Limit

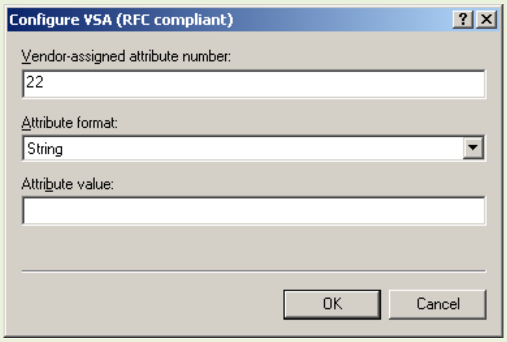

Configure VSA (RFC compliant)

Vendor-assigned attribute number: 12

Attribute format: String

Attribute value:

Attribute Example - WING-User-Group

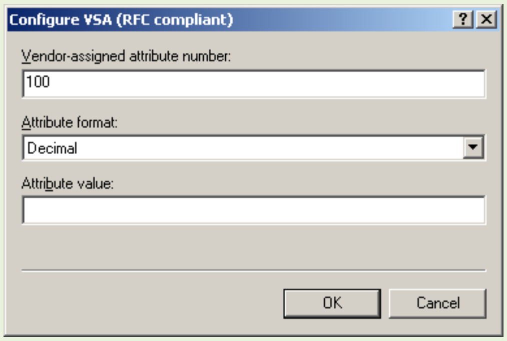

Configure VSA (RFC compliant)

Vendor-assigned attribute number: 22

Attribute format: String

Attribute value:

Attribute Example - WING-VLAN-Name


Configure VSA (RFC compliant)

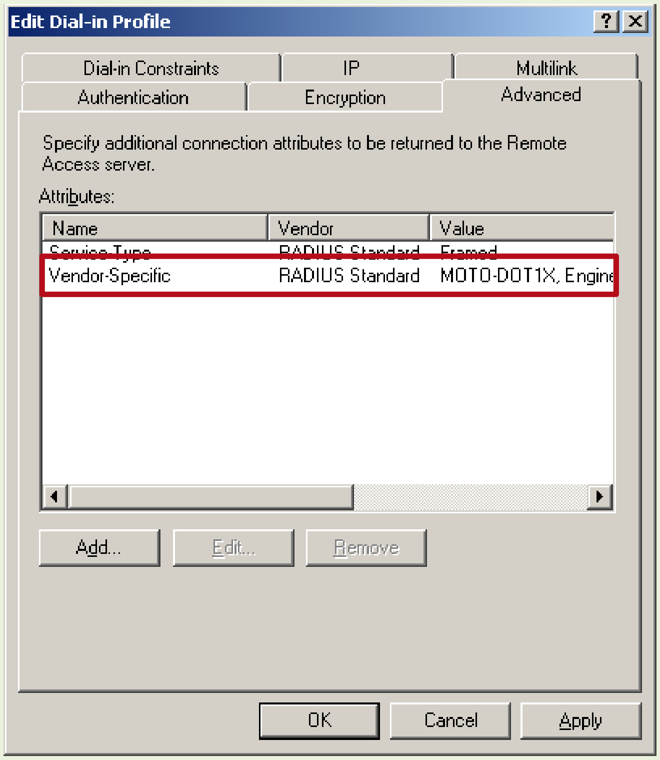
Vendor-assigned attribute number: 100

Attribute format: Decimal

Attribute value:

Attribute Example - WING-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*:**



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

Attributes:

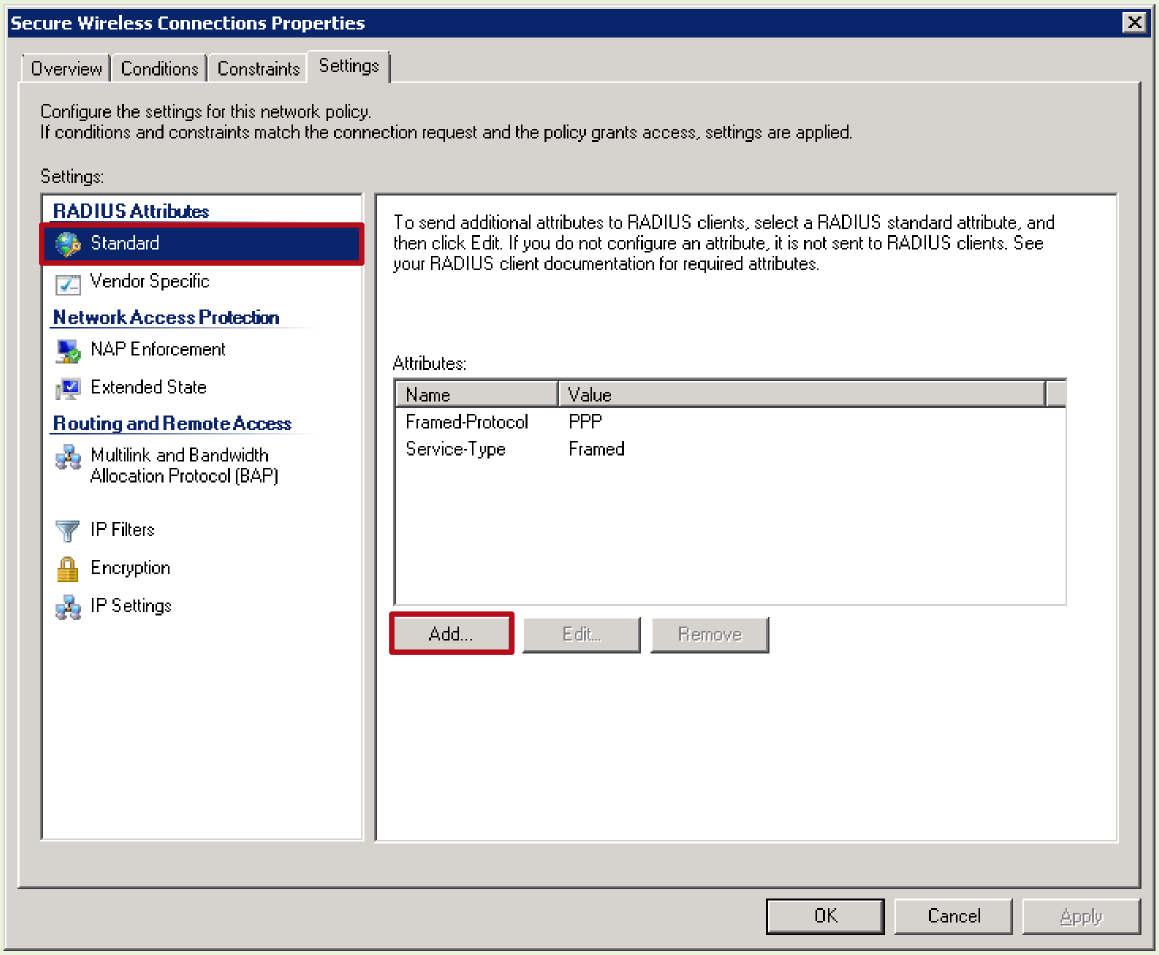
Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Vendor-Specific	RADIUS Standard	MOTO-DOT1X, Engine

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*:



Secure Wireless Connections Properties

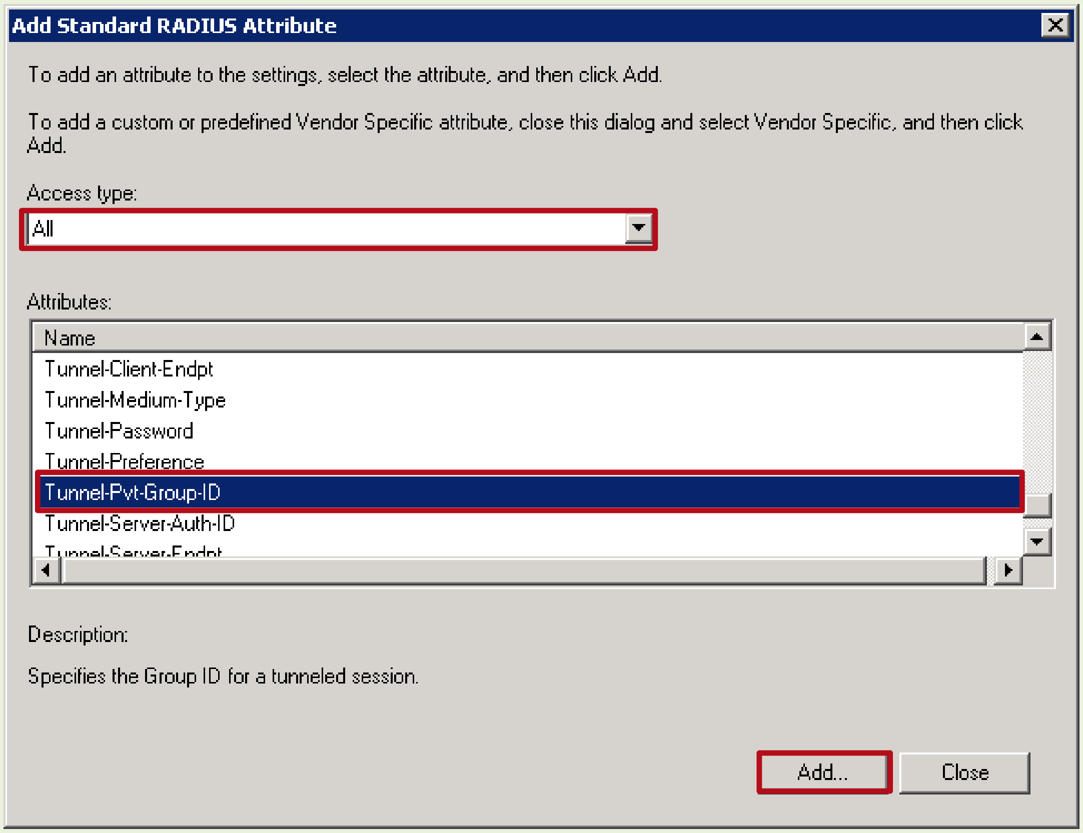
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

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

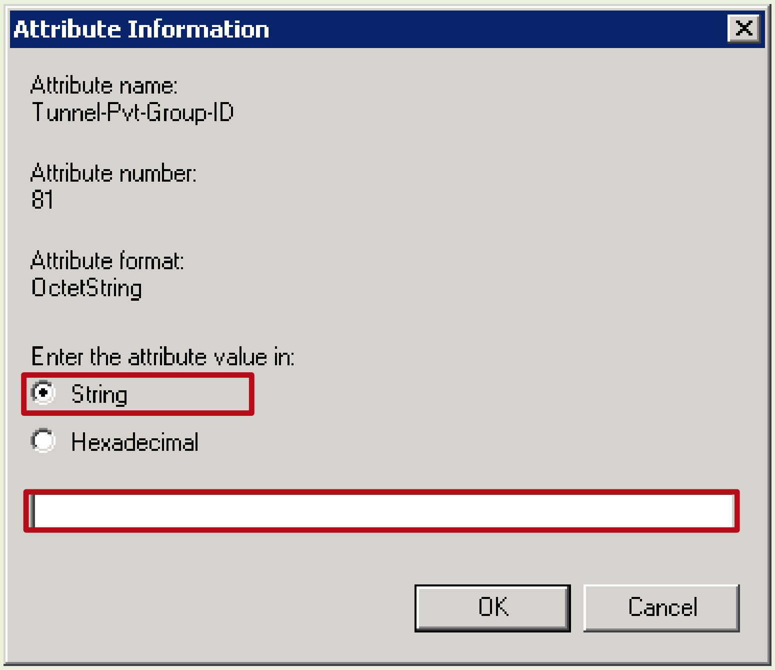
Attributes:

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.

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

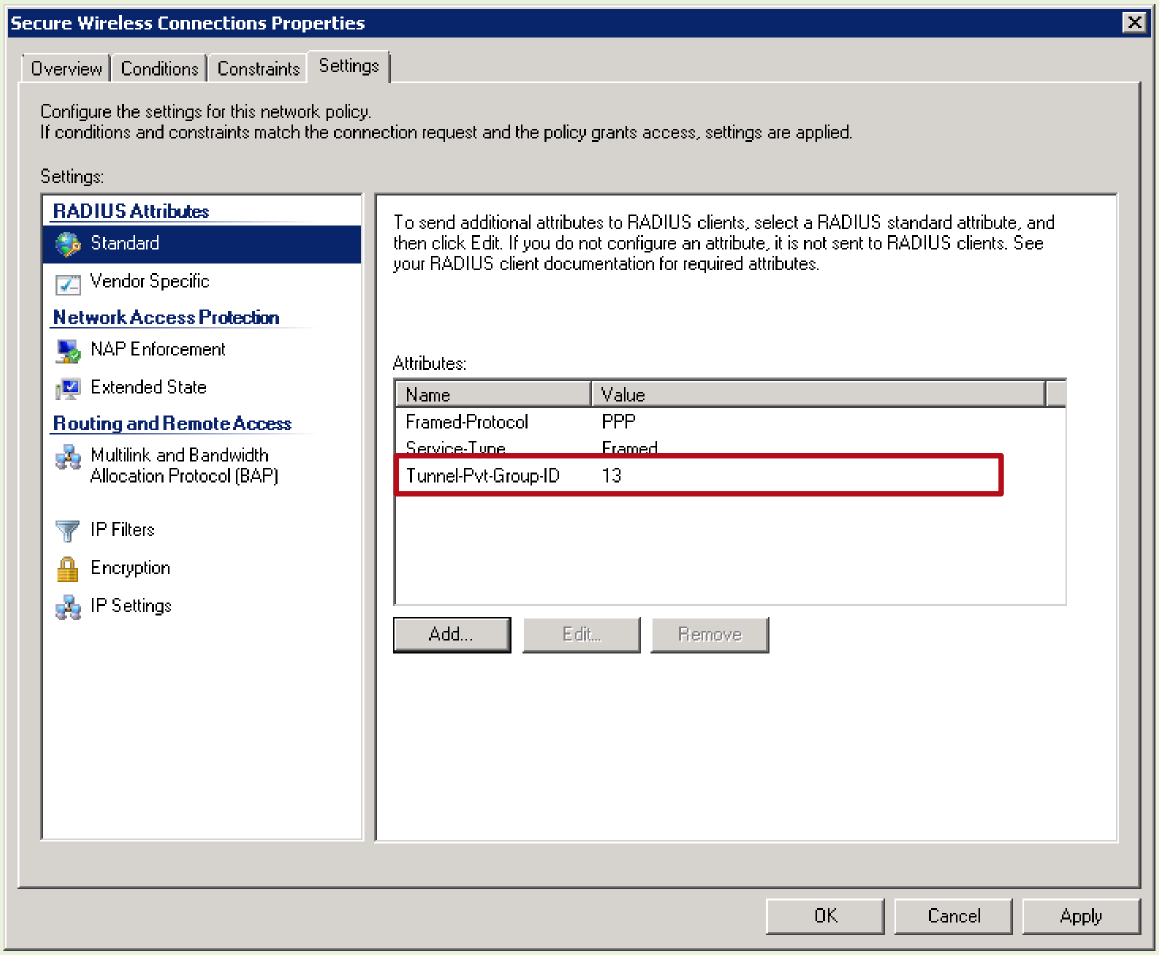
Attribute name:
Tunnel-Pvt-Group-ID

Attribute number:
81

Attribute format:
OctetString

Enter the attribute value in:
● String
○ Hexadecimal

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



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

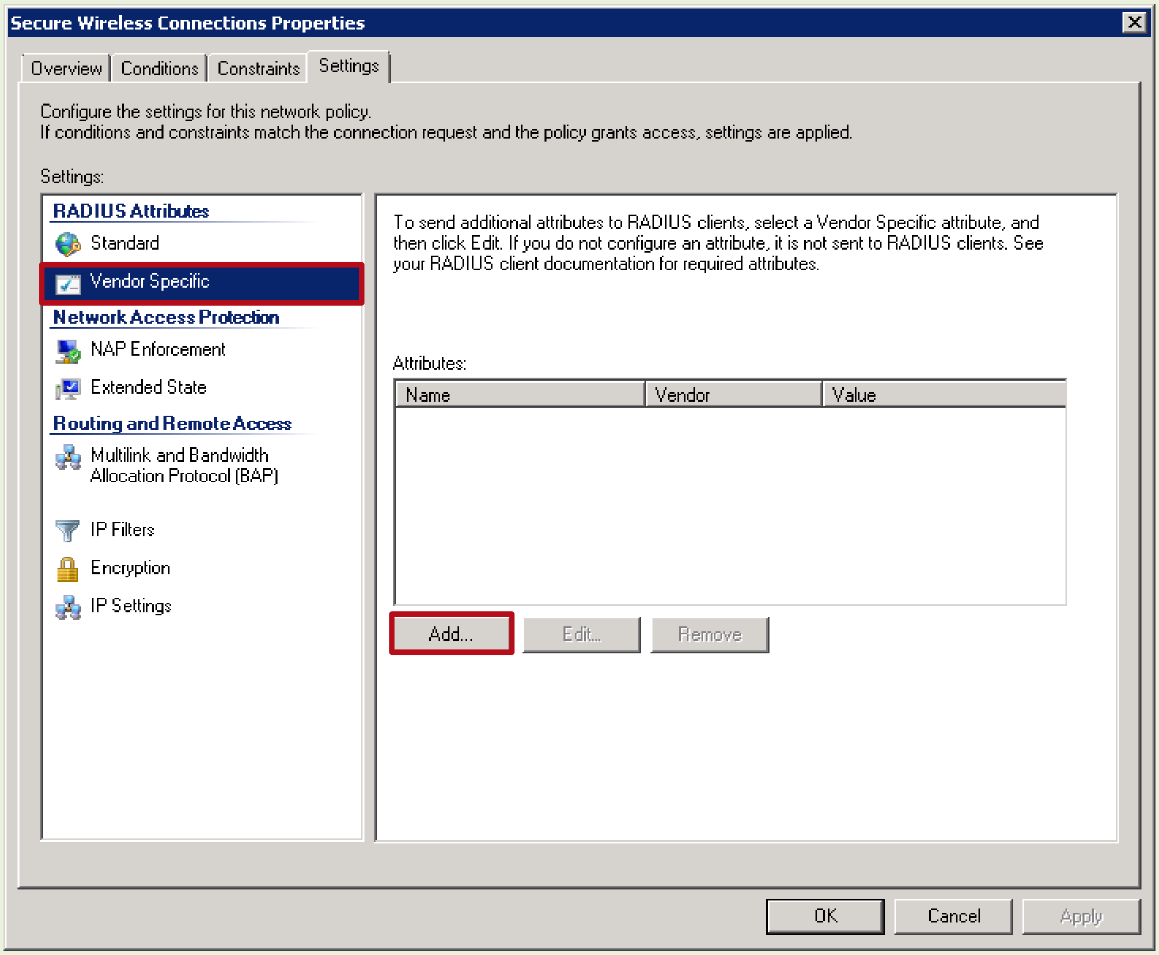
Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Pvt-Group-ID	13

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*:



Secure Wireless Connections Properties

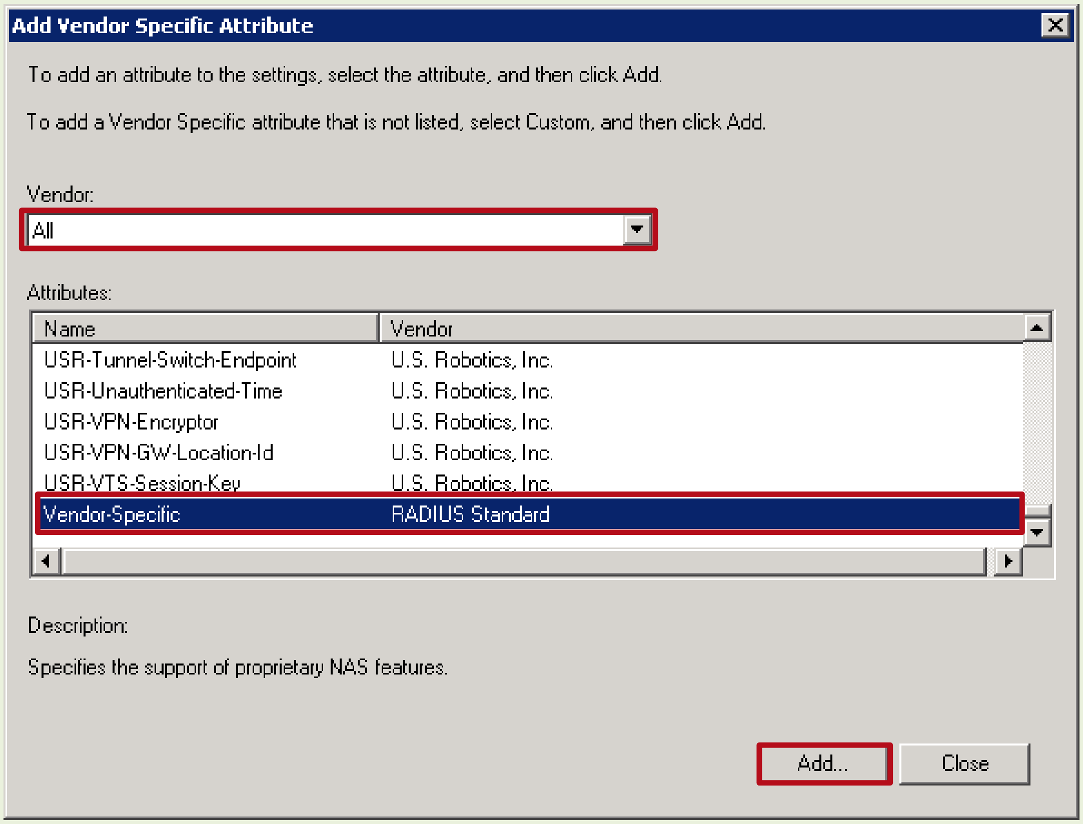
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value

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

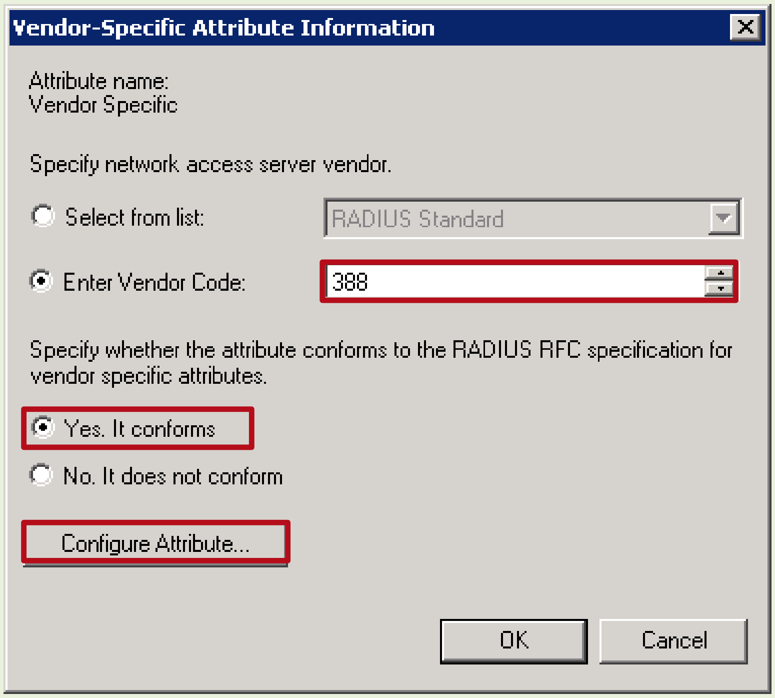
Attributes:

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.

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

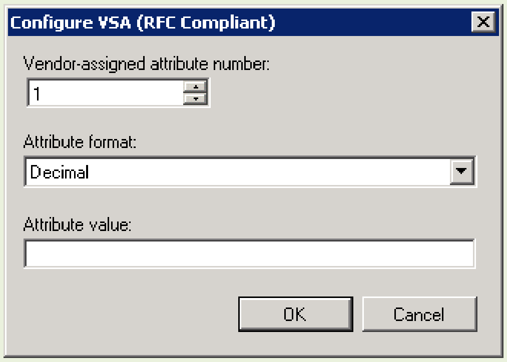
● Enter Vendor Code: 388

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

● Yes. It conforms

○ No. It does not conform

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*:**



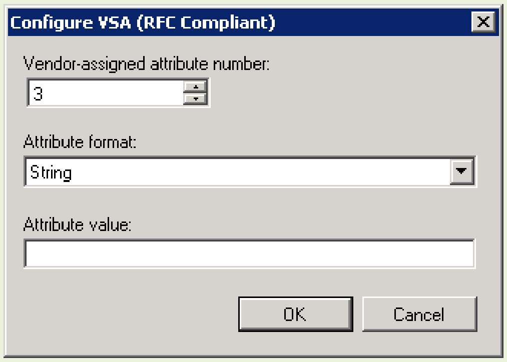
Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 1

Attribute format: Decimal

Attribute value:

Attribute Example - WING-Admin-Role



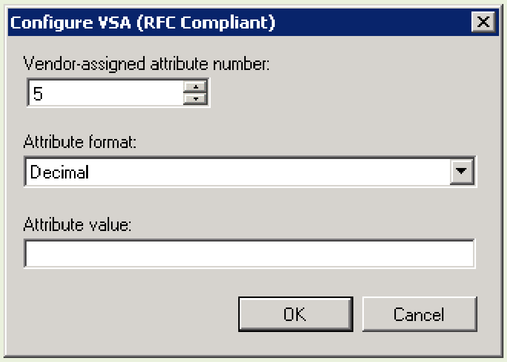
Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 3

Attribute format: String

Attribute value:

Attribute Example - WING-Allowed-SSID



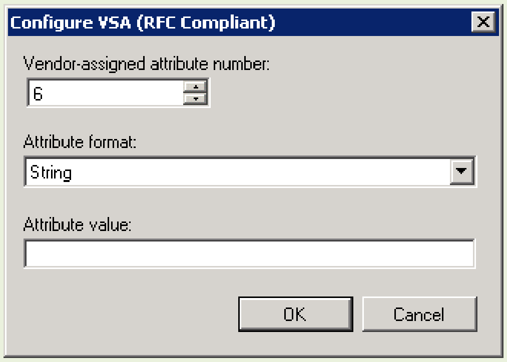
Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 5

Attribute format: Decimal

Attribute value:

Attribute Example - WING-QoS-Profile



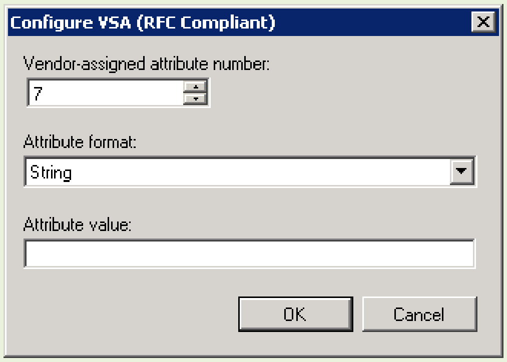
Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 6

Attribute format: String

Attribute value:

Attribute Example - WING-Allowed-Radio



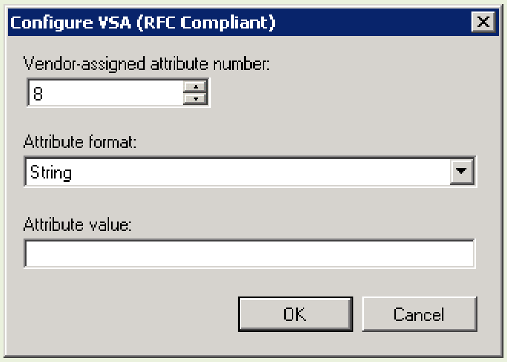
Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 7

Attribute format: String

Attribute value:

Attribute Example - WING-Expiry-Date-Time



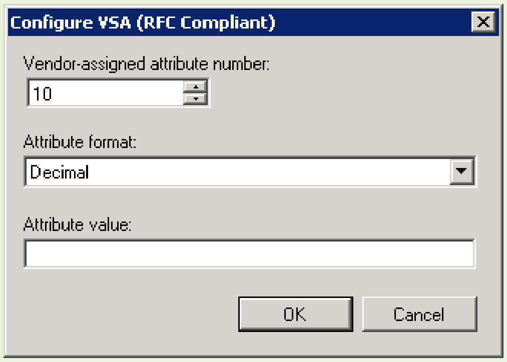
Configure VSA (RFC Compliant)

Vendor-assigned attribute number: 8

Attribute format: String

Attribute value:

Attribute Example - WING-Start-Date-Time

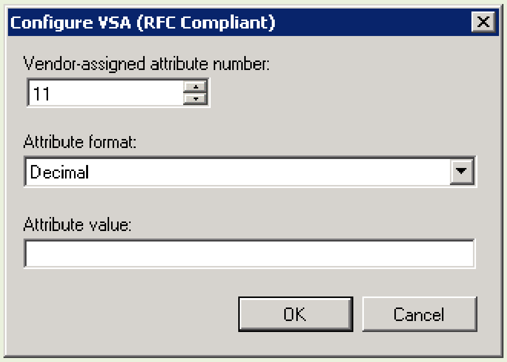


Vendor-assigned attribute number: 10

Attribute format: Decimal

Attribute value:

Attribute Example - WING-Downlink-Limit

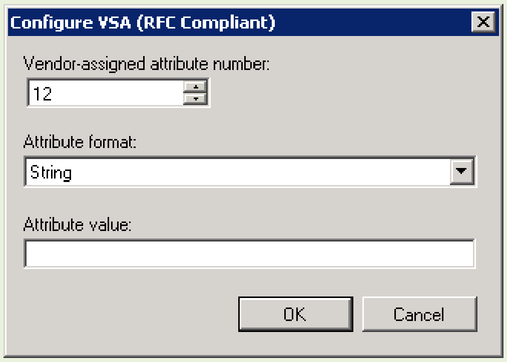


Vendor-assigned attribute number: 11

Attribute format: Decimal

Attribute value:

Attribute Example - WING-Uplink-Limit

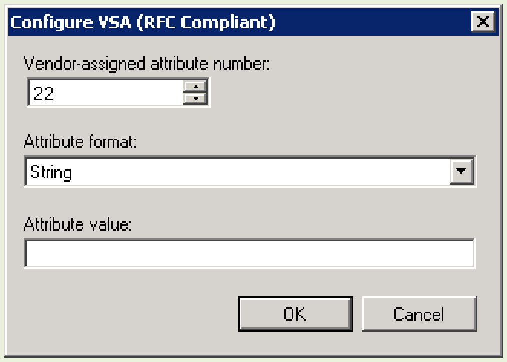


Vendor-assigned attribute number: 12

Attribute format: String

Attribute value:

Attribute Example - WING-User-Group

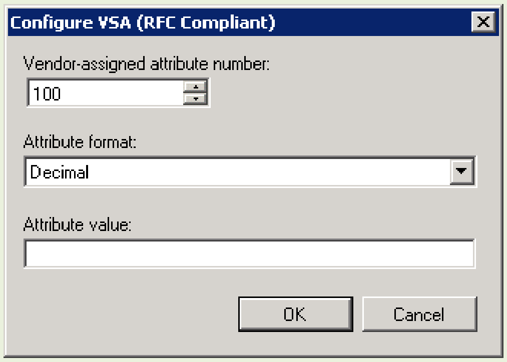


Vendor-assigned attribute number: 22

Attribute format: String

Attribute value:

Attribute Example - WING-VLAN-Name



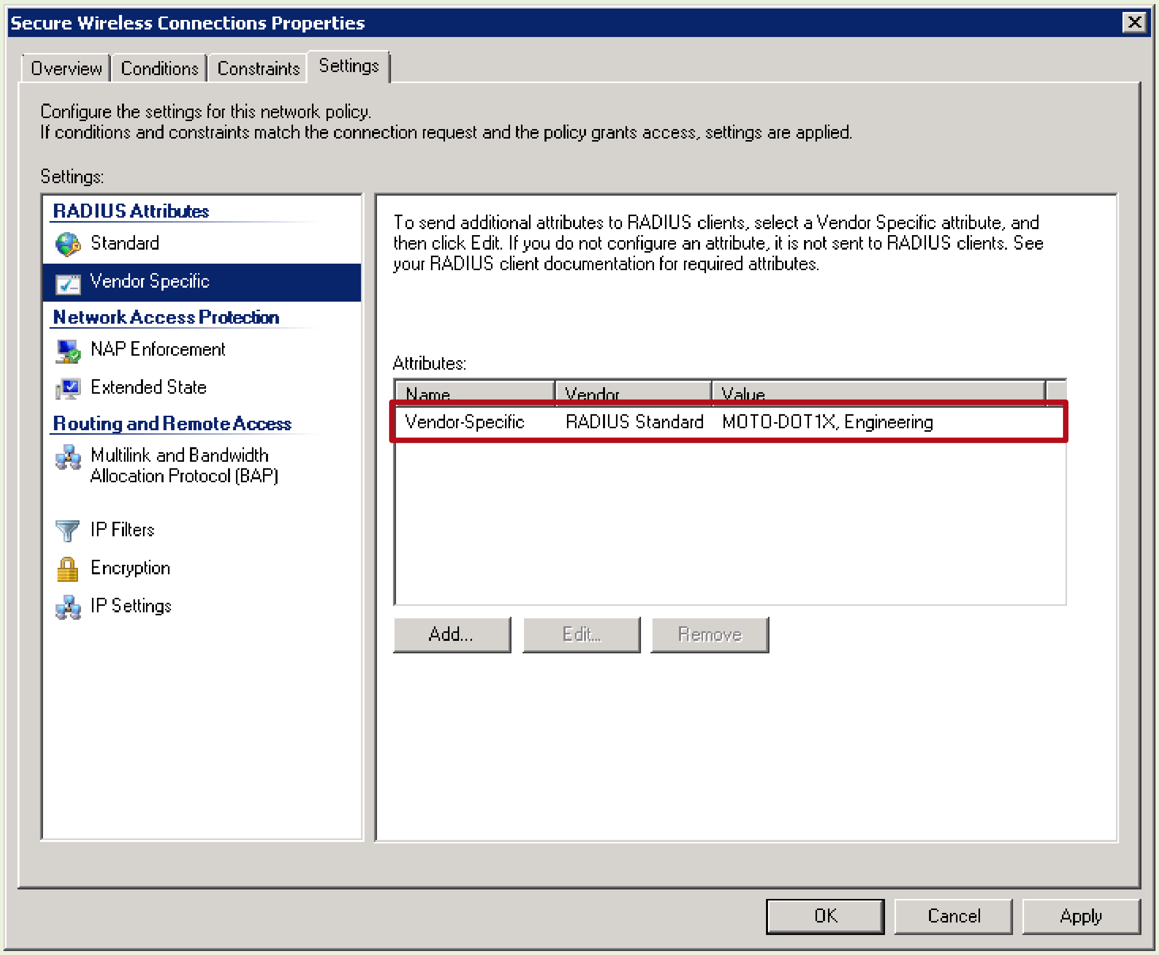
Vendor-assigned attribute number: 100

Attribute format: Decimal

Attribute value:

Attribute Example - WING-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*:**



Secure Wireless Connections Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	MOTO-DOT1X, Engineering