	• **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop down list : • **SNMPv2c Only** – Enables SNMP v2 community protocol. • **SNMPv3 Only** – Enables SNMP v3 protocol. It is secured communication protocol. • **SNMPv2c and SNMPv3** – It enables both the protocols.
Telnet	This option allows to **Enable** and **Disable** Telnet access to the Radio.
FTP	This option allows to **Enable** and **Disable** FTP access to the Radio.
TFTP	This option allows to **Enable** and **Disable** TFTP access to the Radio.

SM Authentication Mode – Require RADIUS or Follow AP

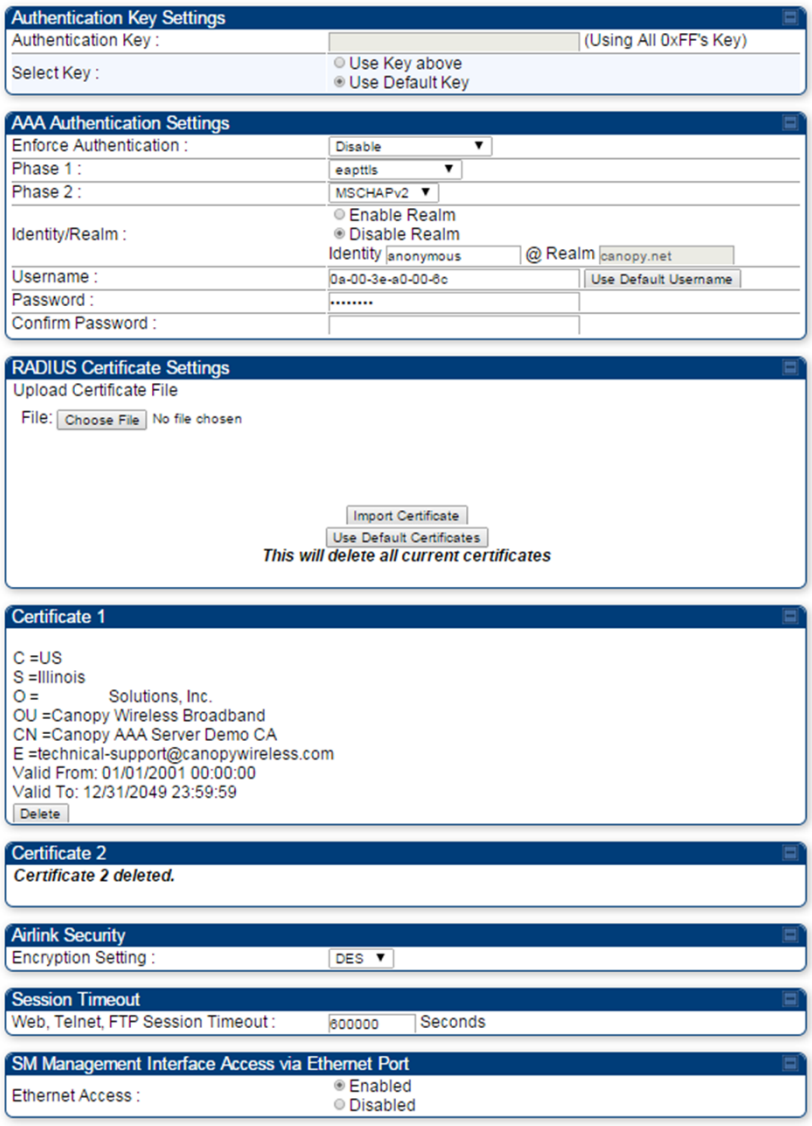
If it is desired that a SM will only authenticate to an AP that is using RADIUS, on the SM's Configuration Security tab set **Enforce Authentication** to **AAA**. With this enabled, SM does not register to an AP that has any **Authentication Mode** other than **RADIUS AAA** selected.

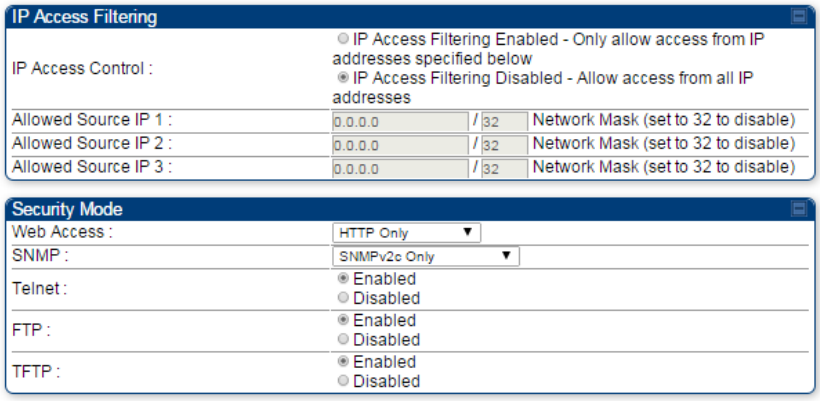
If it is desired that a SM use the authentication method configured on the AP it is registering to, set **Enforce Authentication** to **Disabled.** With **Enforce Authentication** disabled, a SM will attempt to register using whichever **Authentication Mode** is configured on the AP it is attempting to register to.

Note

Having SMs to use RADIUS by enabling **Enforce Authentication** avoids the security issue of SMs possibly registering to "rogue" APs, which have authentication disabled.

Table 171 SM Security tab attributes





Attribute	Meaning
Authentication Key	The authentication key is a 32-character hexadecimal string used when **Authentication Mode** is set to **AP PreShared Key**. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF.
Select Key	This option allows operators to choose which authentication key is used: **Use Key above** means that the key specified in **Authentication Key** is used for authentication **Use Default Key** means that a default key (based off of the SM's MAC address) is used for authentication
Enforce Authentication	The SM may enforce authentication types of **AAA** and **AP Pre-sharedKey**. The SM will not finish the registration process if the AP is not using the configured authentication method (and the SM locks out the AP for 15 minutes). Enforce Authentication default setting is **Disable.**
Phase 1	The protocols supported for the **Phase 1** (Outside Identity) phase of authentication are EAPTTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) or MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).
Phase 2	Select the desired **Phase 2** (Inside Identity) authentication protocol from the **Phase 2** options of **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol), and **MSCHAP** (Microsoft's version of CHAP, version 2 is used). The protocol must be consistent with the authentication protocol configured on the RADIUS server.

Identity/Realm	If Realms are being used, select **Enable Realm** and configure an outer identity in the **Identity** field and a Realm in the **Realm** field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default **Identity** is "anonymous". The **Identity** can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default **Realm** is "canopy.net". The **Realm** can also be up to 128 non-special alphanumeric characters. Configure an outer Identity in the **Username** field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity **Username** is "anonymous". The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Username	Enter a **Username** for the SM. This must match the username configured for the SM on the RADIUS server. The default **Username** is the SM's MAC address. The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Password Confirm Password	Enter the desired password for the SM in the **Password** and **Confirm Password** fields. The **Password** must match the password configured for the SM on the RADIUS server. The default **Password** is "password". The **Password** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Upload Certificate File	To upload a certificate manually to a SM, first load it in a known place on your PC or network drive, then click on a **Delete** button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on **Choose File,** browse to the location of the certificate, and click the **Import Certificate** button, and then reboot the radio to use the new certificate. When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used. The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system. Up to 2 certificates can be resident on a SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate's description block on the Configuration > Security tab. To restore the 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate Settings** parameter block and reboot the radio.

Encryption Setting	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs. **None** provides no encryption on the air link. **DES** (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system. **AES** (Advanced Encryption Standard)**:** An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet or ftp access to the AP.
Ethernet Access	If you want to prevent any device that is connected to the Ethernet port of the SM from accessing the management interface of the SM, select **Ethernet Access Disabled**. This selection disables access through this port to via HTTP (the GUI), SNMP, telnet, FTP, and TFTP. With this selection, management access is available through only the RF interface via either an IP address (if **Network Accessibility** is set to **Public** on the SM) or the Session Status or Remote Subscribers tab of the AP. See **IP Access Control** below. If you want to allow management access through the Ethernet port, select **Ethernet Access Enabled**. This is the factory default setting for this parameter.
IP Access Control	You can permit access to the AP from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address
Allowed Source IP 1 Allowed Source IP 2 Allowed Source IP 3	If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the AP from any IP address. You may populate as many as all three. If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list: • **HTTP Only** – provides non-secured web access. The radio to be accessed via http://<IP of Radio>.

	• **HTTPS Only** – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop down list : • **SNMPv2c Only** – Enables SNMP v2 community protocol. • **SNMPv3 Only** – Enables SNMP v3 protocol. It is secured communication protocol. • **SNMPv2c and SNMPv3** – It enables both the protocols.
Telnet	This option allows to **Enable** and **Disable** Telnet access to the Radio.
FTP	This option allows to **Enable** and **Disable** FTP access to the Radio.
TFTP	This option allows to **Enable** and **Disable** TFTP access to the Radio.

SM - Phase 1 (Outside Identity) parameters and settings

The protocols supported for the **Phase 1** (Outside Identity) phase of authentication are **eapttls** (Extensible Authentication Protocol Tunneled Transport Layer Security) and **eapMSChapV2** (Extensible Authentication Protocol – Microsoft Challenge-Handshake Authentication Protocol).

Configure an outer Identity in the **Username** field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity **Username** is "anonymous". The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters. If Realms are being used in the RADIUS system (**eapttls** only), select **Enable Realm** and configure an outer identity in the **Identity** field and a Realm in the **Realm** field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default **Identity** is "anonymous". The **Identity** can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default **Realm** is "canopy.net". The **Realm** can also be up to 128 non-special alphanumeric characters.

SM - Phase 2 (Inside Identity) parameters and settings

If using **eapttls** for Phase 1 authentication, select the desired **Phase 2** (Inside Identity) authentication protocol from the **Phase 2** options of **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol), and **MSCHAPv2 (**Microsoft's version of CHAP). The protocol must be consistent with the authentication protocol configured on the RADIUS server. Enter a **Username** for the SM. This must match the username configured for the SM on the RADIUS server. The default **Username** is the SM's MAC address. The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.

Enter the desired password for the SM in the **Password** and **Confirm Password** fields. The **Password** must match the password configured for the SM on the RADIUS server. The default **Password** is "password". The **Password** can be up to 128 non-special (no diacritical markings) alphanumeric characters.

Handling Certificates

Managing SM Certificates via the SM GUI

The default public Canopy certificates are loaded into SMs upon factory software installation. The default certificates are not secure and are intended for use during lab and field trials as part of gaining experience with the RADIUS functionalities or as an option during debug. For secure operation, an operator will want to create or procure their own certificates. Resetting a SM to its factory defaults will remove the current certificates and restore the default certificates.

Up to two certificates can be resident on a SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate's description block on the Configuration > Security tab. To restore the 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate Settings** parameter block and reboot the radio.

To upload a certificate manually to a SM, first load it in a known place on your PC or network drive, then click on a **Delete** button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on **Choose File,** browse to the location of the certificate, and click the **Import Certificate** button, and then reboot the radio to use the new certificate.

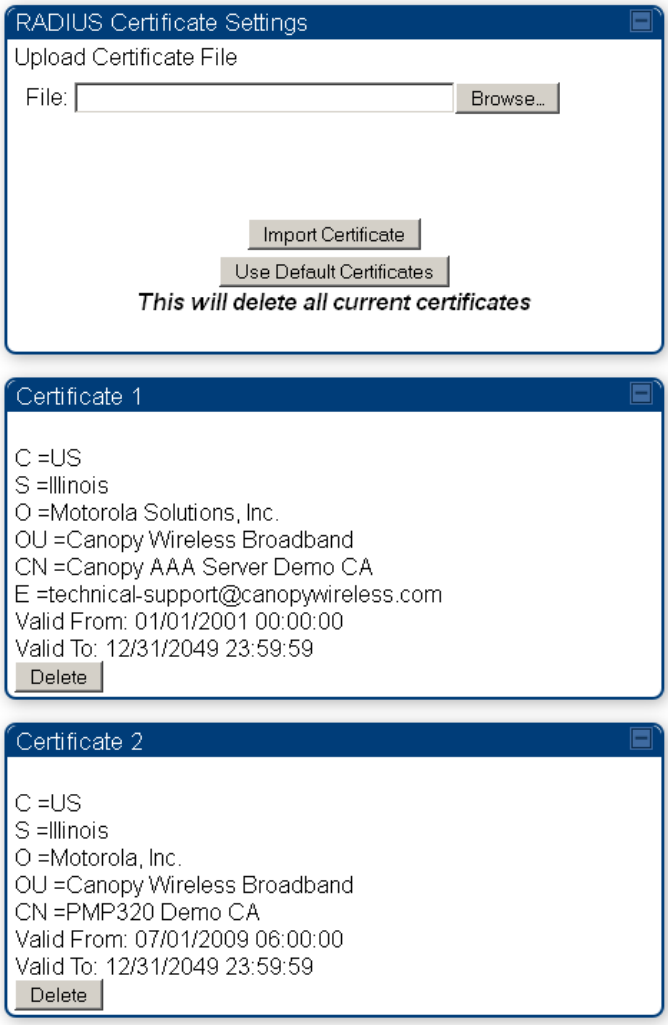
When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used.

The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system.

Note

Root certificates of more than one level (Example - a certificate from someone who received their CA from Verisign) fails. Certificates must be either root or self-signed.

Figure 145 SM Certificate Management



Configuring RADIUS servers for SM authentication

Your RADIUS server must be configured to use the following:

- EAPTTLS or MSCHAPv2 as the Phase 1/Outer Identity protocol.
- If **Enable Realm** is selected on the SM's **Configuration** > **Security** tab, then the same Realm appears there (or access to it).
- The same Phase 2 (Inner Identity) protocol as configured on the SM's **Configuration** > **Security** tab under Phase 2 options.
- The username and password for each SM configured on each SM's **Configuration > Security** tab.
- An IP address and NAS shared secret that is the same as the IP address and **Shared Secret** configured on the AP's **Configuration > Security** tab for that RADIUS server.

- A server private certificate, server key, and CA certificate that complement the public certificates distributed to the SMs, as well as the Canopy dictionary file that defines Vendor Specific Attributes (VSAa). Default certificate files and the dictionary file are available from the software site: https://support.cambiumnetworks.com/files/pmp450 after entering your name, email address, and either Customer Contract Number or the MAC address of a module covered under the 12 month warranty.

Optionally, operators may configure the RADIUS server response messages (Accept or Reject) so that the user has information as to why they have been rejected. The AP displays the RADIUS Authentication Reply message strings in the Session Status list as part of each SM's information. The SM will show this string (listed as Authentication Response on the SM GUI) on the main Status page in the Subscriber Module Stats section.

Note

Aradial AAA servers only support operator-configurable Authentication Accept responses, not Authentication Reject responses.

Assigning SM management IP addressing via RADIUS

Operators may use a RADIUS AAA server to assign management IP addressing to SM modules (framed IP address). SMs now interpret attributes Framed-IP-Address, Framed-IP-Netmask, and Cambium-Canopy-Gateway from RADIUS. The RADIUS dictionary file has been updated to include the Cambium-Canopy-Gateway attribute and is available on the Cambium Software Support website.

In order for these attributes to be assigned and used by the SM, the following must be true:

- The system is configured for AAA authentication
- The SM is *not* configured for DHCP on its management interface. If DHCP is enabled and these attributes are configured in the RADIUS server, the attributes is ignored by the SM.
- The SM management interface must be configured to be publically accessible. If the SM is configured to have local accessibility, the management interface will still be assigned the framed addressing, and the SM iscome publicly accessible via the assigned framed IP addressing.
- When using these attributes, for the addressing to be implemented by the SM operators must configure Framed-IP-Address in RADIUS. If Framed-IP-Address is not configured but Framed-IP-Netmask and/or Cambium-Canopy-Gateway is configured, the attributes is ignored. In the case where only the Framed-IP-Address is configured, Framed-IP-Netmask defaults to 255.255.0.0 (NAT disabled) / 255.255.255.0 (NAT enabled) and Cambium-Canopy-Gateway defaults to 0.0.0.0.

Configuring RADIUS server for SM configuration

Canopy Vendor Specific Attributes (VSAs) along with VSA numbers and other details are listed in Table 172. The associated SM GUI page, tab and parameter are listed to aid cross-referencing and understanding of the VSAs.

A RADIUS dictionary file is available from the software site:

https://support.cambiumnetworks.com/files/pmp450

The RADIUS dictionary file defines the VSAs and their values and is usually imported into the RADIUS server as part of server and database setup.

Note

Beginning with System Release 12.0.2, two RADIUS dictionary files are available on the Cambium website – "RADIUS Dictionary file – Cambium" and "RADIUS Dictionary file – Motorola".

In addition to a renaming of attributes, the Cambium-branded dictionary file contains two new VSAs for controlling uplink and downlink Maximum Burst Data Rate (these VSAs are listed below in Table 172).

If you are transitioning from the Motorola-branded dictionary file to the Cambium-branded dictionary file, ensure that all RADIUS profiles containing Motorola-Canopy attribute references are updated to include Cambium-Canopy attribute references (for all applicable VSAs listed in Table 172). Also, ensure that all RADIUS configuration files reference the new dictionary file (as an alternative, operators may rename the Cambium-branded dictionary file to the filename currently in use by the RADIUS server). Once the profiles are updated and the new Cambium-branded dictionary file is installed on the RADIUS server, restart the RADIUS server to ensure that the new VSAs and attribute names are enabled.

Table 172 RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Required	Value	
MS-MPPE-Send-Key*	26.311.16	-	Y	-	
-				-	-
MS-MPPE-Recv-Key*	26.311.17	-	Y	-	
-				-	-
Cambium-Canopy-LPULCIR	26.161.1	integer	N	0-65535 kbps	
Configuration > Quality of Service > Low Priority Uplink CIR				0 kbps	32 bits
Cambium-Canopy-LPDLCIR	26.161.2	integer	N	0-65535 kbps	
Configuration > Quality of Service > Low Priority Downlink CIR				0 kbps	32 bits
Cambium-Canopy-HPULCIR	26.161.3	integer	N	0-65535 kbps	
Configuration > Quality of Service > Hi Priority Uplink CIR				0 kbps	32 bits
Cambium-Canopy-HPDLCIR	26.161.4	integer	N	0-65535 kbps	
Configuration > Quality of Service > Hi Priority Uplink CIR				0 kbps	32 bits
Cambium-Canopy-HPENABLE	26.161.5	integer	N	0-disable, 1-enable	
Configuration > Quality of Service > Hi Priority Channel Enable/Disable				0	32 bits
26.161.6		integer	N	0-100000 kbps	

Configuration > Quality of Service > Sustained Uplink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-ULBL	26.161.7	integer	N	0-2500000 kbps	
Configuration > Quality of Service > Uplink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-DLBR	26.161.8	integer	N	0-100000 kbps	
Configuration > Quality of Service > Sustained Downlink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-DLBL	26.161.9	integer	N	0-2500000 kbps	
Configuration > Quality of Service > Downlink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-VLLEARNEN	26.161.14	integer	N	0-disable, 1-enable	
Configuration > VLAN > Dynamic Learning				1	32 bits
Cambium-Canopy-VLFRAMES	26.161.15	integer	N	0-all, 1-tagged, 2-untagged	
Configuration > VLAN > Allow Frame Types				0	32 bits
Cambium-Canopy-VLIDSET	26.161.16	integer	N	VLAN Membership (1-4094)	
Configuration > VLAN Membership				0	32 bits
Cambium-Canopy-VLAGETO	26.161.20	integer	N	5 - 1440 minutes	
Configuration > VLAN > VLAN Aging Timeout				25 mins	32 bits
Cambium-Canopy-VLIGVID	26.161.21	integer	N	1 – 4094	
Configuration > VLAN > Default Port VID				1	32 bits
Cambium-Canopy-VLMGVID	26.161.22	integer	N	1 – 4094	
Configuration > VLAN > Management VID				1	32 bits
Cambium-Canopy-VLSMMGPASS	26.161.23	integer	N	0-disable, 1-enable	
Configuration > VLAN > SM Management VID Pass-through				1	32 bits
Cambium-Canopy-BCASTMIR	26.161.24	integer	N	0-100000 kbps, 0=disabled	
Configuration > Quality of Service > Broadcast/Multicast Uplink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-Gateway	26.161.25	ipaddr	N	-	
Configuration > IP > Gateway IP Address				0.0.0.0	-

Cambium-Canopy-ULMB	26.161.26	integer	N	0-100000 kbps	
Configuration > Quality of Service > Max Burst Uplink Data Rate				0	32 bits
Cambium-Canopy-DLMB	26.161.27	integer	N	0-100000 kbps	
Configuration > Quality of Service > Max Burst Downlink Data Rate				0	32 bits
Cambium-Canopy-UserLevel	26.161.50	integer	N	1-Technician, 2-Installer, 3-Administrator	
Account > Add User > Level				0	32 bits
Cambium-Canopy-DHCP-State	26.161.31	integer	N	1-Enable	
Configuration > IP > DHCP state				1	32 bits
Cambium-Canopy-BCASTMIRUNITS	26.161.28	integer	N		
Configuration > QoS > Broadcast Downlink CIR				0	32 bits
Cambium-Canopy-ConfigFileImportUrl	26.161.29	string	N		
Configuration > Unit Settings				0	32 bits
Cambium-Canopy-ConfigFileExportUrl	26.161.30	string	N		
Configuration > Unit Settings				0	32 bits
Cambium-Canopy-UserMode	26.161.51	integer	N	1=Read-Only 0=Read-Write	
Account > Add User > User Mode				0	32 bits

(*) Contains key for encrypting packets sent by the NAS to the remote host (for Microsoft Point-to-Point Encryption Protocol).

Note

VSA numbering:

26 connotes Vendor Specific Attribute, per RFC 2865

26.311 is Microsoft Vendor Code, per IANA

Configuring RADIUS server for SM configuration using Zero Touch feature

The RADIUS VSA (Vendor Specific Attributes) is updated for Zero Touch feature. This feature enables the ability for a SM to get its configuration via RADIUS VSA. The RADIUS VSA is updated for an URL which points to the configuration file of SM (see Table 172 for list of VSA).

The RADIUS will push the vendor specific attribute to SM after successful authentication. The VSA contains URL of config file which will redirect SM to download configuration. If there is any change in SM confirmation, the SM will reboot automatically after applying the configuration.

The RADIUS VSA attributes concerning Zero Touch are as follows:

```
VSA                                    Type       String

Cambium-Canopy-ConfigFileImportUrl (29) string  Maximum Length 127
characters.
Cambium-Canopy-ConfigFileExportUrl (30) string  Maximum Length 127
characters.
```

The updated RADIUS dictionary can be downloaded from below link:

https://support.cambiumnetworks.com/files/pmp450/

Note

The feature is not applicable to the AP.

Using RADIUS for centralized AP and SM user name and password management

AP – Technician/Installer/Administrator Authentication

To control technician, installer, and administrator access to the AP from a centralized RADIUS server:

Procedure 28 Centralized user name and password management for AP

1. Set **Authentication Mode** on the AP's Configuration > Security tab to **RADIUS AAA**
2. Set **User Authentication Mode** on the AP's Account > User Authentication tab (the tab only appears after the AP is set to RADIUS authentication) to **Remote** or **Remote then Local**.
   - **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed.
   - **Remote**: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **RADIUS AAA Authentication Mode** selected. For up to 2 minutes a test pattern is displayed until the server responds or times out.
   - **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.

~~**Figure 137** User Authentication and Access Tracking tab of the AP~~

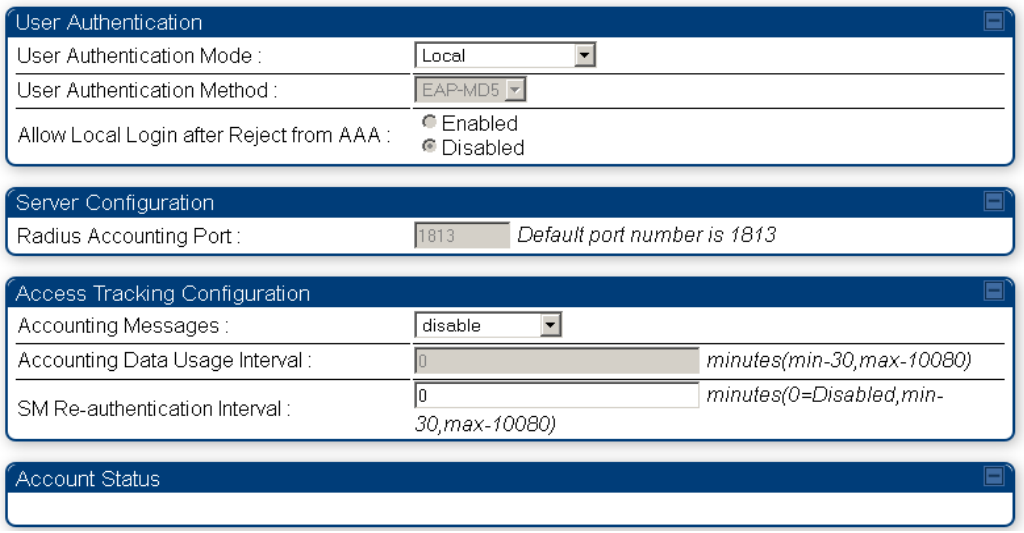
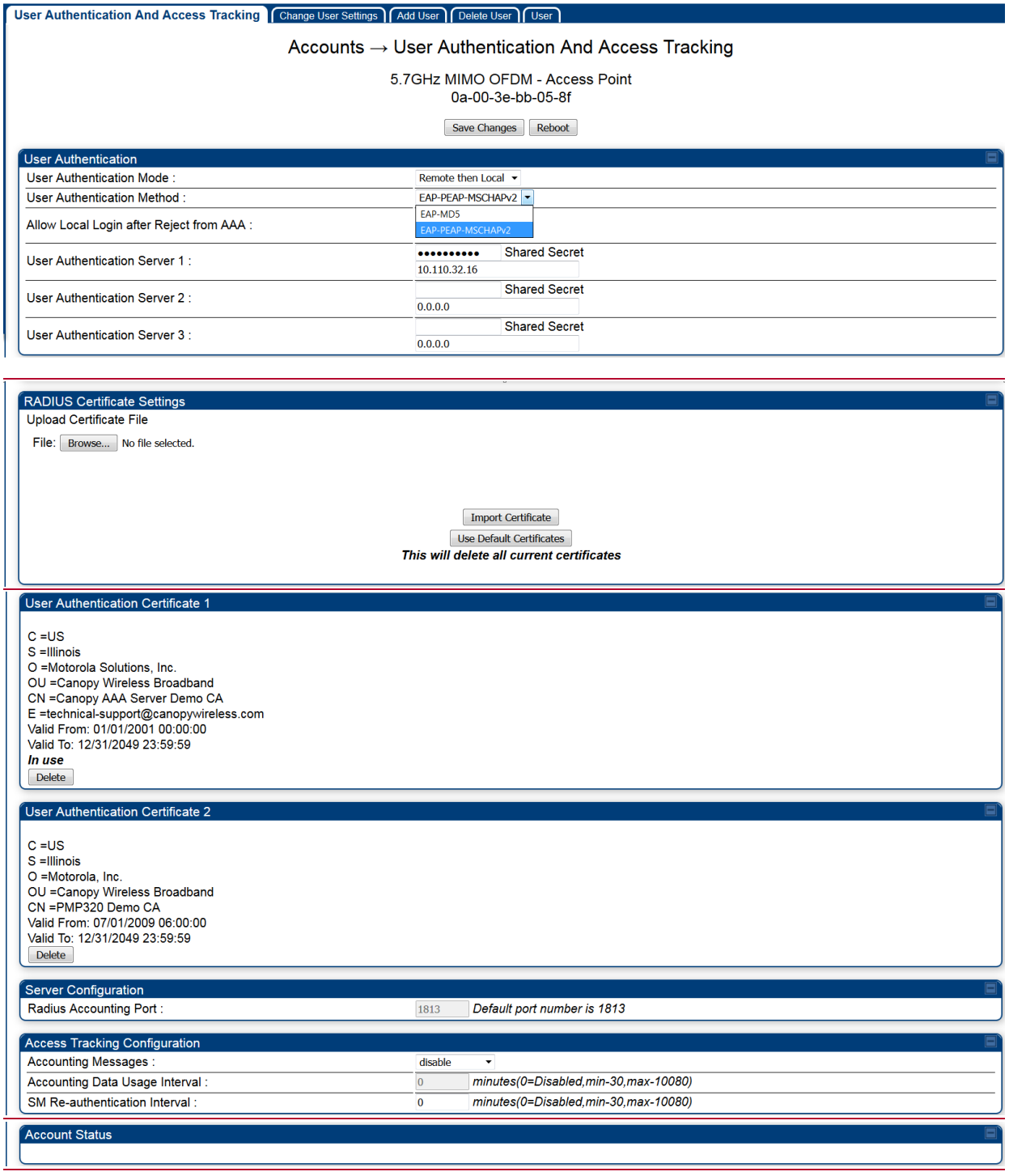


Table 173 AP User Authentication and Access Tracking attributes



Attribute	Meaning
User Authentication Mode	• **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed. • **Remote**: Authentication by the centralized RADIUS server is required to gain access to the AP. For up to 2 minutes a test pattern is displayed until the server responds or times out.

	• **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the AP.
User Authentication Method	The user authentication method employed by the radios: • EAP-MD5 • EAP-PEAP-MSCHAPv2.
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user is allowed to login locally to the radio's management interface.
User Authentication Server 1	The IP address and the shared secret key of the User authentication RADIUS server 1.
User Authentication Server 2	The IP address and the shared secret key of the User Authentication Server 2 configured in RADIUS Server.
User Authentication Server 3	The IP address and the shared secret key of the User Authentication Server 3 configured in RADIUS Server.
RADIUS Certificate Settings	Import Cetificate – browse and select the file to be uploaded and click on "Import Certificate" to import a new certificate. Use Default Certificates – use the preloaded default certificates.
User Authentication Certificate 1	Cerificate provided by default for User authentication.
User Authentication Certificate 2	Cerificate provided by default for User authentication.
Radius Accounting Port	The destination port on the AAA server used for Radius accounting communication.
Accounting Messages	disable – no accounting messages are sent to the RADIUS server deviceAccess – accounting messages are sent to the RADIUS server regarding device access (see Table 175). dataUsage – accounting messages are sent to the RADIUS server regarding data usage (see Table 175). all –
Accounting Data Usage Interval	The interval for which accounting data messages are sent from the radio to the RADIUS server. If 0 is configured for this parameter, no data usage messages are sent.
SM Re-authentication Interval	The interval for which the SM will re-authenticate to the RADIUS server.
Account Status	Displays the account status.

SM – Technician/Installer/Administrator Authentication

The centralized user name and password management for SM is same as AP. Follow AP – Technician/Installer/Administrator Authentication on page 7-236 procedure.

Note

Remote access control is enabled only after the SM registers to an AP that has **Authentication Mode** set to **RADIUS AAA**. Local access control will always be used before registration and is used after registration if the AP is not configured for RADIUS.

Figure 146 User Authentication and Access Tracking tab of the SM

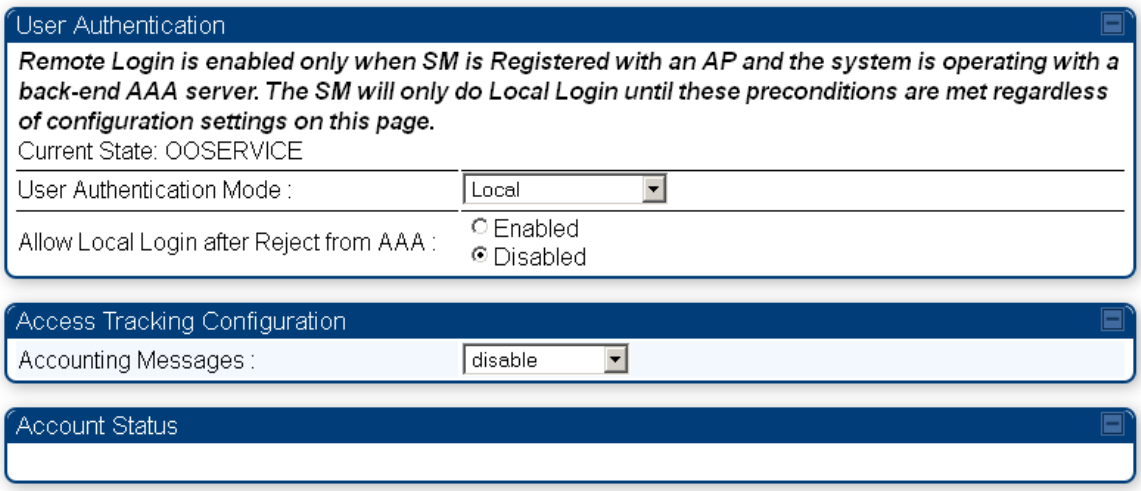
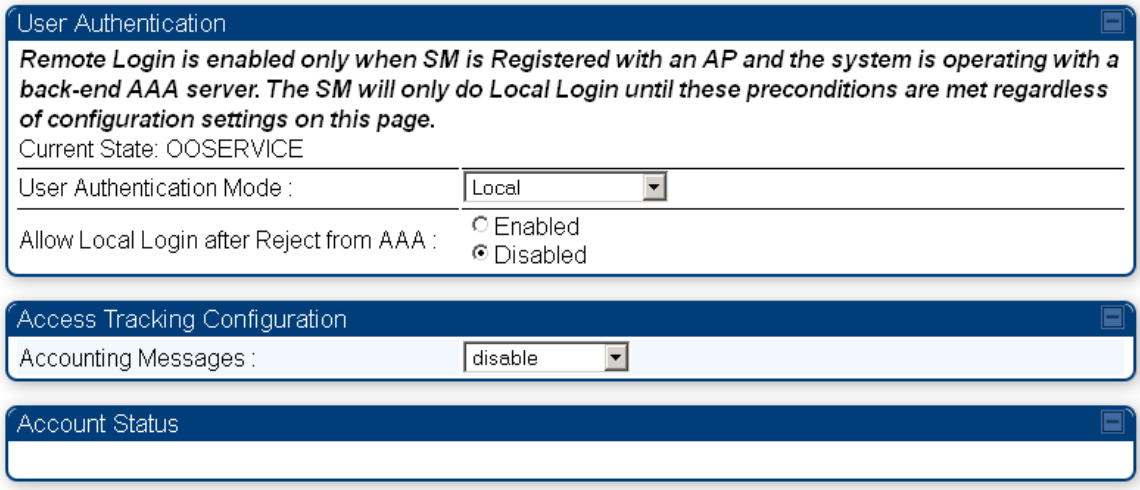


Table 174 SM User Authentication and Access Tracking attributes



Attribute	Meaning
User Authentication Mode	• **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed.

	• **Remote**: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **RADIUS AAA Authentication Mode** selected. For up to 2 minutes a test pattern is displayed until the server responds or times out. • **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user is allowed to login locally to the radio's management interface. It is applicable ONLY when the **User Authentication Mode** is set to "**Remote then Local**". **Note** When the radio User Authentication Mode is set to "Local" or "Remote", the Allow Local Login after Reject from AAA does not any effect.
Accounting Messages	• disable – no accounting messages are sent to the RADIUS server • deviceAccess – accounting messages are sent to the RADIUS server regarding device access (see Table 175).

Access Tracking

To track logon and logoff times on individual radios by technicians, installers, and administrators, on the AP or SM's **Account** > **User Authentication and Access Tracking** tab under **Accounting** (Access Tracking) set **Accounting Messages** to "deviceAccess".

Device Access Tracking is enabled separately from **User Authentication Mode**. A given AP or SM can be configured for both, either, or neither.

RADIUS Device Data Accounting

PMP 450 Platform systems include support for RADIUS accounting messages for usage-based billing. This accounting includes indications for subscriber session establishment, subscriber session disconnection, and bandwidth usage per session for each SM that connects to the AP. The attributes included in the RADIUS accounting messages are shown in the table below.

Table 175 Device data accounting RADIUS attributes

Sender	Message	Attribute	Value	Description
AP		Acct-Status-Type	1 - Start	

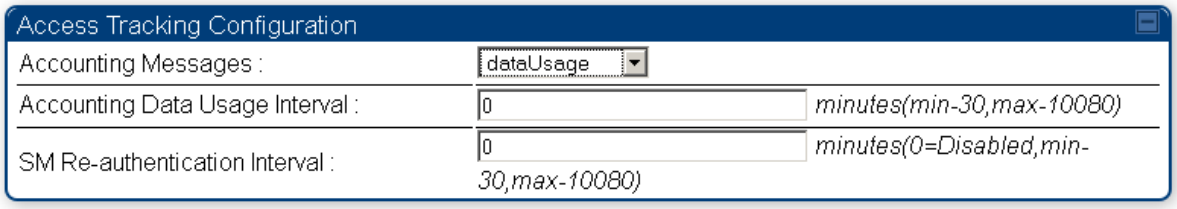
Sender	Message	Attribute	Value	Description
	Accounting-Request	Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	This message is sent every time a SM registers with an AP, and after the SM stats are cleared.
		Event-Timestamp	UTC time the event occurred on the AP	
AP	Accounting-Request	Acct-Status-Type	2 - Stop	This message is sent every time a SM becomes unregistered with an AP, and when the SM stats are cleared.
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
		Acct-Input-Octets	Sum of the input octets received at the SM over regular data VC and the high priority data VC (if enabled). Will not include broadcast.	
		Acct-Output-Octets	Sum of the output octets sent from the SM over regular data VC and the high priority data VC (if enabled).	
		Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Output-Gigawords	Number of times the Acct-Output-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Input-Packets	Sum of unicast and multicast packets that are sent to a particular SM over the regular data VC and the high priority data VC (if enabled). It will not include broadcast.	

Sender	Message	Attribute	Value	Description
		Acct-Output-Packets	Sum of unicast and multicast packets that are sent from a particular SM over the regular data VC and the high priority data VC (if enabled).	
		Acct-Session-Time	Uptime of the SM session.	
		Acct-Terminate-Cause	Reason code for session termination	
AP	Accounting-Request	Acct-Status-Type	3 - Interim-Update	This message is sent periodically per the operator configuration on the AP in seconds. Interim update counts are cumulative over the course of the session
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
		Acct-Input-Octets	Sum of the input octets sent to the SM over regular data VC and the high priority data VC (if enabled). Will not include broadcast.	
		Acct-Output-Octets	Sum of the output octets set from the SM over regular data VC and the high priority data VC (if enabled).	
		Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Output-Gigawords	Number of times the Acct-Output-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Session-Time	Uptime of the SM session.	

Sender	Message	Attribute	Value	Description
		Acct-Input-Packets	Sum of unicast and multicast packets that are sent to a particular SM over the regular data VC and the high priority data VC (if enabled). It will not include broadcast.	
		Acct-Output-Packets	Sum of unicast and multicast packets that are sent from a particular SM over the regular data VC and the high priority data VC (if enabled).	

The data accounting configuration is located on the AP's **Accounts** > **User Authentication and Access Tracking** GUI menu, and the AP's **Authentication Mode** must be set to **Radius AAA** for the menu to appear. The accounting may be configured via the AP GUI as shown in the figures below. By default accounting messages are not sent and the operator has the choice of configuring to send only Device Access accounting messages (when a user logs in or out of the radio), only Data Usage messages, or both. When Data Accounting is enabled, the operator must specify the interval of when the data accounting messages are sent (0 – disabled, or in the range of 30-10080 minutes). The default interval is 30 minutes.

Figure 147 RADIUS accounting messages configuration



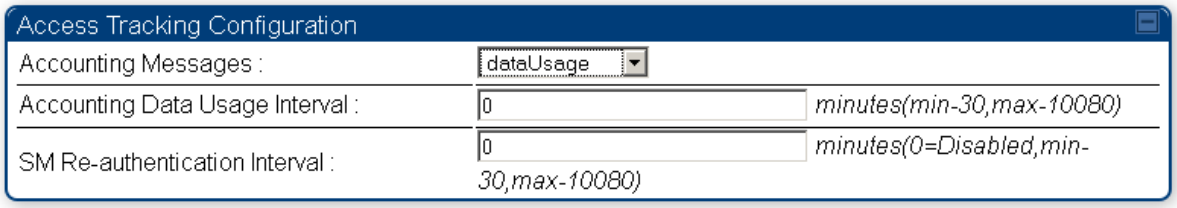
The data accounting message data is based on the SM statistics that the AP maintains, and these statistics may be cleared on the AP by an operator. If an operator clears these messages and data accounting is enabled, an accounting stop message is sent followed by an accounting start message to notify the AAA of the change.

If an operator clears the VC statistics on the device through the management GUI, a RADIUS stop message and data start message is issued for each device affected. The start and stop messages will only be sent once every 5 minutes, so if an operator clears these statistics multiple times within 5 minutes, only one set of data stop/start messages is sent. This may result in inaccurate data accumulation results.

RADIUS Device Re-authentication

PMP 450 Platform systems include support for periodic SM re-authentication in a network without requiring the SM to re-register (and drop the session). The re-authentication may be configured to occur in the range of every 30 minutes to weekly.

Figure 148 Device re-authentication configuration



The re-authentication interval is only configurable on the AP. When this feature is enabled, each SM that enters the network will re-authenticate each the interval time has expired without dropping the session. The response that the SM receives from the AAA server upon re-authentication is one of the following:

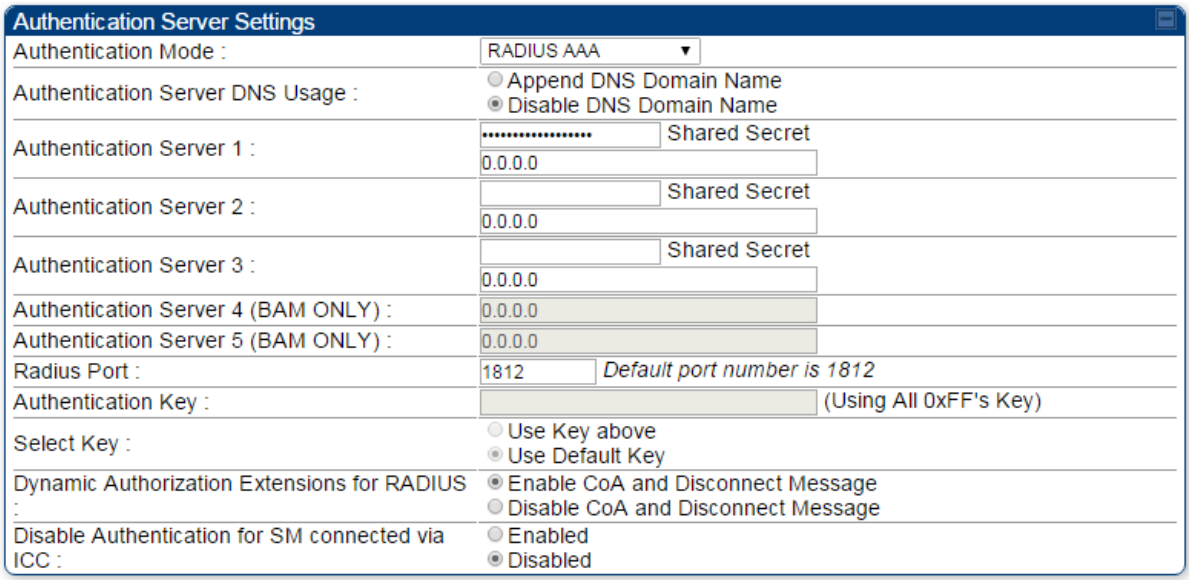
- **Success**: The SM continues normal operation
- **Reject**: The SM de-registers and will attempt network entry again after 1 minute and then if rejected will attempt re-entry every 15 minutes
- **Timeout or other error**: The SM remains in session and attempt 5 times to re-authenticate with the RADIUS-REQUEST message. If these attempts fail, then the SM will go out of session and proceed to re-authenticate after 5 minutes, then every 15 minutes.

Although re-authentication is an independent feature, it was designed to work alongside with the RADIUS data usage accounting messages. If a user is over their data usage limit the network operator can reject the user from staying in the network. Operators may configure the RADIUS 'Reply-Message' attribute with an applicable message (i.e. "Data Usage Limit Reached") that is sent to the subscriber module and displayed on the general page.

RADIUS Change of Authorization and Disconnect Message

Prior to this feature, SM will get configuration parameters from a RADIUS server during authentication process. This feature allows an administrator to control configuration parameters in the SM while SM is in session. The configuration changes in SM are done using RADIUS Change of Authorization method (RFC 3576) on the existing RADIUS authentication framework for AP and SM. A typical use case could be changing the QOS parameters after a certain amount of bandwidth usage by a SM.

Figure 149 RADIUS CoA configuration for AP



The RADIUS CoA feature enables initiating a bi-directional communication from the RADIUS server(s) to the AP and SM.

The AP listens on UDP port 3799 and accepts CoA requests from the configured RADIUS servers. This CoA request should contain SM MAC address in 'User-Name' attribute as identifier and all other attributes which control the SM config parameters. For security reasons, a timestamp also needs to be added as 'Event-Timestamp' attribute. Hence the time should also be synchronized between the RADIUS server(s) and the AP to fit within a window of 300 seconds.

Once the configuration changes are applied on the SM, CoA-ACK message is sent back to RADIUS server. If the validation fails, the AP sends a CoA-NACK response to the RADIUS server with proper error code.

A **Disconnect-Message** is sent by the RADIUS server to NAS in order to terminate a user session on a NAS and discard all associated session context. It is used when the authentication AAA server wants to disconnect the user after the session has been accepted by the RADIUS.

In response of Disconnect-Request from RADIUS server, the NAS sends a Disconnect-ACK if all associated session context is discarded, or a Disconnect-NACK, if the NAS is unable to disconnect the session.

Note

The RADIUS CoA feature will only enabled if Authentication mode is set to RADIUS AAA.

Microsoft RADIUS support

This feature allows to configure Microsoft RADIUS (Network Policy and Access Services a.k.a NPS) as Authentication server for SM and User authentication.

- For SM Authentication, SM will user PEAP-MSCHAPv2 since NPS doesn't support TTLS protocol.
- For User Authentication, the Canopy software will use EAP-MD5 but the user has to do certain configuration in order to enable EAP-MD5 on NPS.

Note

All this configuration has been tested on Windows Server 2012 R2 version.

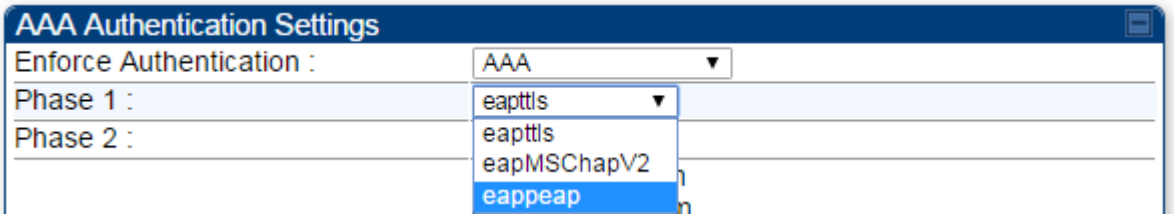
This feature is not supported on hardware board type P9 or lower platforms.

SM Authentication Configuration

There are no new configuration on AP. However SM has to be configured for PEAP authentication protocol.

1. Go to Configuration > Security page
2. Select "**eappeap**" for Phase 1 attribute under tab AAA Authentication Settings.

Figure 150 EAPPEAP settings



The Phase 2 will change automatically to MSCHAPv2 on select of Phase 1 attribute as EAP-PEAP. Other parameters of Phase 2 protocols like PAP/CHAP will be disabled.

Windows Server Configuration

Import Certificate

The SM certificate has to be imported to Windows Server for certificate authentication.

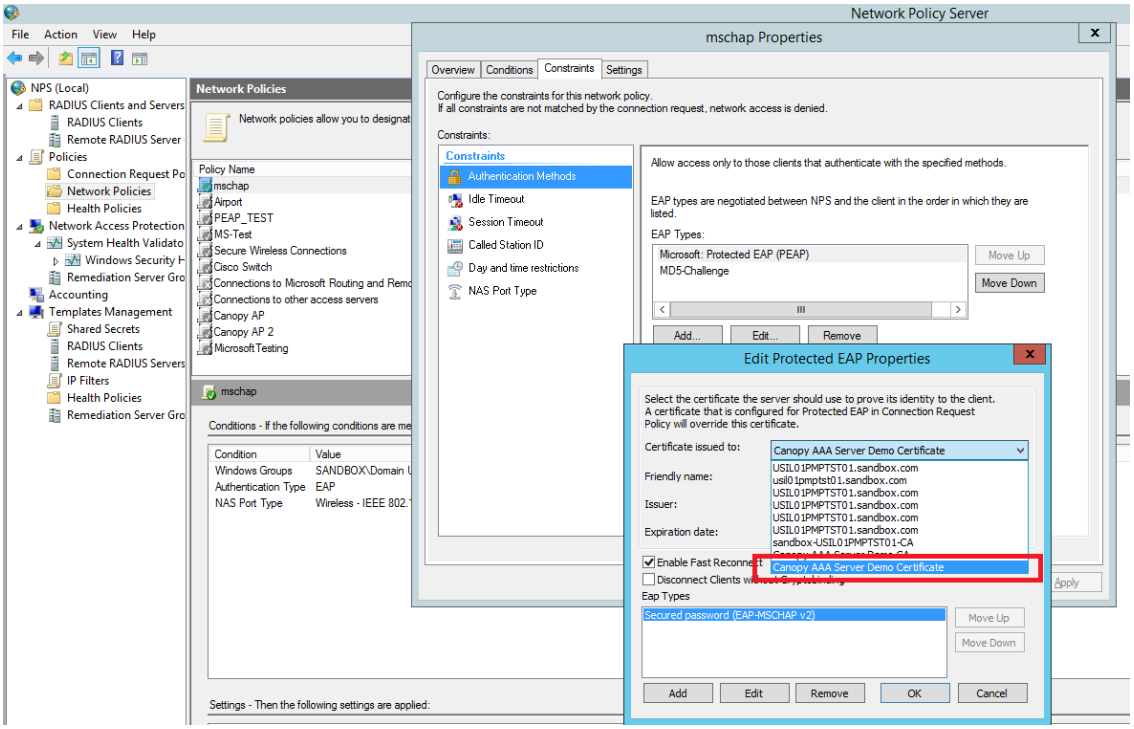
1. Copy the certificate which is configured in SM under **Configuration > Security -> Certificate1** to Windows Server machine.
2. Right click and select 'Install Certificate'. This will install the certificate and it's ready for use. This certificate will be used while configuring PEAP-MSCHAPv2 in NPS.

NPS Configuration (https://technet.microsoft.com/en-us/network/bb545879.aspx**)**

Following **items** should be configured in NPS Console:

- RADIUS Client
  - https://technet.microsoft.com/en-us/library/cc732929
- Connection Request Policies
  - https://technet.microsoft.com/en-us/library/cc730866
  - Choose 'Wireless-Other' in NAS-Port-Type
- Network Policy
  - https://technet.microsoft.com/en-us/library/cc755309
  - Choose 'Wireless-Other' in NAS-Port-Type.
  - While configuring PEAP, select the above imported certificate.

Figure 151 Importing certificate in NPS



User Authentication Configuration

Enabling EAP-MD5

As mentioned earlier, Microsoft has deprecated the support for MD5 from versions of Windows. To enable MD5, the following steps to be followed:

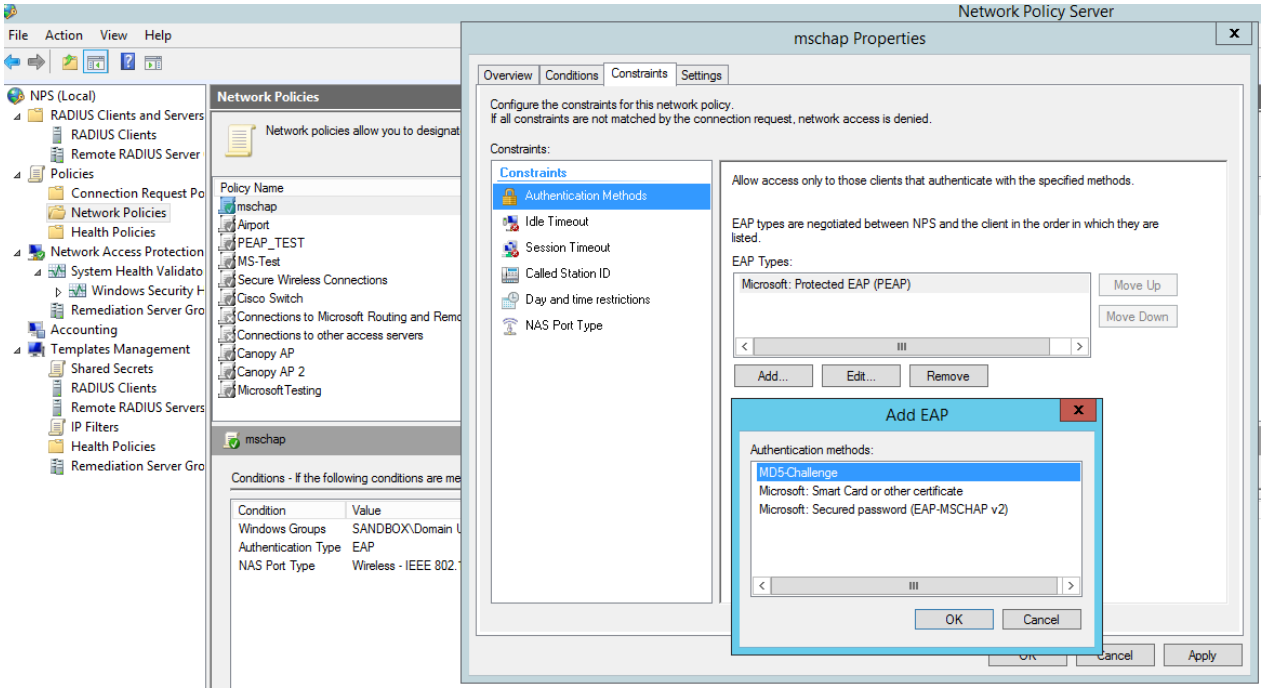
1. Follow the instructions:

   https://support.microsoft.com/en-us/kb/922574/en-us?wa=wsignin1.0

   Optionally, the registry file can be downloaded. It can be installed by double-click it in Windows Registry.

2. From NPS Console **Network Policy >** <Policy Name> **> Properties > Constrains > Authentication Method** and click Add. Select MD5 and click OK.

Figure 152 Selecting MD5 from NPS console

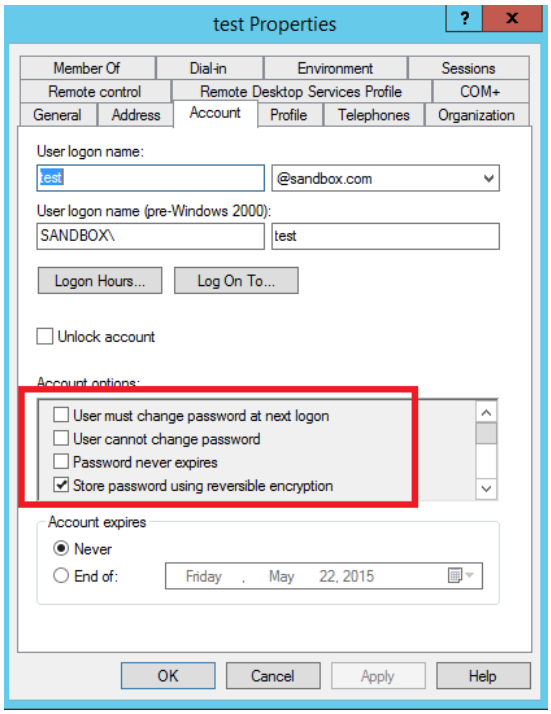


User Configuration in Active Directory

Next open '**Active Directory Users and Computers**' and create user.

Make sure user property is configured as shown below.

Figure 153 User configuration



RADIUS VSA Configuration

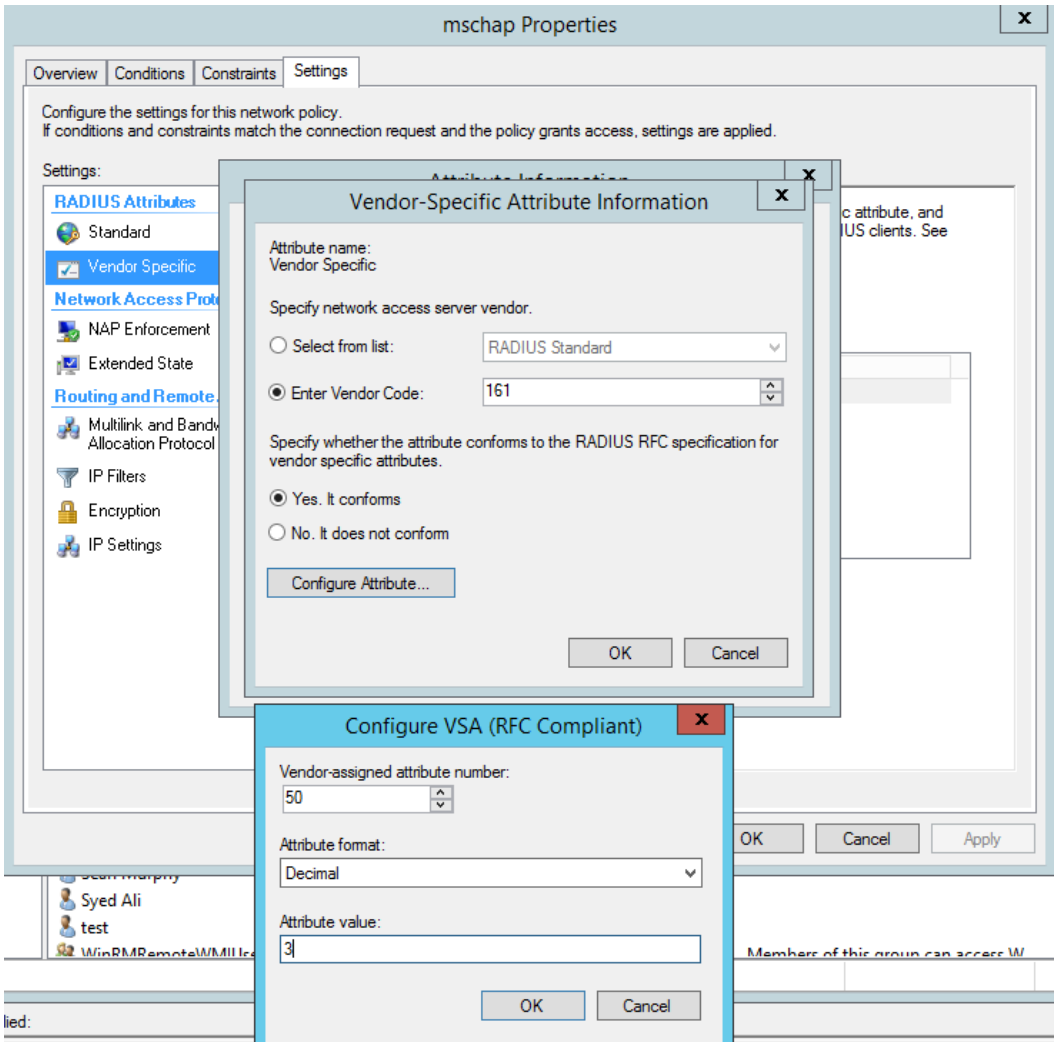
Before using VSA, the **Cambium-Canopy-UserLevel(50)** VSA must be configured with some access level say ADMIN(3).

Follow below link for configuring VSA:

https://technet.microsoft.com/en-us/library/cc731611

The Cambium's vendor code is 161.

Figure 154 RADIUS VSA configuration



Accounting

User can enable accounting in NPS under **NPS Console > Accounting > Configure Accounting**.

For more details refer https://technet.microsoft.com/library/dd197475

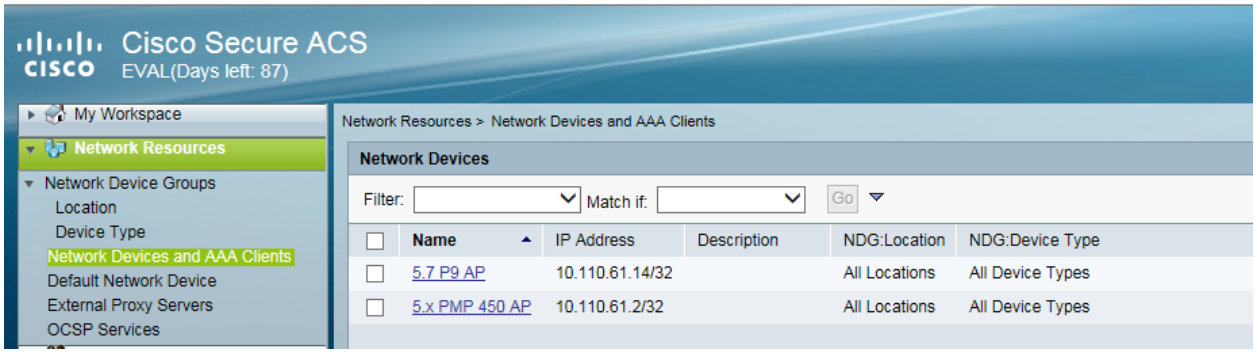
Cisco ACS RADIUS Server Support

This briefly explains how to configure CIsco ACS RADIUS server for PEAP-MSCHAPv2 authentication.

The configuration had been tested on **CISCO ACS Version : 5.7.0.15**

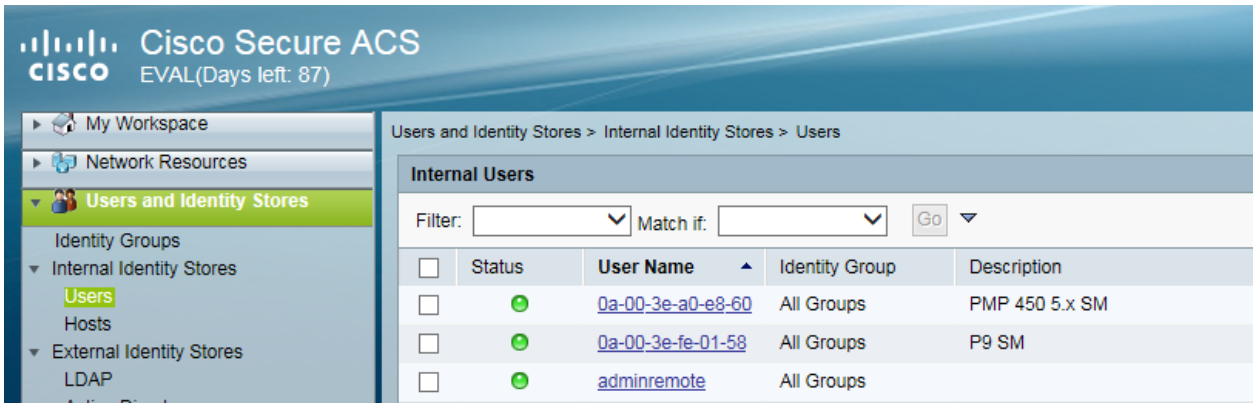
Adding RADIUS client

Figure 155 Adding RADIUS client



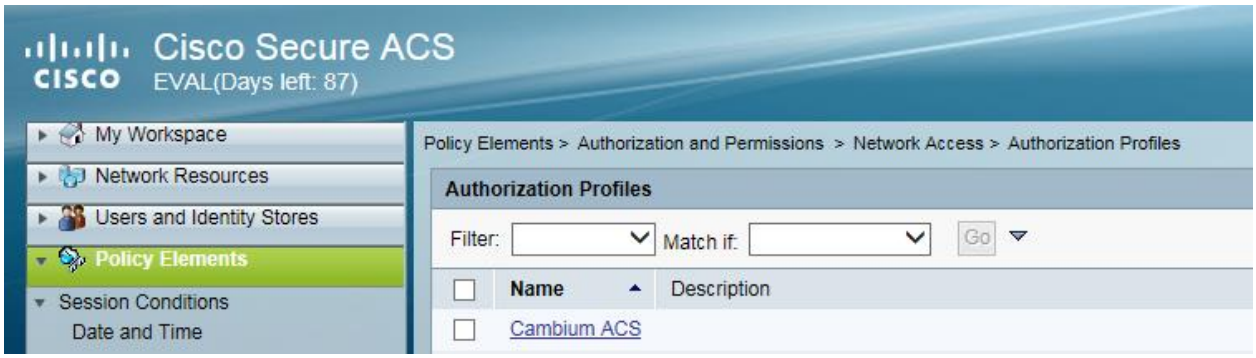
Creating Users

Figure 156 Creating users



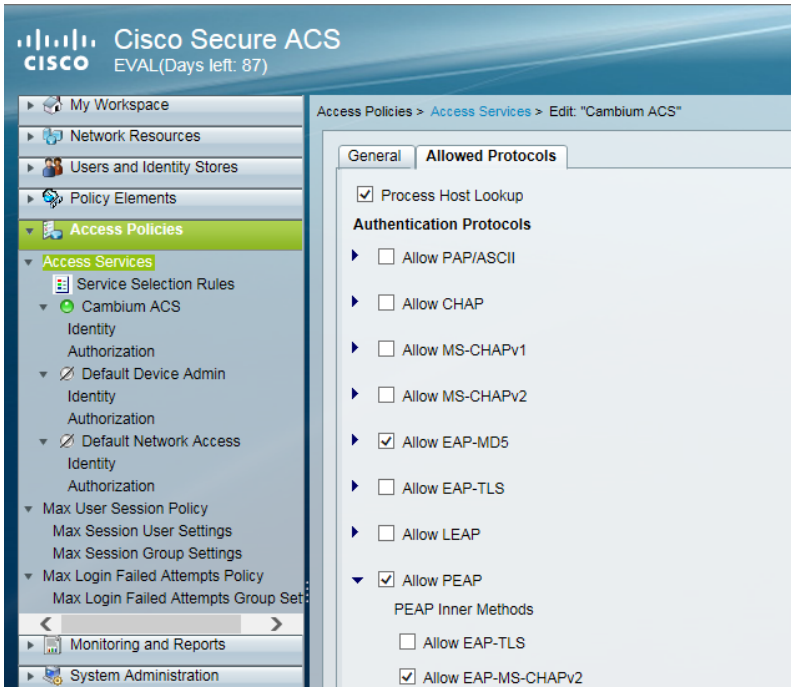
Creating RADIUS instance

Figure 157 Creating RADIUS instance



RADIUS protocols

Figure 158 RADIUS protocols

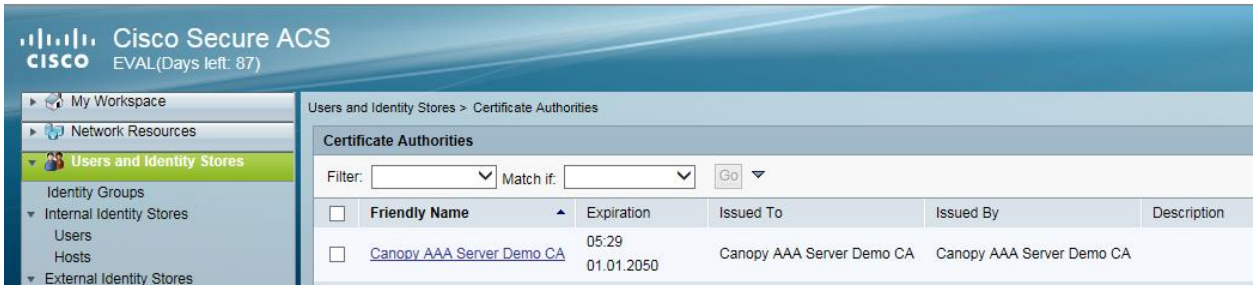


Service selection

Figure 159 Service selection

Adding Trusted CA

Figure 160 Adding Trusted CA



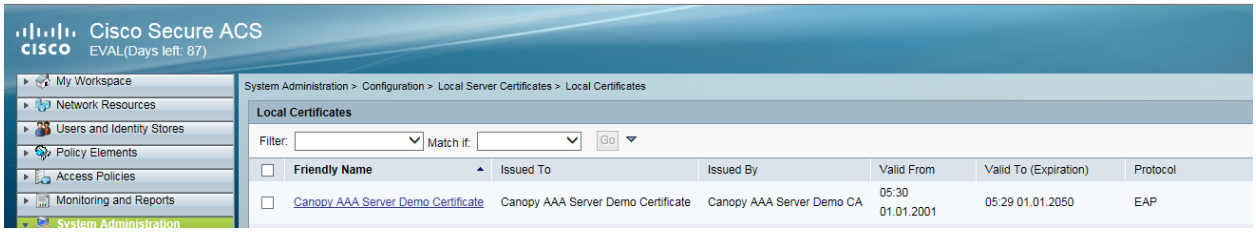
Note that certificate has to be in DER form, so if you have in PEM format convert using openssl.

```
 openssl.exe x509 -in <path-to->/cacert_aaasvr.pem  -outform DER -out <path-to>/cacert_aaasvr.der
```

Installing Server Certificate

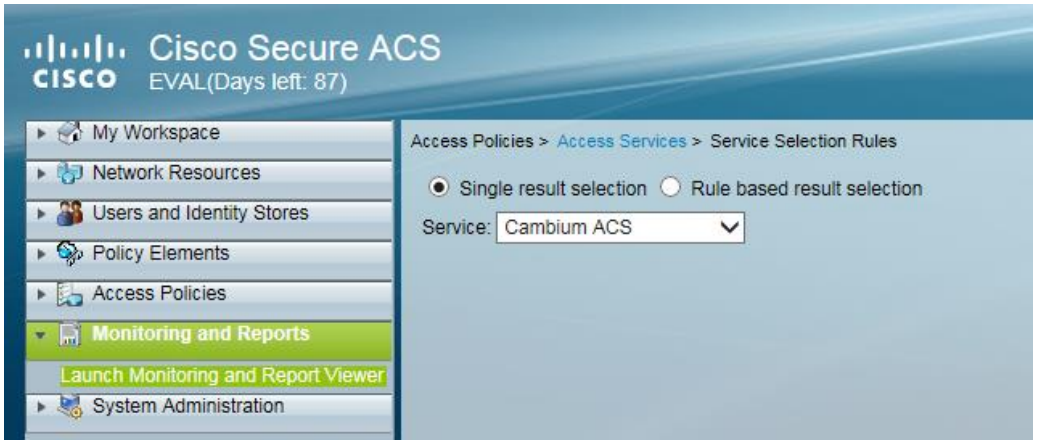
After installing trusted CA, you need to add a server certificate which will be used for TLS tunnel. Generally you have to install same certificate which is installed in your AP, so that AP can trust the radius server.

Figure 161 Installing Server Certificate



Monitoring Logs

Figure 162 Monitoring logs



Configuring VSA

Before using VSA , user has to add Cambium Vendor Specific Attribute

Navigate to System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA > Motorola

If Motorola is not present you can create Vendor with ID 161 and add all the VSA one by one.

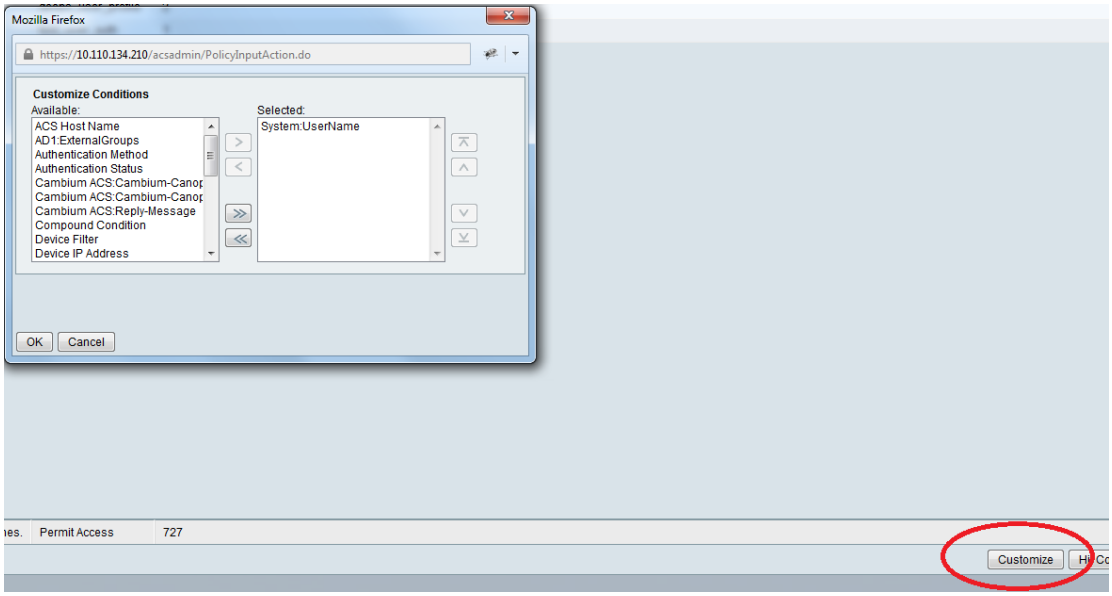
Figure 163 VSA list

Attribute	ID	Type	Direction	Multiple Allowed
Cambium-Canopy-BCASTMIR	24	Unsigned Integer 32	BOTH	false
Cambium-Canopy-DLBL	9	Unsigned Integer 32	BOTH	false
Cambium-Canopy-DLBR	8	Unsigned Integer 32	BOTH	false
Cambium-Canopy-DLMB	27	Unsigned Integer 32	BOTH	false
Cambium-Canopy-Gateway	25	IP Address	BOTH	false
Cambium-Canopy-HPDLCIR	4	Unsigned Integer 32	BOTH	false
Cambium-Canopy-HPENABLE	5	Unsigned Integer 32	BOTH	false
Cambium-Canopy-HPULCIR	3	Unsigned Integer 32	BOTH	false
Cambium-Canopy-LPDLCIR	2	Unsigned Integer 32	BOTH	false
Cambium-Canopy-LPULCIR	1	Unsigned Integer 32	BOTH	false
Cambium-Canopy-ULBL	7	Unsigned Integer 32	BOTH	false
Cambium-Canopy-ULBR	6	Unsigned Integer 32	BOTH	false
Cambium-Canopy-ULMB	26	Unsigned Integer 32	BOTH	false
Cambium-Canopy-UserLevel	50	Unsigned Integer 32	BOTH	false
Cambium-Canopy-UserMode	51	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLAGETO	20	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLFRAMES	15	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLIDSET	16	Unsigned Integer 32	BOTH	true
Cambium-Canopy-VLIGVID	21	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLLEARNEN	14	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLMGVID	22	Unsigned Integer 32	BOTH	true
Cambium-Canopy-VLSMMGPASS	23	Unsigned Integer 32	BOTH	false

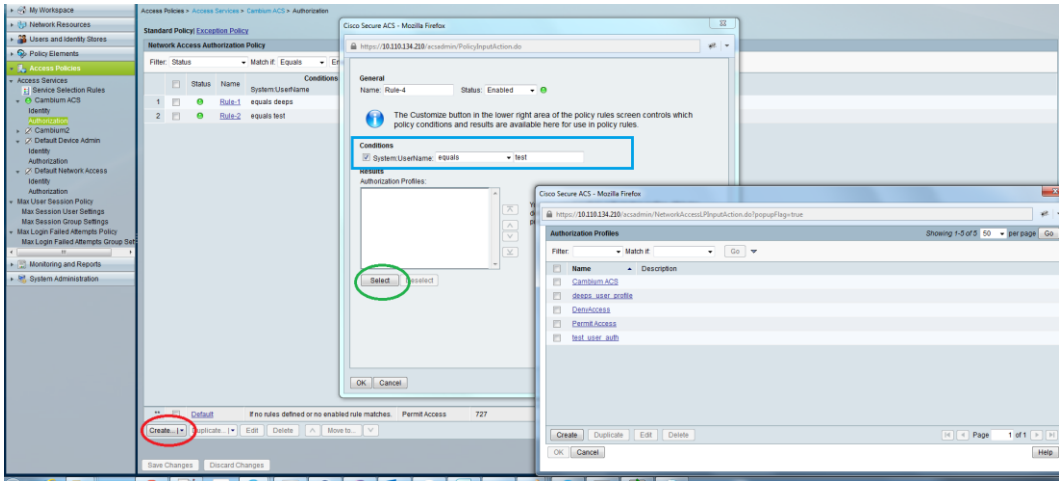
Using VSA for users

Navigate to Access Policies > Access Services > Cambium ACS > Authorization

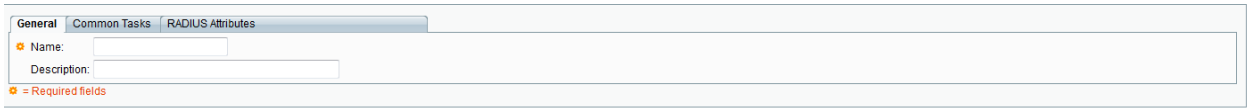
1. Change condition to User name



2. Next click Create and then click Select see diagram below

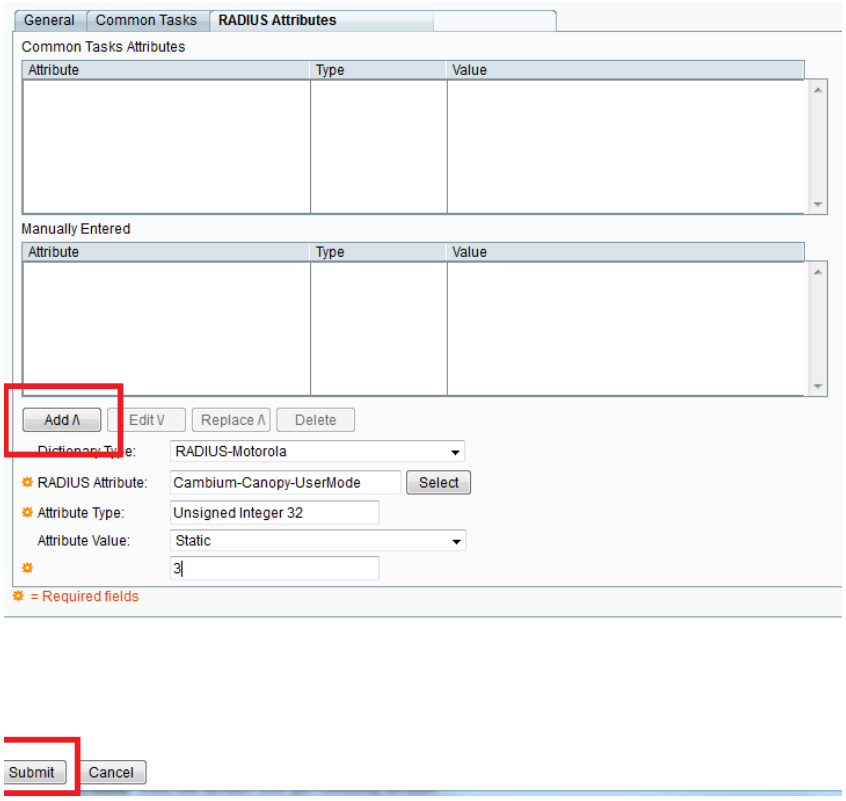


3. Click Create from the screen you get following screen



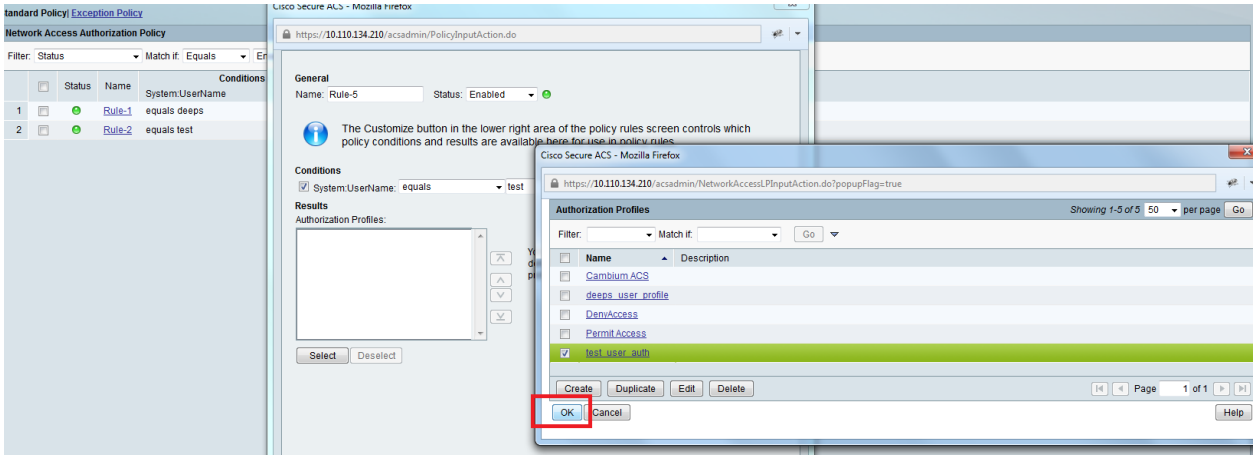
Chose some name and then move to RADIUS Attributes tab

4. Fill attribute which all you want for that particular user



Important: Click Add for each attribute and when done click Submit.

5. Now you are ready to use this Authorization profile for the use Select and Press OK



6. Finally press Save Changes and you are ready to use it.

Chapter 8: Tools

The AP and SM GUIs provide several tools to analyze the operating environment, system performance and networking, including:

Using Spectrum Analyzer tool

The integrated spectrum analyzer can be very useful as a tool for troubleshooting and RF planning, but is not intended to replicate the accuracy and programmability of a high-end spectrum analyzer, which sometime can be used for other purposes.

The AP/BHM and SM/BHS perform spectrum analysis together in the Sector Spectrum Analyzer tool.

Caution

On start of the Spectrum Analyzer on a module, it enters a scan mode and drops any RF connection it may have had. When choosing **Start Timed Spectrum Analysis**, the scan is run for the amount of time specified in the **Duration** configuration parameter. When choosing **Start Continuous Spectrum Analysis**, the scan is run continuously for 24 hours, or until stopped manually (using the **Stop Spectrum Analysis** button).

Any module can be used to see the frequency and power level of any detectable signal that is within, just above, or just below the frequency band range of the module.

Note

Vary the days and times when you analyze the spectrum in an area. The RF environment can change throughout the day or throughout the week.

Mapping RF Neighbor Frequencies

The neighbor frequencies can be analyzed using Spectrum Analyzer tool. Following modules allow user to:

- Use a BHS or BHM for PTP and SM or AP for PMP as a Spectrum Analyzer.
- View a graphical display that shows power level in RSSI and dBm at 5 MHz increments throughout the frequency band range, regardless of limited selections in the **Custom Radio Frequency Scan Selection List** parameter of the SM/BHS.
- Select an AP/BHM channel that minimizes interference from other RF equipment.

Caution

The following procedure causes the SM/BHS to drop any active RF link. If a link is dropped when the spectrum analysis begins, the link can be re-established when either a 15 minute interval has elapsed or the spectrum analyzer feature is disabled.

Temporarily deploy a SM/BHS for *each* frequency band range that need to monitor and access the Spectrum Analyzer tab in the Tools web page of the module.

- Using Spectrum Analyzer tool
- Using the Remote Spectrum Analyzer tool

Spectrum Analyzer tool

Analyzing the spectrum

To use the built-in spectrum analyzer functionality of the AP/SM/BH, proceed as follows:

Procedure 29 Analyzing the spectrum

1 Predetermine a power source and interface that works for the AP/SM/BH in the area to be analyzed.

2 Take the AP/SM/BH, power source and interface device to the area.

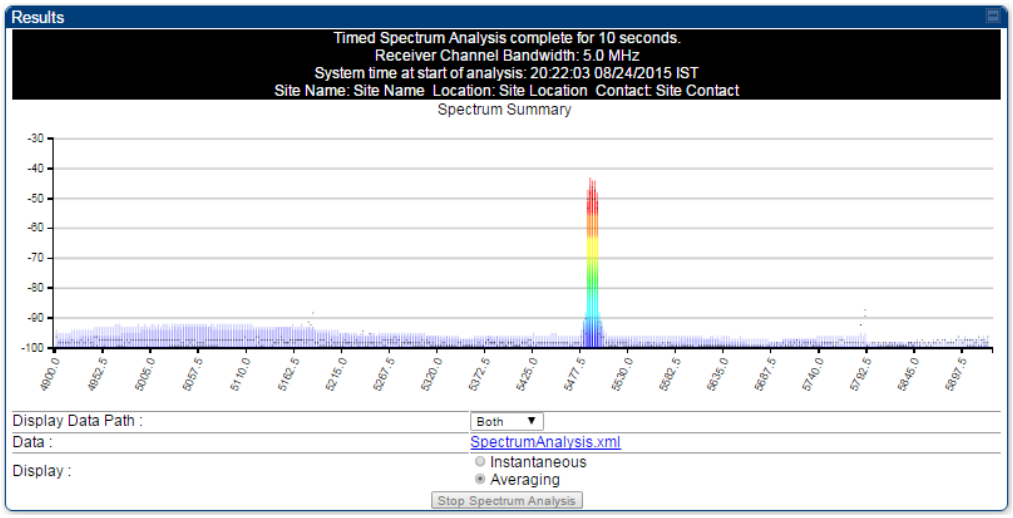
3 Access the **Tools** web page of the AP/SM/BH.

4 Enter **Duration** in Timed Spectrum Analyzer Tab. Default value is 10 Seconds

5 Click **Start Timed Sector Spectrum Analysis**

6 The results are displayed:

Figure 164 Spectrum analysis - Results



Note

AP/SM/BH scans for extra 40 seconds in addition to configured **Duration**

7 Travel to another location in the area to BHS.

8 Click **Start Timed Spectrum Analysis**

9 Repeat Steps 4 and 6 until the area has been adequately scanned and logged.

As with any other data that pertains to your business, a decision today to put the data into a retrievable database may grow in value to you over time.

Note

Wherever the operator find the measured noise level is greater than the sensitivity of the radio that is plan to deploy, use the noise level (rather than the link budget) for your link feasibility calculations.

The AP/SM/BH perform spectrum analysis together in the Sector Spectrum Analyzer feature.

Graphical spectrum analyzer display

The AP/SM/BH display the graphical spectrum analyzer. An example of the **Spectrum Analyzer** page is shown in Figure 164.

The navigation feature includes:

- Results may be panned left and right through the scanned spectrum by clicking and dragging the graph left and right
- Results may be zoomed in and out using mouse

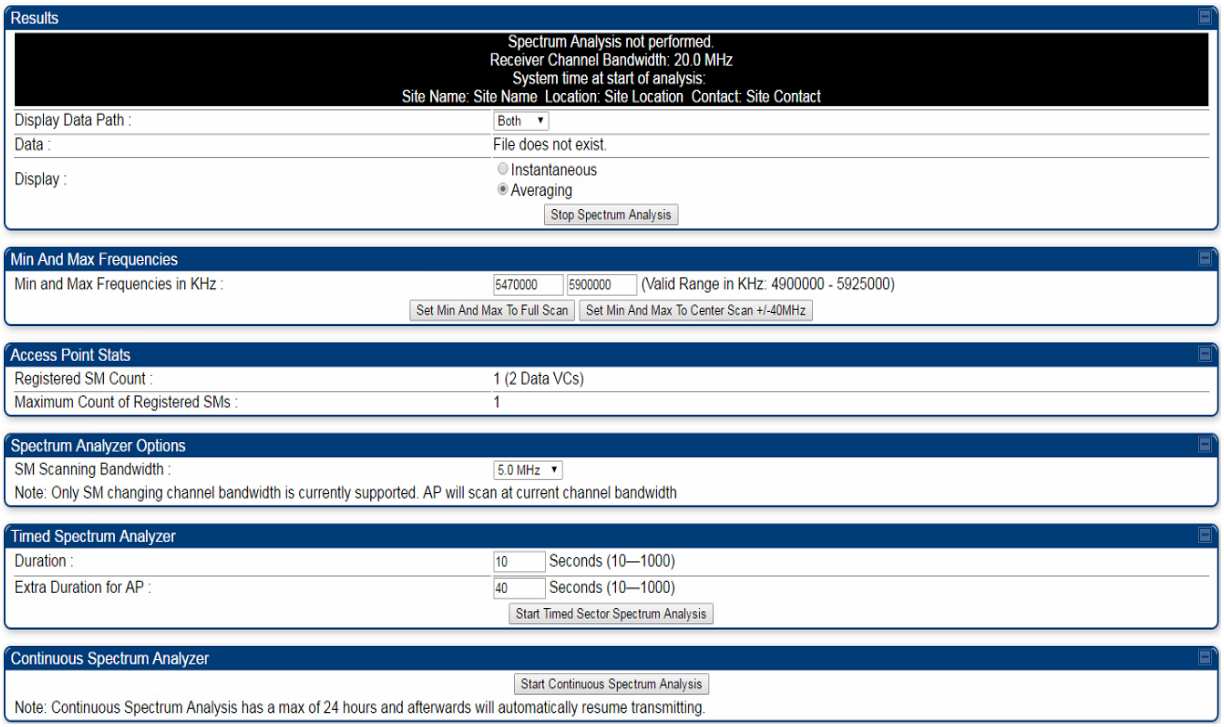
When the mouse is positioned over a bar, the receive power level, frequency, maximum and mean receive power levels are displayed above the graph

To keep the displayed data current, either set “Auto Refresh” on the module’s **Configuration > General.**

Spectrum Analyzer page of AP

The Spectrum Analyzer page of AP is explained in Table 176.

Table 176 Spectrum Analyzer page attributes - AP



Attribute	Meaning
Display Data Path	**Both** means that the vertical and horizontal paths are displayed or an individual path may be selected to display only a single-path reading.
Data	For ease of parsing data and to facilitate automation, the spectrum analyzer results may be saved as an XML file. To save the results in an XML formatted file, right-click the “SpectrumAnalysis.xml” link and save the file.
Display	**Instantaneous** means that each reading (vertical bar) is displayed with two horizontal lines above it representing the max power level received (top horizontal line) and the average power level received (lower horizontal line) at that frequency. **Averaging** means that each reading (vertical bar) is displayed with an associated horizontal line above it representing the max power level received at that frequency.
Min and Max Frequencies in KHz	Enter minimum and maximum frequencies to be scanned.
Set Min And Max to Full Scan	On the button press, it sets mimimum and maximum allowed frequencies for scanning.
Set Min And Max to Center Scan +/-40 MHz	On the button press, it sets mimium and maximum frequencies to ± 40 MHz of center frequency for scanning.

Registered SM Count	This field displays the MAC address and Site Name of the registered SM.
Maximum Count of Registered SMs	This field displays the maximum number of registered SMs.
SM Scanning Bandwidth	This field allows to select SM's scanning bandwidth.
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.
Continuous Spectrum Analyzer	***Start Continuous Spectrum Analysis*** button ensures that when the SM is powered on, it automatically scans the spectrum for 10 seconds. These results may then be accessed via the **Tools > Spectrum Analyzer** GUI page.

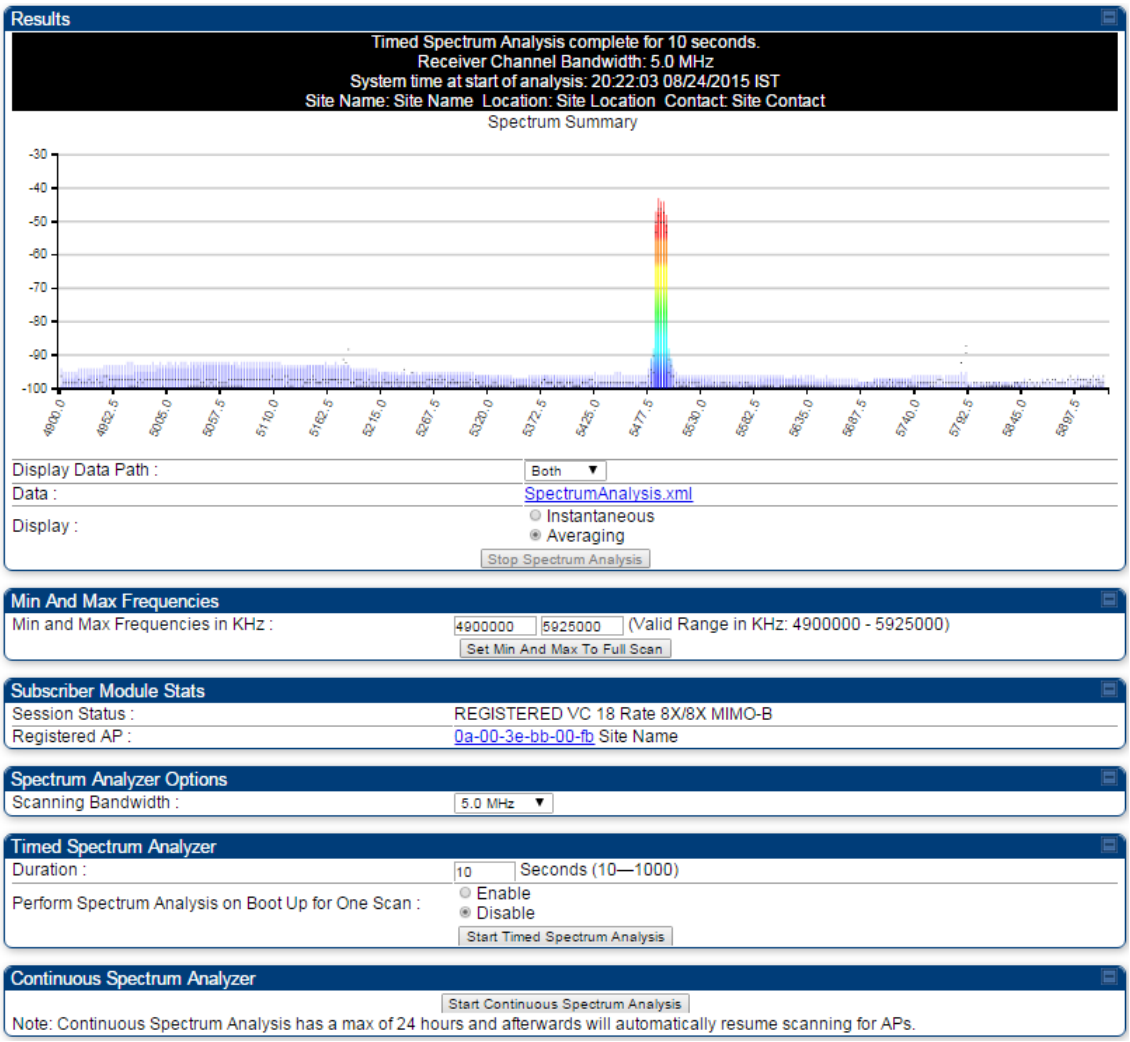
Spectrum Analyzer page of SM

The Spectrum Analyzer page of SM is explained in Table 177.

Note

Spectrum Analyzer is not currently supported by 450m.

Table 177 Spectrum Analyzer page attributes - SM

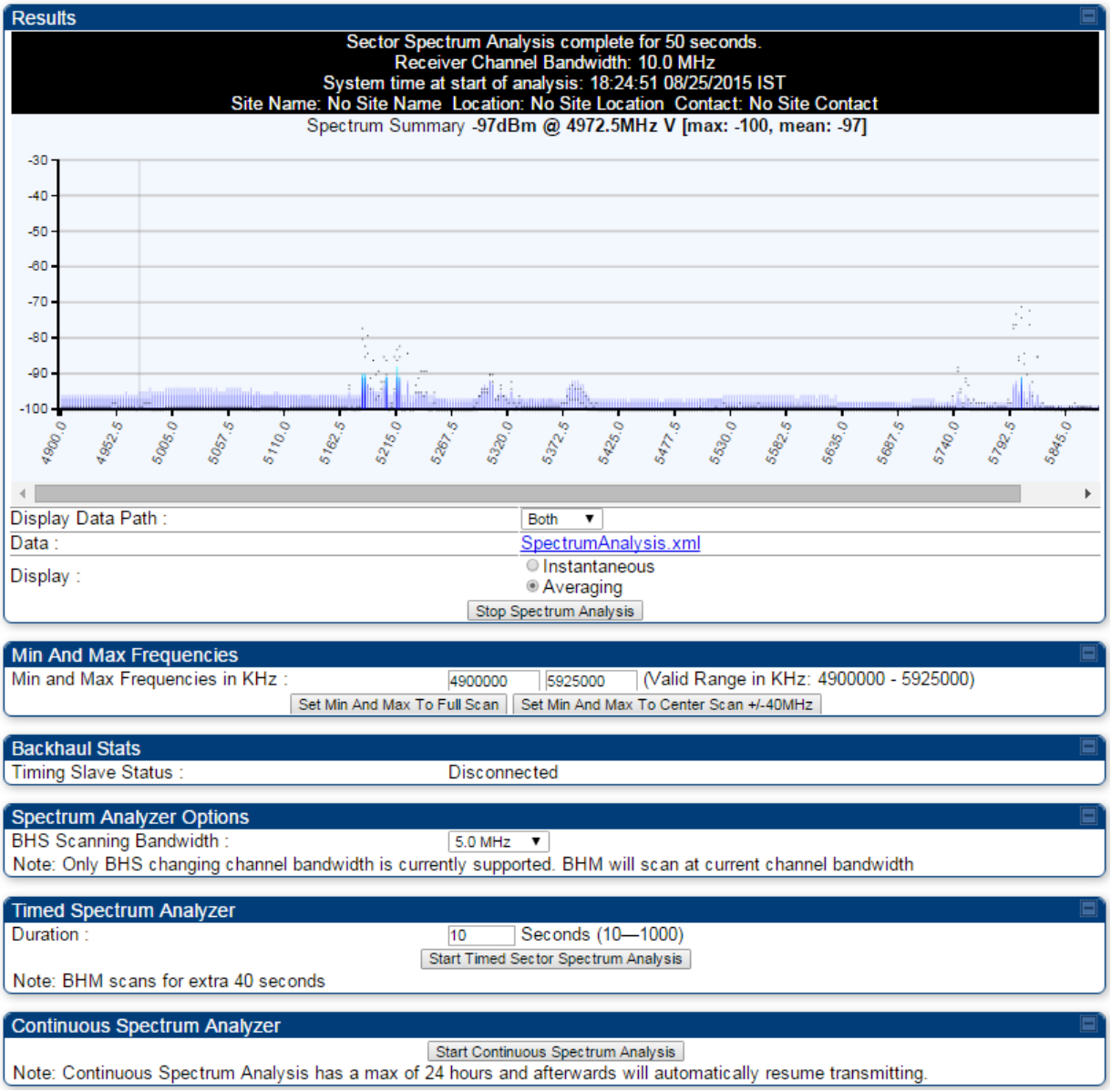


Attribute	Meaning
Display Data Path	Refer Table 176 on page 8-5
Data	Refer Table 176 on page 8-5
Display	Refer Table 176 on page 8-5
Min and Max Frequencies in KHz	To scan min to max range of frequencies, enter min and max frequencies in KHz and press **Set Min and Max to Full Scan** button. To scan +/- 40 MHz from center frequency, enter center frequency in KHz and press **Set Min And Max To Center Scan +/- 40KHz** button.
Registered SM Count	Refer Table 176 on page 8-5
Maximum Count to Registered SMs	Refer Table 176 on page 8-5
Duration	Refer Table 176 on page 8-5

Spectrum Analyzer page of BHM

The Spectrum Analyzer page of BHM is explained in Table 178.

Table 178 Spectrum Analyzer page attributes - BHM

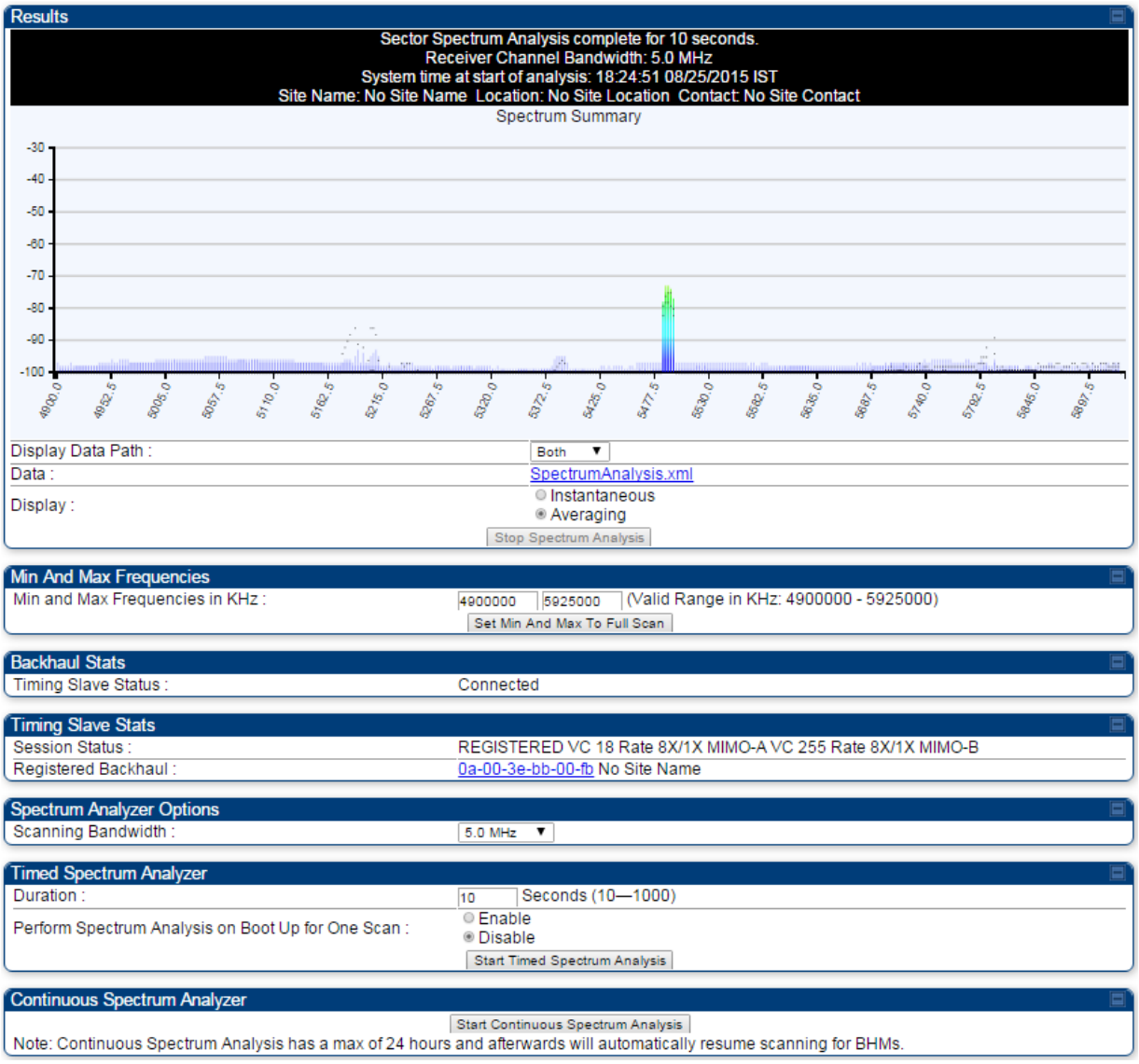


Attribute	Meaning
Data	Refer Table 176 on page 8-5
Display	Refer Table 176 on page 8-5
Duration	Refer Table 176 on page 8-5
Continuous Spectrum Analyzer	Refer Table 176 on page 8-5

Spectrum Analyzer page of BHS

The Spectrum Analyzer page of BHS is explained in Table 179.

Table 179 Spectrum Analyzer page attributes - BHS

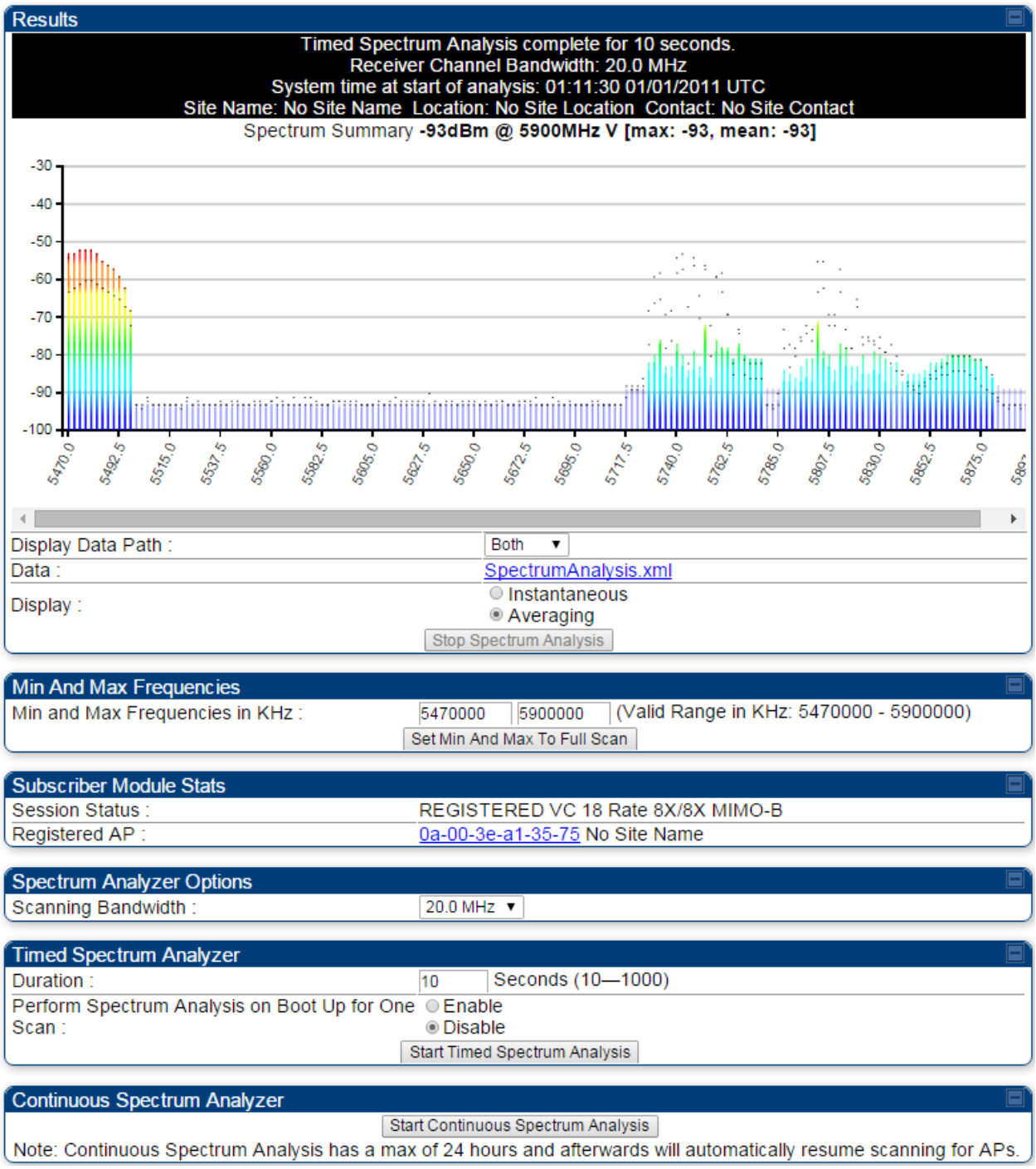


Attribute	Meaning
Data	Refer Table 176 on page 8-5
Display	Refer Table 176 on page 8-5
Session Status	This field displays current session status and rates. The session states can be Scanning, Syncing, Registering or Registered.

Registered Backhaul	This field displays MAC address of BHM and PTP model number
Duration	Refer Table 176 on page 8-5
Perform Spectrum Analysis on Boot Up for one scan	This field allows to Enable or Disable to start Spectrum Analysis on boot up of module for one scan.
Continuous Spectrum Analyzer	Refer Table 176 on page 8-5

Spectrum Analyzer page result of PMP 450 SM

Figure 165 Spectrum Analyzer page result – PMP 450 SM



Remote Spectrum Analyzer tool

The Remote Spectrum Analyzer tool in the AP/BHM provides additional flexibility in the use of the spectrum analyzer in the SM/BHS. Set the duration of 10 to 1000 seconds, then click the **Start Remote Spectrum Analysis** button to launch the analysis from that SM/BHS.

In PMP configuration, a SM has to be selected from the drop-down list before launching **Start Remote Spectrum Analysis**.

Analyzing the spectrum remotely

Procedure 30 Remote Spectrum Analyzer procedure

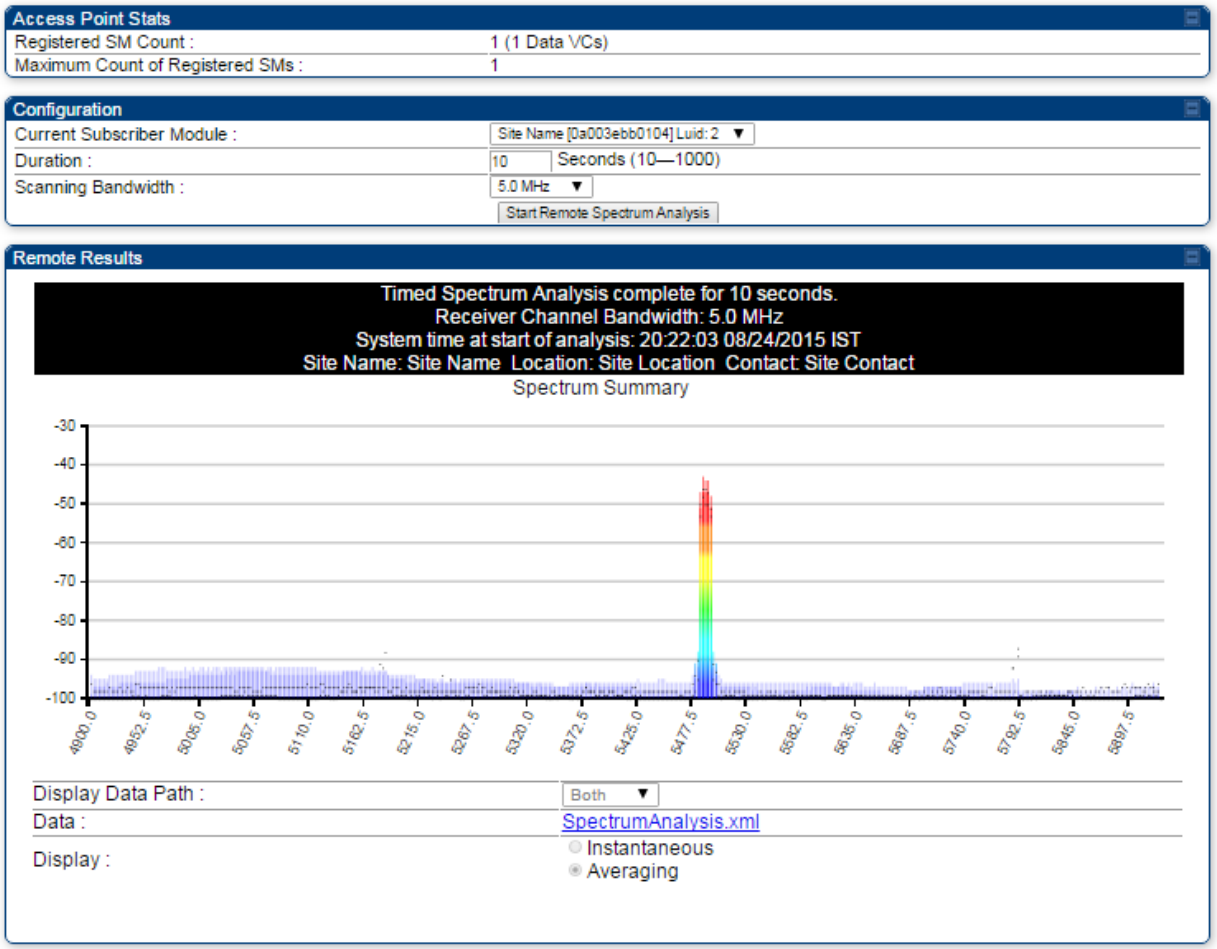
1. The AP/BHM de-registers the target SM/BHS.
2. The SM/BHS scans (for the duration set in the AP/BHM tool) to collect data for the bar graph.
3. The SM/BHS re-registers to the AP/BHM.
4. The AP/BHM displays the bar graph.

The bar graph is an HTML file, but can be changed to an XML file, which is then easy to analyze through the use of scripts that you may write for parsing the data. To transform the file to XML, click the “SpectrumAnalysis.xml” link below the spectrum results. Although the resulting display appears mostly unchanged, the bar graph is now coded in XML. You can now right-click on the bar graph for a **Save Target As** option to save the `Spectrum Analysis.xml` file.

Remote Spectrum Analyzer page of AP

The Remote Spectrum Analyzer page of AP is explained in Table 180.

Table 180 Remote Spectrum Analyzer attributes - AP

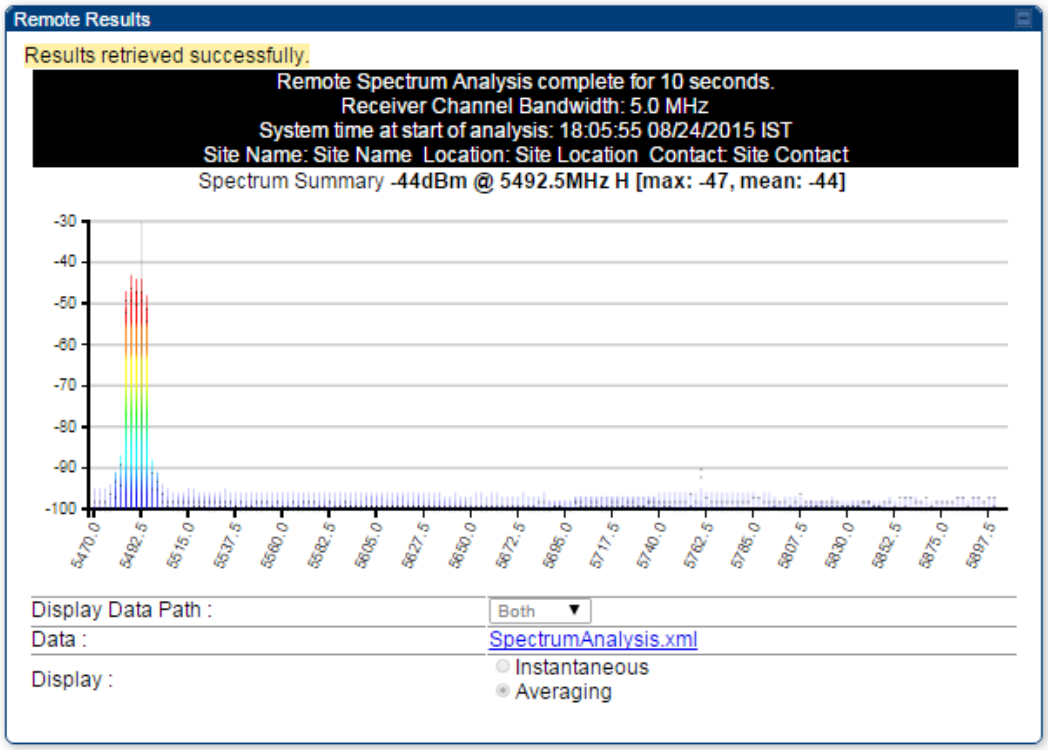


Attribute	Meaning
Registered SM Count	This field displays the number of SMs that were registered to the AP before the SA was started. This helps the user know all the SMs re-registered after performing a SA.
Maximum Count of Registered SMs	This field displays the largest number of SMs that have been simultaneously registered in the AP since it was last rebooted. This count can provide some insight into sector history and provide comparison between current and maximum SM counts at a glance.
Current Subscriber Module	The SM with which the Link Capacity Test is run.
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.
Scanning Bandwidth	This parameter defines the size of the channel scanned when running the analyzer.

Remote Spectrum Analyzer page of BHM

The Remote Spectrum Analyzer page of BHM is explained in Table 181.

Table 181 Remote Spectrum Analyzer attributes - BHM



Attribute	Meaning
Duration	Refer Table 176 on page 8-5

Using the Alignment Tool

The SM's or BHS's Alignment Tool may be used to maximize Receive Power Level, Signal Strength Ratio and Signal to Noise Ratio to ensure a stable link. The Tool provides color coded readings to facilitate in judging link quality.

Note

To get best performance of the link, the user has to ensure the maximum Receive Power Level during alignment by pointing correctly. The proper alignment is important to prevent interference in other cells. The achieving Receive Power Level green (>- 70 dBm) is not sufficient for the link.

Figure 166 Alignment Tool tab of SM – Receive Power Level > -70 dBm

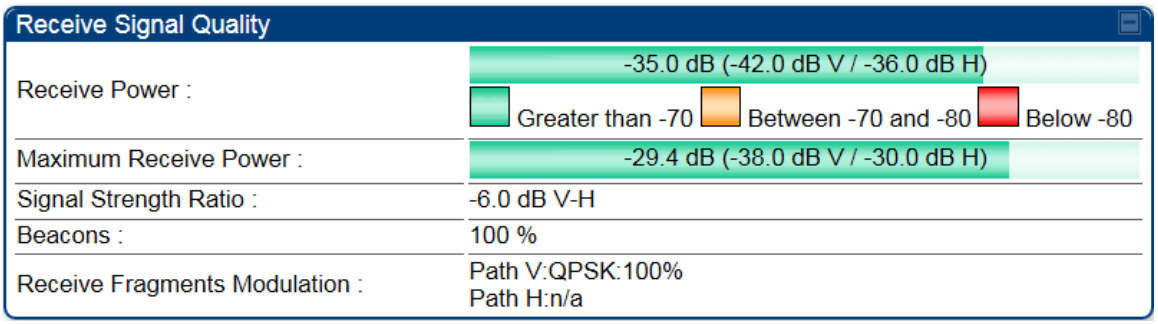


Figure 167 Alignment Tool tab of SM – Receive Power Level between -70 to -80 dBm

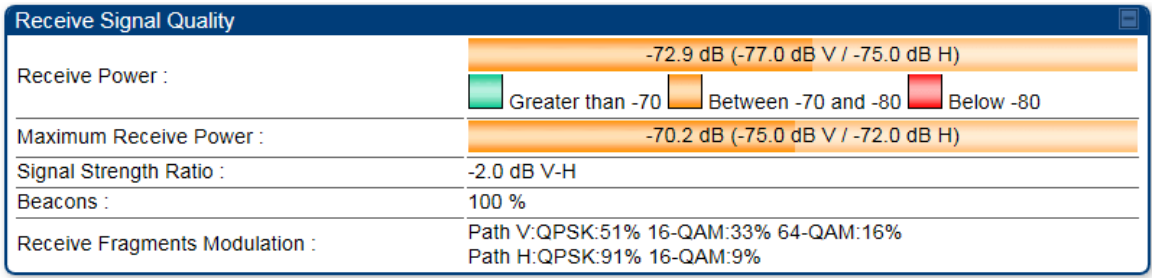
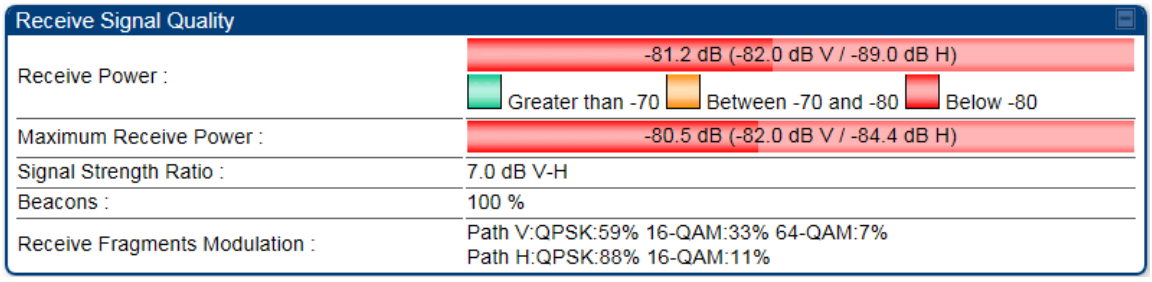


Figure 168 Alignment Tool tab of SM – Receive Power Level < -80 dBm



Aiming page and Diagnostic LED – SM/BHS

The SM's/BHS's Alignment Tool (located in GUI **Tools -> Aiming**) may be used to configure the SM's/BHS's LED panel to indicate received signal strength and to display decoded beacon information/power levels. The SM/BHS LEDs provide different status based on the mode of the SM/BHS. A SM/BHS in "operating" mode will register and pass traffic normally. A SM/BHS in "aiming" mode will not register or pass traffic, but will display (via LED panel) the strength of received radio signals (based on radio channel selected via **Tools** ->**Aiming**). See SM/BHS LEDs on page 2-16.

Note

In order for accurate power level readings to be displayed, traffic must be present on the radio link.

Refer Table 20 SM/BHS LED descriptions on page 2-17 for SM/BHS LED details.

Aiming page of SM

The Aiming page is similar to Spectrum Analyzer where it scans the spectrum but it does not establish any session with any Aps. It has two modes – Single Frequency Only and Normal Frequency Scan List.

The Aiming page of SM is explained in Table 182.

Table 182 Aiming page attributes – SM

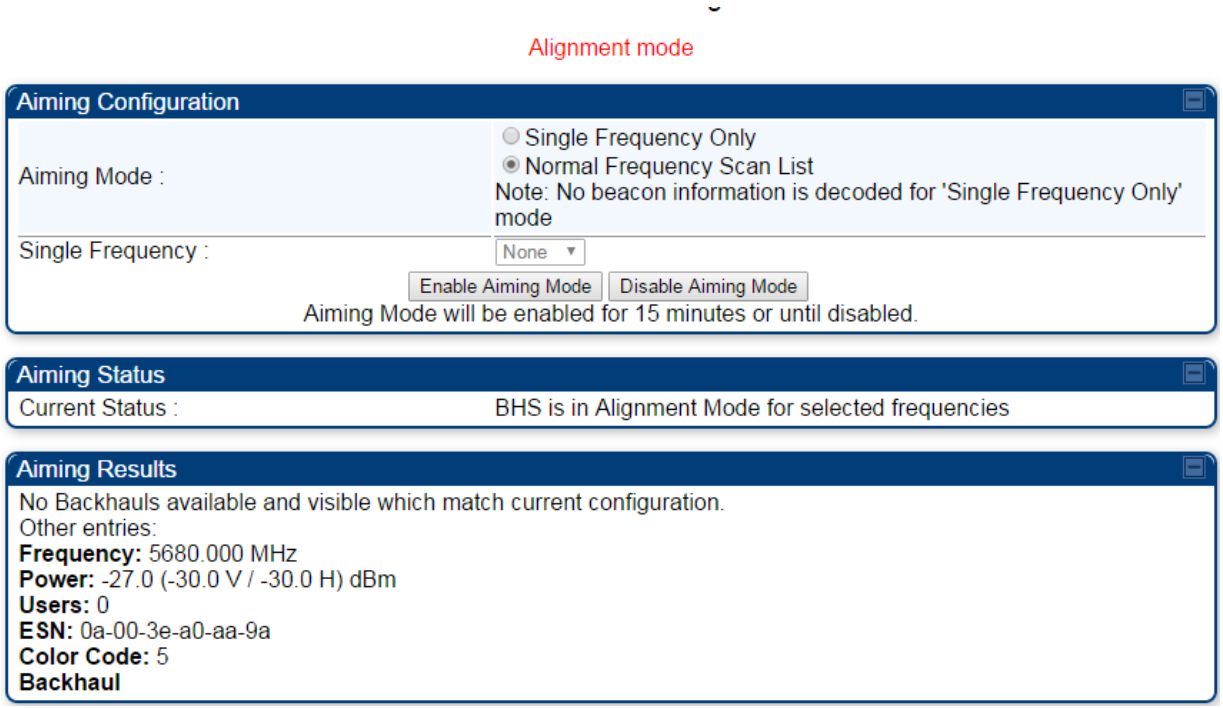
Attribute	Meaning
Aiming Mode	**Single Frequency Only:** scans only selected single frequency. **Normal Frequency Scan List: scans:** scans all frequency of scan list.
Single Frequency	Select a particular frequency from drop down menu for scanning.
Scan Radio Frequency Only Mode	**Enabled**: the radio is configured to "aiming" or "alignment" mode, wherein the LED panel displays an indication of receive power level. See Table 20 SM/BHS LED descriptions on page 2-17. **Disabled:** the radio is configured to "operating" mode, wherein the SM registers and passes traffic normally.
Aiming Results	The Aiming Results are displayed in two sections – Current entry and Other entries. **Frequency**: this field indicates the frequency of the AP which is transmitting the beacon information.

	Power: This field indicates the current receive power level (vertical channel) for the frequency configured in parameter **Radio Frequency.** **Users**: This field indicates the number of SMs currently registered to the AP which is transmitting the beacon information. **ESN**: This field indicates the MAC, or hardware address of the AP/BHM which is transmitting the beacon information. **Color Code**: This field displays a value from 0 to 254 indicating the AP's configured color code. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes). **Multipoint or Backhaul**: this field indicates type of configuration - point-Multipoint(PMP) or Backhaul (PTP).

Aiming page of BHS

The Alignment page of BHS is explained in Table 183.

Table 183 Aiming page attributes - BHS



Attribute	Meaning
Refer Table 161 for Atributes details.	

Alignment Tone

For coarse alignment of the SM/BHS, use the Alignment Tool located at **Tools -> Alignment Tool**. Optionally, connect a headset alignment tone kit to the AUX/SYNC port of the SM/BHS and listen to the alignment tone, which indicates greater SM/BHS receive signal power by pitch. By adjusting the SM's/BHS's position until the highest frequency pitch is obtained operators and installers can be confident that the SM/BHS is properly positioned. For information on device GUI tools available for alignment, see sections Aiming page and Diagnostic LED – SM/BHS on page 8-16, Using the Link Capacity Test tool on page 8-22 and Using AP Evaluation tool on page 8-34.

Figure 169 PMP/PTP 450i Series link alignment tone

Note

The Alignment Tone cable for a 450i Series uses an RJ-45 to headset cable where as the 450 Series alignment tone cable uses an RJ-12 to headset cable.

Alignment Tool Headset and alignment tone adapters can be ordered from Cambium and Best-Tronics (http://btpa.com/Cambium-Products/) respectively using the following part numbers:

Table 184 Alignment Tool Headsets and Alignment tone adapter third party product details

Reference	Product description
ACATHS-01A	Alignment tool headset for the PMP/PTP 450 and 450i Series products
BT-1277	Headset alignment cable (RJ-45) for the PMP/PTP 450i Series products
BT-0674	Headset alignment cable (RJ-12) for the PMP/PTP 450 Series products.

Using the Link Capacity Test tool

The **Link Capacity Test** tab allows you to measure the throughput and efficiency of the RF link between two modules. Many factors, including packet length, affect throughput.

The Link Capacity Test tool has following modes:

- **Link Test with Multiple VCs**: Tests radio-to-radio communication across selected or all registered VCs, but does not bridge traffic (PMP 450m Series AP only).
- **Link Test without Bridging**: Tests radio-to-radio communication, but does not bridge traffic.
- **Link Test with Bridging**: Bridges traffic to "simulated" Ethernet ports, providing a status of the bridged link.
- **Link Test with Bridging and MIR**: Bridges the traffic during test and also adheres to any MIR (Maximum Information Rate) settings for the link.
- **Extrapolated Link Test**: Estimates the link capacity by sending few packets and measuring link quality.

The **Link Capacity Test** tab contains the settable parameter **Packet Length** with a range of 64 to 1714 bytes. This allows you to compare throughput levels that result from various packet sizes.

The **Current Results Status** also displayed date and time of last performed Link Capacity Test. If there is any change in time zone, the date and time will be adjusted accordingly.

Note

The Extrapolated Link Test can be run by Read-Only login also.

Performing Link Test

The link test is a tool that allows the user to test the performance of the RF link. Packets are added to one or more queues in the AP in order to fill the frame. Throughput and efficiency are then calculated during the test. The 450 and 450i APs offer link test options to one SM at a time. The 450m AP offers the option of a link test to multiple VCs at the same time. This allows the user to test throughput in MU-MIMO mode, in which multiple SMs are served at the same time.

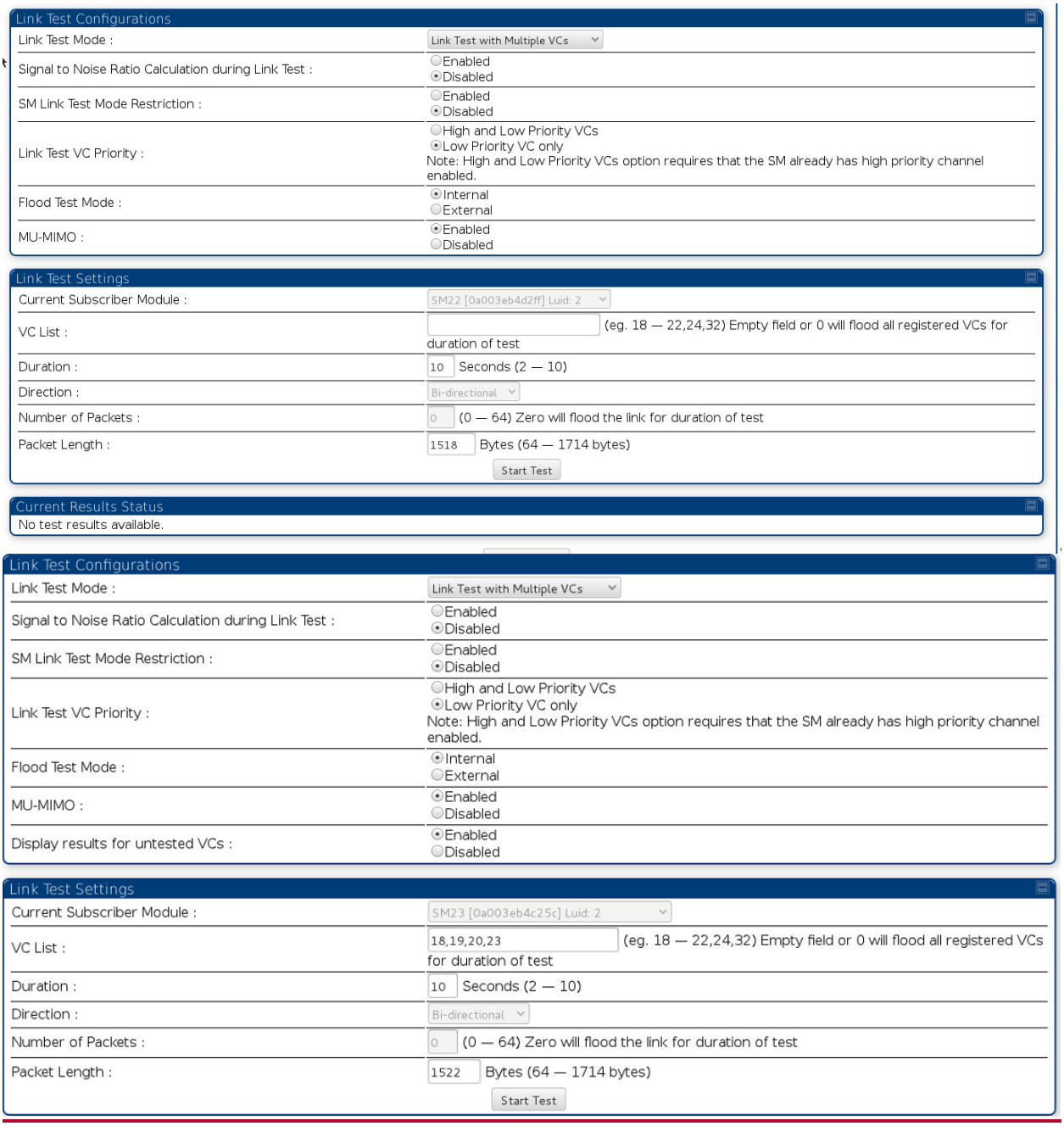
This new link test can be found under **Tools > Link Capacity Test**

Link Test with Multiple VCs

Note

The “Link Test with Multiple VCs” Link Capacity Test is supported for PMP 450m Series AP only.

Figure 170 Link Capacity Test – PMP 450m Series AP



Procedure 31 Performing a Link Capacity Test - **Link Test with Multiple VCs**

Link Test Configurations parameters

1 Access the Link Capacity Test tab in the Tools web page of the module.

2 Select Link Test Mode –

Options are: **Link Test with Multiple VCs**, **Link Test without Bridging**, **Link Test with Bridging**, **Link Test with Bridging** and **MIR, Extrapolated Link Test**
All options except for the Link Test with Multiple VCs are available also for the 450 and 450i APs.

3 Set the **SM Link Test Mode Restriction** attribute to enable or disable. Setting this to enabled, prevents activation of SM initated link tests.

4 Set **Signal to Noise Ratio Calculation during Link Test** attribute to enable or disable.

5 Set **Link Test VC Priority** attribute to either High and Low Priority VCs or Low Priority VC only.

6 Select **Flood Test Mode** –

Options are: Internal and External

Default is Internal. When set to Internal, packets are sent from AP -> SM over RF. When set to External, packets will all flow out the Ethernet port.

7 Set MU-MIMO attribute to enable or disable .

Note: The MU-MIMO feature is enabled on the Low Priority VC only

Link Test Settings parameters

6 Select the subscriber module to test using the Current Subscriber Module parameter.
Note: This parameter is not available in BHM.

7 Enter **VC List** (applicable for PMP 450m AP only)

The Current Subscriber Module and VC List are valid only when selecting Link Test with Multiple VCs.

- Current Subscriber Module: select the VC to perform the link test with
- VC list: select a list or range of VCs to include in the link test with multiple VCs

  If left blank, all VCs will be included in the link test

8 Type into the **Duration** field how long (in seconds) the RF link must be tested.

9 Select the **Direction** – Bi-directional, Uplink Only or Downlink Only.

10 Type into the **Number of Packets** field a value of **0** to flood the link for the duration of the test.

11 Type into the **Packet Length** field a value of **1714** to send 1714-byte packets during the test.

12 Click the **Start Test** button.

Figure 171 Link Test with Multiple VCs (1518-byte packet length)

Current Results Status

Test Duration: 10 Pkt Length: 1500 Test Direction Downlink

Link Test with Multiple VCs

VC	Rate	Efficiency	Fragments		Downlink Rate		Grouping Ratio
			Transmit	Received	SU-MIMO	MU-MIMO	
Total VCs	**422.20 Mbps**	**99%**	**8294086**	**8246226**			
18 (Low Priority)	60.53 Mbps	99%	1184676	1182411	8X/8X MIMO-B	8X/4X MIMO-B	100%
19 (Low Priority)	59.43 Mbps	98%	1184260	1160784	8X/6X MIMO-B	8X/4X MIMO-B	100%
20 (Low Priority)	60.45 Mbps	99%	1184670	1180694	8X/8X MIMO-B	8X/4X MIMO-B	100%
21 (Low Priority)	60.45 Mbps	99%	1184972	1180774	8X/8X MIMO-B	8X/4X MIMO-B	100%
22 (Low Priority)	60.38 Mbps	99%	1185564	1179346	8X/8X MIMO-B	8X/4X MIMO-B	100%
23 (Low Priority)	60.53 Mbps	99%	1184972	1182386	8X/8X MIMO-B	8X/4X MIMO-B	100%
24 (Low Priority)	60.40 Mbps	99%	1184972	1179831	8X/8X MIMO-B	8X/4X MIMO-B	100%

Slot Grouping

Group Size	% Distribution	Average Slot Count
1	0.0	0
2	0.0	0
3	0.0	0
4	0.0	0
5	0.0	0
6	0.0	0
7	100.0	73

Link Test ran on 01:33:45 01/02/2016 UTC

Current Results Status

Test Duration: 10 Pkt Length: 1522 Test Direction Downlink

Link Test with Multiple VCs

Subscriber Module	VC	Throughput	Efficiency	Fragments		Downlink Rate		Grouping Ratio
				Transmit	Received	SU-MIMO	MU-MIMO	
	Total VCs	**185.33 Mbps**	**99%**	**3625769**	**3619730**			
SM23 - [0a-00-3e-b4-c2-5c] - LUID: 002	18 (Low Priority)	46.01 Mbps	99%	899716	898796	8X/8X MIMO-B	8X/8X MIMO-B	99%
SM11 - [0a-00-3e-b4-24-1a] - LUID: 003	19 (Low Priority)	33.47 Mbps	99%	655056	653873	8X/8X MIMO-B	8X/8X MIMO-B	100%
SM12 - [0a-00-3e-b4-24-08] - LUID: 004	20 (Low Priority)	59.03 Mbps	99%	1156205	1153053	8X/8X MIMO-B	8X/8X MIMO-B	99%
SM21 - [0a-00-3e-b4-d3-36] - LUID: 007	23 (Low Priority)	46.79 Mbps	99%	914792	914008	8X/8X MIMO-B	8X/8X MIMO-B	99%

Slot Grouping

Group Size	% Distribution	Average Slot Count
1	0.0	0
2	100.0	56
3	0.0	0
4	0.0	0
5	0.0	0
6	0.0	0
7	0.0	0

Aggregate Throughput: 185.33 Mbps

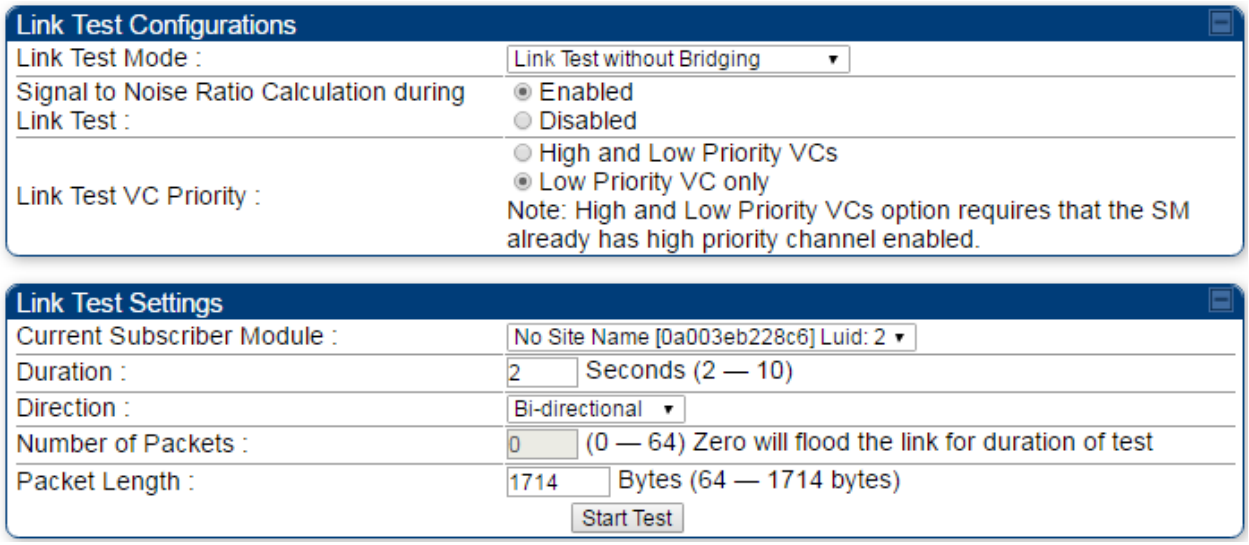
Unicast traffic to untested VCs

VC	Throughput
Total VCs	**1.22 kbps**
21 (Low Priority)	204 bps
22 (Low Priority)	204 bps
24 (Low Priority)	204 bps
25 (Low Priority)	204 bps
26 (Low Priority)	204 bps
27 (Low Priority)	204 bps

Link Test ran on 22:52:09 01/06/2016 UTC

Link Test without Bridging, Link Test with Bridging or Link Test with Bridging and MIR

Figure 172 Link Capacity Test – PMP 450/450i Series AP



Refer Link Test with Multiple VCs on page 8-23 for Link Test procedure.

Figure 173 Link Test without Bridging (1714-byte packet length)

Current Results Status

Stats for LUID: 2 Test Duration: 2 Pkt Length: 1714 Test Direction Bi-Directional

Link Test without Bridging

VC	Downlink	Uplink	Aggregate	Packet Transmit	Packet Receive
				Actual	Actual
18	10.90 Mbps	4.10 Mbps	15.00 Mbps, 1084 pps	1575 (787 pps)	595(297 pps)

Efficiency

Downlink				Uplink			
Efficiency	Fragments count		Signal to Noise Ratio	Efficiency	Fragments count		Signal to Noise Ratio
	Actual	Expected			Actual	Expected	
100%	42594	42594	40 dB V 39 dB H	100%	16020	16020	42 dB V 41 dB H

Link Quality

Downlink

RF Path	Modulation	Fragments	Modulation Percentage	Average Corrected Bit Errors
V	QPSK	6370	30%	0.261
V	16-QAM	5514	26%	0.310
V	64-QAM	5009	23%	0.350
V	256-QAM	4506	21%	0.366
H	QPSK	6017	28%	0.294
H	16-QAM	5513	26%	0.421
H	64-QAM	5009	24%	0.683
H	256-QAM	4506	21%	0.427

Uplink

RF Path	Modulation	Fragments	Modulation Percentage	Average Corrected Bit Errors
V	QPSK	2397	30%	0.080
V	16-QAM	2088	26%	0.137
V	64-QAM	1899	23%	0.147
V	256-QAM	1710	21%	0.167
H	QPSK	2277	28%	0.150
H	16-QAM	2087	26%	0.242
H	64-QAM	1898	24%	0.401
H	256-QAM	1709	21%	0.256

Link Test ran on 00:15:31 01/01/1970 UTC

Currently transmitting at:

VC 18 Rate 8X/8X MIMO-B

Performing Extrapolated Link Test

The Extrapolated Link Test estimates the link capacity by sending few packets and measuring link quality. Once the test is initiated, the radio starts session at the lower modulation, 1X, as traffic is passed successfully across the link, the radio decides to try the next modulation, 2X. This process repeats until it find best throughput to estimate capacity of link.

Note

It is recommended to run Extrapolated Link Test where the session must have been up and have traffic present on it in order to get accurate test results. This is essential for the radio to modulate up to get an accurate measurement.

Running the Extrapolated test just after establishing session will not provide accurate results.

The procedure for performing Extrapolated Link Test is as follows:

Procedure 32 Performing an Extrapolated Link Test

1. Access the Link Capacity Test tab in the Tools web page of the module.
2. Select Link Test Mode **Extrapolated Link Test**
3. Click the **Start Test** button.
4. In the Current Results Status block of this tab, view the results of the test.

Figure 174 Extrapolated Link Test results

Current Results Status

Stats for LUID: 2 Test Duration: 2 Pkt Length: 1714 Test Direction Bi-Directional

Extrapolated Link Test

Downlink	Uplink	Aggregate
48.66 Mbps	7.78 Mbps	56.44 Mbps

Transmit modulation Down: 4X Up: 2X
Efficiencies Down:99 Up:100
Slots carrying data: Downlink/Uplink: 60/19

Note: Extrapolated Link Test just sends over a few packets measuring their quality and extrapolates that to what the expected throughput would be. This is just an approximation to have minimal service impact.

Efficiency

Downlink				Uplink			
Efficiency	Fragments count		Signal to Noise Ratio	Efficiency	Fragments count		Signal to Noise Ratio
	Actual	Expected			Actual	Expected	
99%	2049	2044	22 dB V 22 dB H	100%	2009	2009	0 dB V 0 dB H

Link Quality

Downlink

RF Path	Modulation	Fragments	Modulation Percentage	Average Corrected Bit Errors
V	QPSK	426	50%	0.000
V	16-QAM	425	50%	0.000
H	QPSK	425	50%	0.000
H	16-QAM	425	50%	0.000

Uplink

RF Path	Modulation	Fragments	Modulation Percentage	Average Corrected Bit Errors

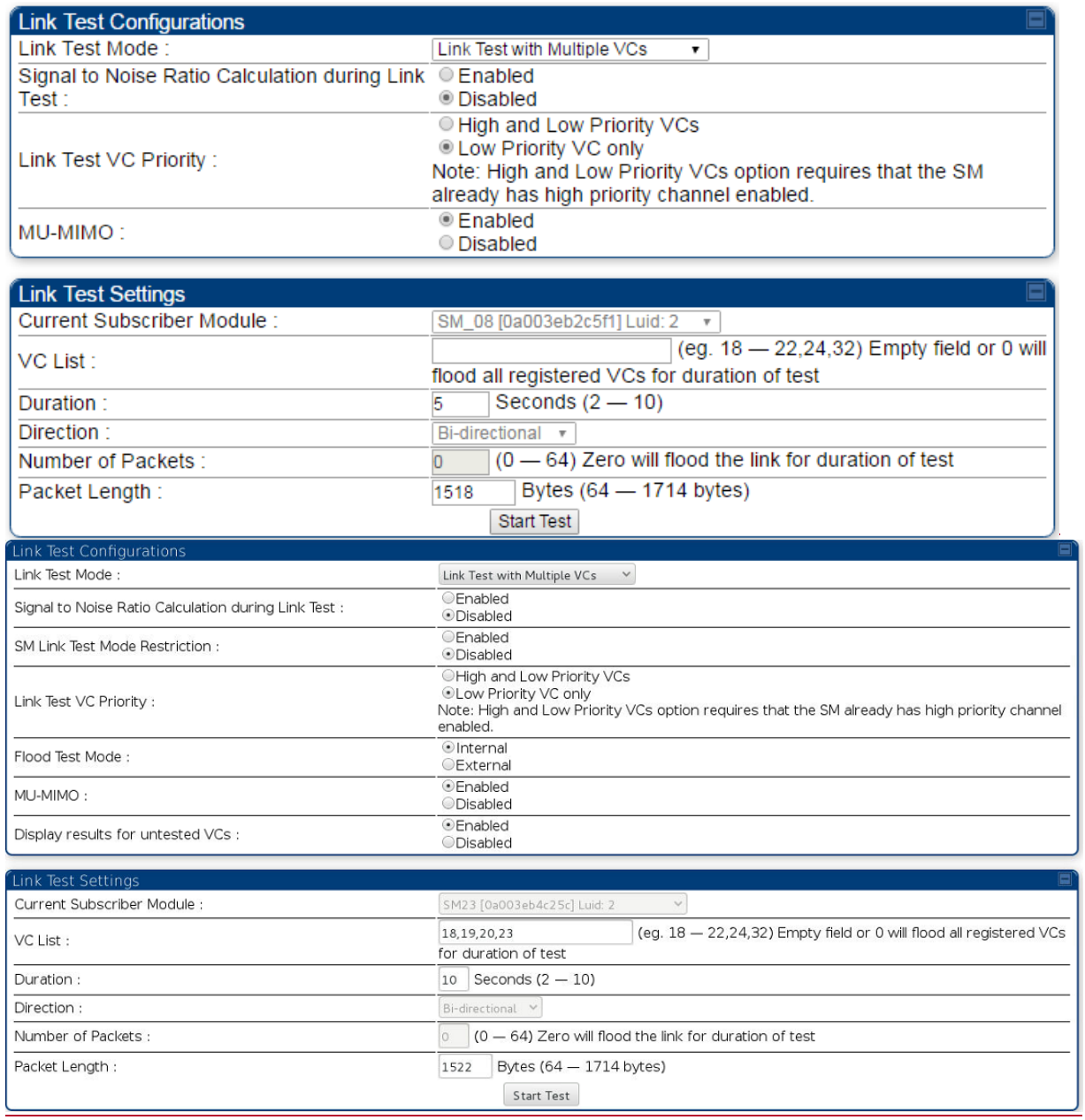
Link Test ran on 00:08:25 01/01/2011 UTC

Currently transmitting at:
VC 18 Rate 8X/6X MIMO-B

Link Capacity Test page of AP

The Link Capacity Test page of AP is explained in Table 185.

Table 185 Link Capacity Test page attributes – AP



Attribute	Meaning

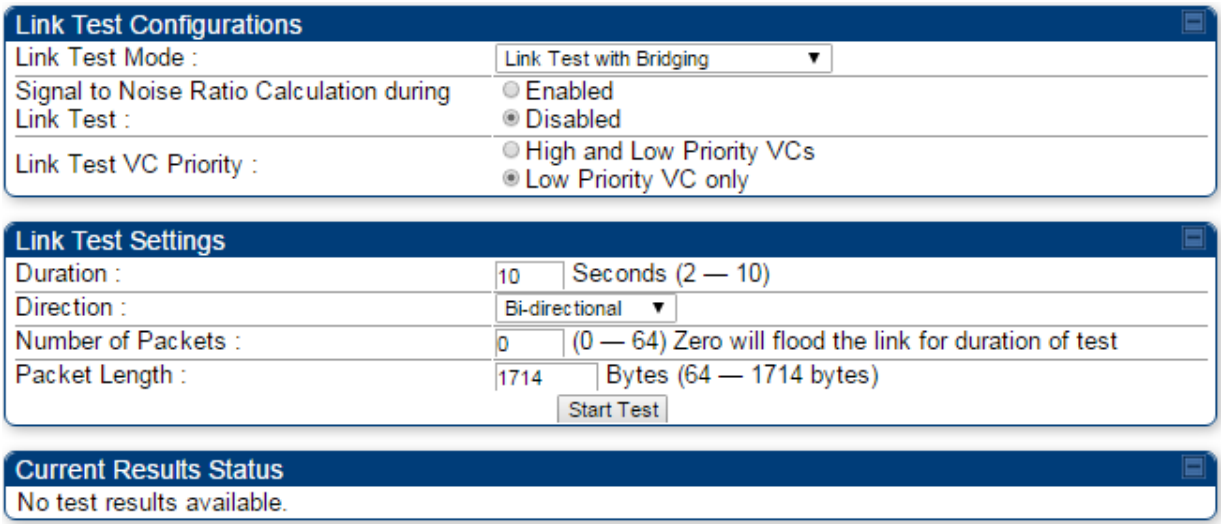
Link Test Mode	Select Link Test Mode from drop down menu : • Link Test with Multiple VCs (PMP 450m Series AP only) • Link Test without Bridging • Link Test with Bridging • Link Test with Bridging and MIR • Extrapolated Link Test
Signal to Noise Ratio Calculation during Link Test	Enable this attribute to display Signal-to-Noise information for the downlink and uplink when running the link test.
Link Test VC Priority	This attribute may be used to enable/disable usage of the high and low priority virtual channel during the link test.
Flood Test Mode	This field determines whether a packet is sent out of the SM's Ethernet port (external) or not (internal). **Note:** This field is applicable only when the "Link Test Mode" field is set to "Link Test with Multiple VC's" option.
MU-MIMO	This field determines whether the DL flood test packets use MU-MIMO grouping or not. **Note:** This field is applicable only when the "Link Test Mode" field is set to "Link Test with Multiple VC's" option.
Display results for untested VCs	If "Link test with multiple VC's" is run and a subset of registered VC's enters into the VC List field, then enabling this field produces a table that displays results for VC's with traffic which are in session; but not tested as part of the link test.
Current Subscriber Module	The SM with which the Link Capacity Test is run. This field is only applicable for AP (not SM page).
VC List	This field is displayed for PMP 450m Series AP. It is only applicable for "Link Test with Multiple VCs" Test mode. Enter **VC List** (e.g. 18 or above for low priority VCs and 255 or above for high priority VCs or 0 for all registered VCs) which needs to be used for link test traffic.
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.
Direction	Configure the direction of the link test. Specify **Downlink** or **Uplink** to run the test only in the corresponding direction only. Specific **Bi-Directional** to run the test in both directions.
Number of Packets	The total number of packets to send during the Link Capacity Test. When Link Test Mode is set to **RF Link Test** this field is not configurable.

Packet Length	The size of the packets in Bytes to send during the Link Capacity Test

Link Capacity Test page of BHM/BHS/SM

The Link Capacity Test page of BHM/BHS is explained in Table 186.

Table 186 Link Capacity Test page attributes – BHM/BHS



Attribute	Meaning
Link Test Mode	See Table 185 on page 8-31
Signal to Noise Ratio Calculation during Link Test	See Table 185 on page 8-31
Link Test VC Priority	See Table 185 on page 8-31
Duration	See Table 185 on page 8-31
Direction	See Table 185 on page 8-31
Number of Packets	See Table 185 on page 8-31
Packet Length	See Table 185 on page 8-31

Using AP Evaluation tool

The **AP Evaluation** tab on **Tools** web page of the SM provides information about the AP that the SM sees.

Note

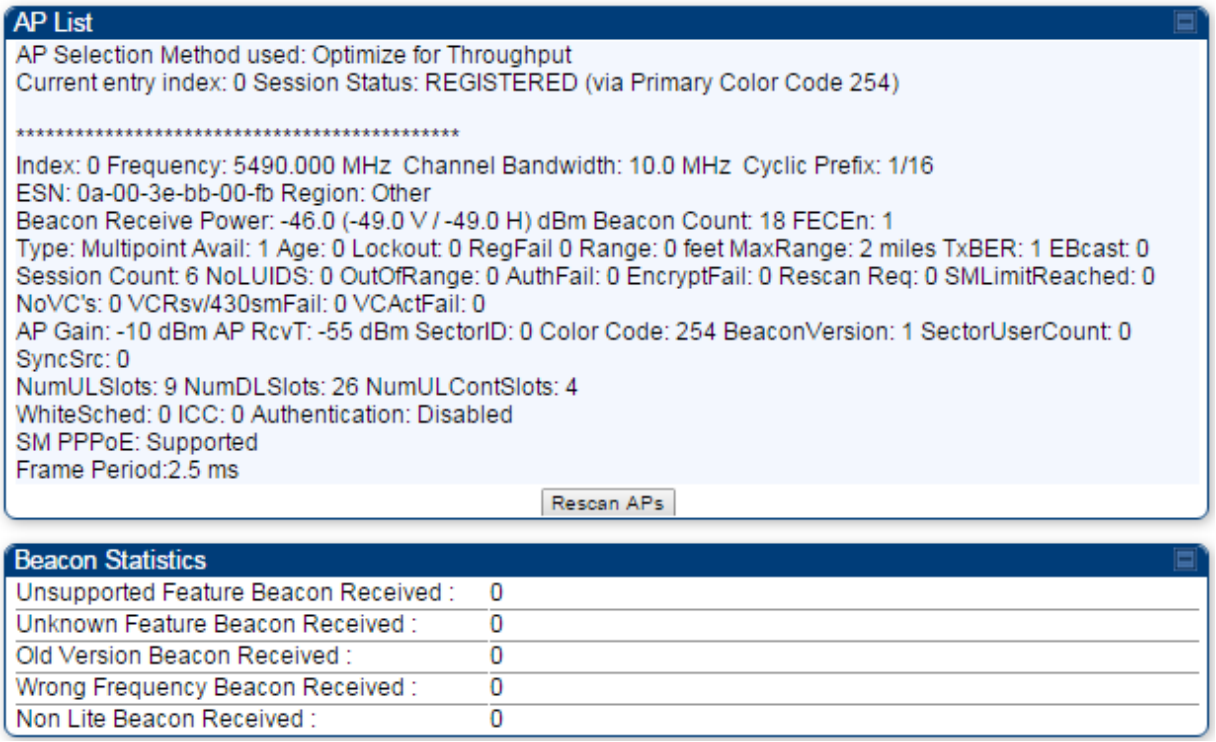
The data for this page may be suppressed by the **SM Display of AP Evaluation Data** setting in the **Configuration > Security** tab of the AP.

The AP Eval results can be accessed via SNMP and config file.

AP Evaluation page

The AP Evaluation page of AP is explained in Table 187.

Table 187 AP Evaluation tab attributes - AP



Attribute	Meaning
Index	This field displays the index value that the system assigns (for only this page) to the AP where this SM is registered.
Frequency	This field displays the frequency that the AP transmits.
Channel Bandwidth	The channel size used by the radio for RF transmission. The setting for the channel bandwidth must match between the AP and the SM.

Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefixes mean that for every 16 bits of throughput data transmitted, an additional bit is used. The Cyclic Prefix 1/16 only can be selected at this time.
ESN	This field displays the MAC address (electronic serial number) of the AP. For operator convenience during SM aiming, this tab retains each detected ESN for up to 15 minutes. If the broadcast frequency of a detected AP changes during a 15-minute interval in the aiming operation, then a multiple instance of the same ESN is possible in the list. Eventually, the earlier instance expires and disappears and the later instance remains to the end of its interval, but you can ignore the early instance(s) whenever two or more are present.
Region	This field displays the AP's configured Country Code setting.
Power Level	This field displays the SM's combined received power level from the AP's transmission.
Beacon Count	A count of the beacons seen in a given time period.
FECEn	This field contains the SNMP value from the AP that indicates whether the Forward Error Correction feature is enabled. 0: FEC is disabled 1: FEC is enabled
Type	Multipoint indicates that the listing is for an AP.
Age	This is a counter for the number of minutes that the AP has been inactive. At 15 minutes of inactivity for the AP, this field is removed from the AP Evaluation tab in the SM.
Lockout	This field displays how many times the SM has been temporarily locked out of making registration attempts.
RegFail	This field displays how many registration attempts by this SM failed.
Range	This field displays the distance in feet for this link. To derive the distance in meters, multiply the value of this parameter by 0.3048.
MaxRange	This field indicates the configured value for the AP's Max Range parameter.
TxBER	A 1 in this field indicates the AP is sending Radio BER.
EBcast	A 1 in this field indicates the AP or BHM is encrypting broadcast packets. A 0 indicates it is not.