



Wireless Network Manager

Administration Guide

SONICWALL[®]

Contents

Getting Started with Wireless Network Manager	5
About Wireless Network Manager	5
Using the Wireless Network Manager Interface	5
Using Wireless Network Manager Guide	7
Overview	8
Dashboard	8
Alerts	12
Threats	12
Logs	13
Using Air Marshal	15
RF Survey	15
Discover and Report Unassociated Wireless Clients	16
Manually Manage Unauthorized Access Points	16
RF Spectrum	16
RF Monitor	17
Bluetooth LE	18
Managing Your Network	20
Network Hierarchy	20
Zones	21
Devices	22
General	23
Radio	27
SSL VPN	27
Port Settings	29
Viewing the Wireless Client Journey	31
Managing Switches Using Wireless Network Manager	33
Upgrading the Firmware for Specific Access Points	35
SonicWave Diagnostics	35
Managing Policies	37
Policy Hierarchy	38
Select a Network Policy	38
Select an SSID	50
Select a Security Policy	61

SSID Policies	66
Adding SSID Security Policies	66
Editing SSID Security Policies	67
Network Policies	70
Using Tags to Manage Access Points and SSIDs	70
Using Tags to Manage Access Points	70
Using Tags to Manage SSIDs	71
Wi-Fi Multimedia (WMM) Profiles	72
Creating Wi-Fi Multimedia (WMM) Policies	72
Enabling Wi-Fi Multimedia (WMM) Policies	73
Managing Switch Policies	73
Adding Switch Policies	73
Editing Switch Policies	74
Managing SNMP Policies	74
Setting the SNMP ID	74
Adding SNMP Policies	75
Editing SNMP Policies	76
Deleting SNMP Policies	76
Setting SNMP Policies	76
Managing Switch SNMP Policies	77
Adding Switch SNMP Policies	77
Editing Switch SNMP Policies	78
Applying Switch SNMP Policies	78
Disabling the Strict Rekey	79
Security	80
Security Policies	80
Content Filtering Service	81
Customizing Blockpage	84
Applying a Security Policy to an SSID Group	85
Capture Advanced Threat Protection	86
Cloud Anti-Virus	88
Access Control Policies	89
Geo-IP & Botnet	92
Application Control	92
Schedule Objects	93
Scheduling VAP Security Policy	94
App Objects	95
App Group	95
Admin	98
Reports	98
Generating Report Tasks	99
General Settings	100

Users	101
Configuring User Quota Control	101
Settings	103
General	103
Firmware	104
Notification Center	105
Certificates	110
Certificate for Guest Portal SAML Authentication	110
Using the WiFi Planner	110
SonicWall Support	112
About This Document	113

Getting Started with Wireless Network Manager

This SonicWall Wireless Network Manager Administration Guide gives you information to manage the security of your network.

Topics:

- [About Wireless Network Manager](#)
- [Using the Wireless Network Manager Interface](#)

About Wireless Network Manager

SonicWall Wireless Network Manager is a cloud-based network management system that simplifies access-point deployment, management, and monitoring. Wireless Network Manager is fully integrated with Capture Security Appliance, providing seamless integration with MySonicWall, Licensing, and the SonicExpress mobile app on your mobile device. The cloud-based infrastructure is user-friendly and resilient, simplifying access, control, and troubleshooting. Wireless Network Manager can be deployed across multiple regions, and is accessible from anywhere through an Internet connection.

The SonicWave access point devices in the Wireless Network Manager network handle all aspects of authentication, association, fast and secure roaming, data forwarding, and power and channel management. Even if the Internet goes down, the Wi-Fi stays up, so you can still reach critical network resources such as files, servers and databases.

Using the Wireless Network Manager Interface

The first screen that appears when you launch Wireless Network Manager is the main screen seen below. It is from this screen that most of the activities and options start in Wireless Network Manager. The Wireless Network Manager user interface has a main navigation pane down the left side. It is from this pane that the user makes choices for navigating through the various Wireless Network Manager tools, features, and displays. The small arrow at the top middle of the screen sends you back to the Capture Security Appliance. Many of the secondary

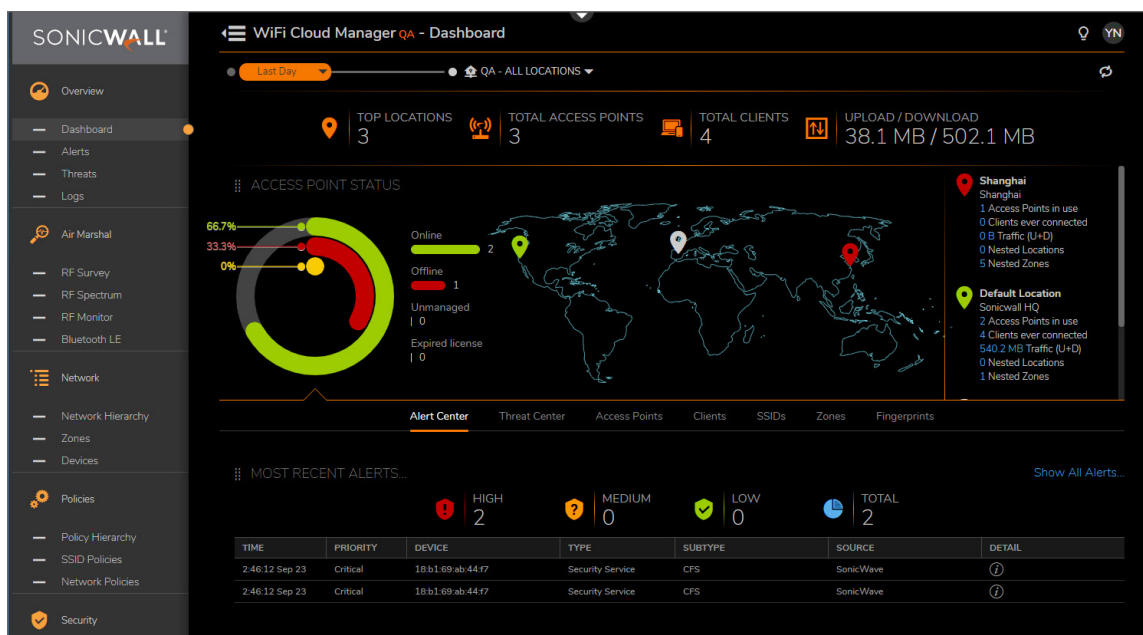
screens have an icon on the upper right border of the screen that, when clicked, sends you back to the main screen for that navigation pane item.

Clicking an option on the left navigation pane can sometimes open other choices. The principal headings on the navigation pane are:

- **Overview**
- **Air Marshal**
- **Network**
- **Policies**
- **Security**
- **Admin** (which includes Reports, User Settings, and Certificates)
- **Tools** (which includes **WiFi Planner**)

By clicking on a heading, some of these areas can be expanded or collapsed to show any additional sections or just the main headings.

The **Dashboard**, shown here, is the screen that is active when you sign on. On the screen below, all of the topics on the navigation pane are expanded to show the full range of choices. The small orange circle to the right of the navigation pane indicates which choice is currently active on the screen. This marker carries through the various screens resulting from steps started on the main screen. Other choices also appear from time to time within the various screens. By hovering over one of your locations, for example, you can bring up information about it. On some screens, hovering over a row brings up options to be applied to that row.



The topics available in this guide work through each of the choices on the navigation pane, giving an explanation of the selections that are available, and the screens that appear with each selection. This will help you configure and use Wireless Network Manager.

Using Wireless Network Manager Guide

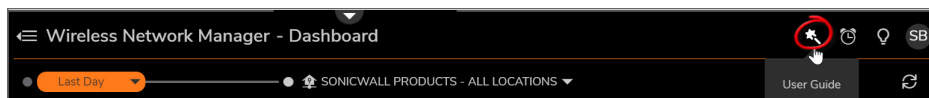
Wireless User Guide is an intuitive option available in the interface that guides you the steps needed to setup a new device. It also displays a screenshot of the interface as you navigate using the arrows. In each step, there is a button that directs you to the page where you can perform the necessary actions.

To navigate to Wireless Network Manager Guide:

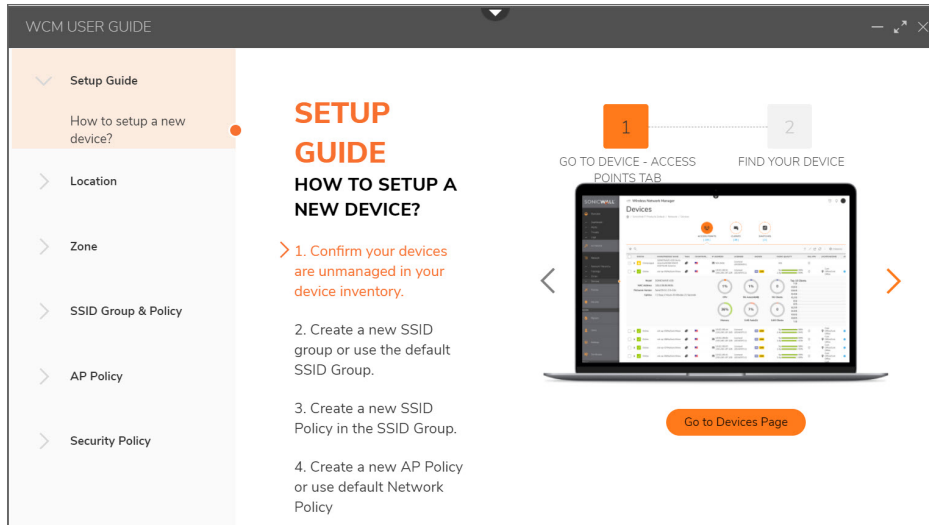
1. In the first screen that appears when you launch Wireless Network Manager, there are icons on the top right of the screen.



2. Click  and it opens WirelessGuide in a separate window. You can choose to resize, minimize or close the window. While going through the steps, you may close the window and if you click the icon again, you can resume from where you left off.



3. You can see the sections listed in the left view, step-by-step instructions in the right view with the screenshot of the respective steps. You also have an option to choose **Creating New** if you are creating a new device; or **Default** for the default settings.



Overview

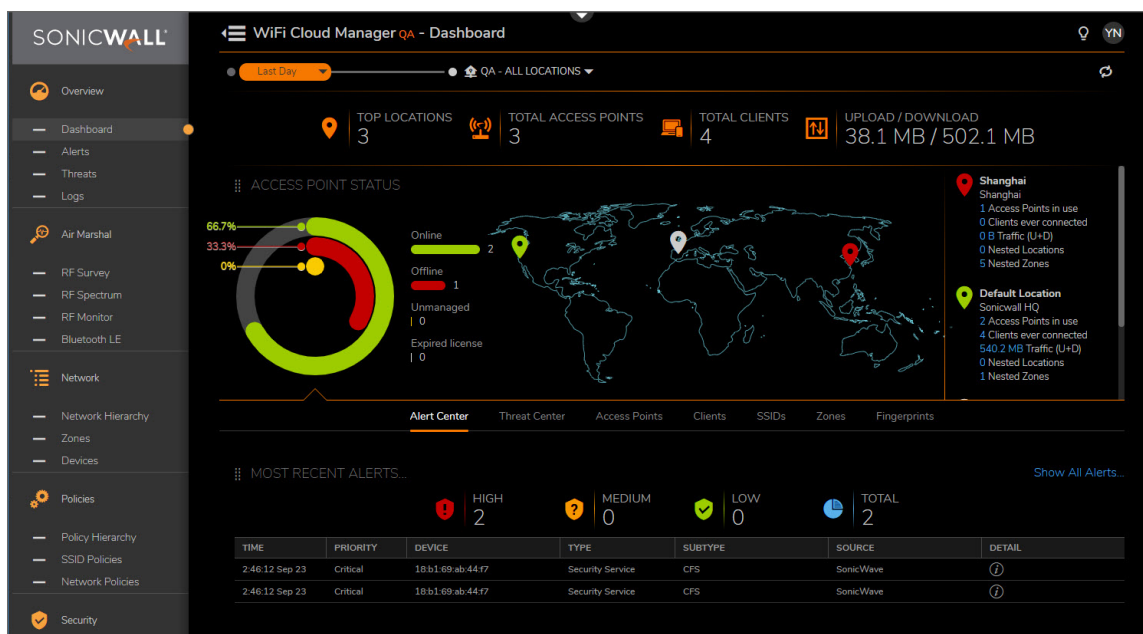
Overview, at the top of the navigation pane, includes four screen sets:

- **Dashboard**
- **Alerts**
- **Threats**
- **Logs**

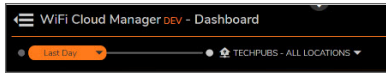
These screens provide an overview of the information Wireless Network Manager can provide, and allow the user to make choices about configuring the Wireless Network Manager environment.

Dashboard

The **Dashboard** provides a global map that displays all of your wireless deployment sites around the world.



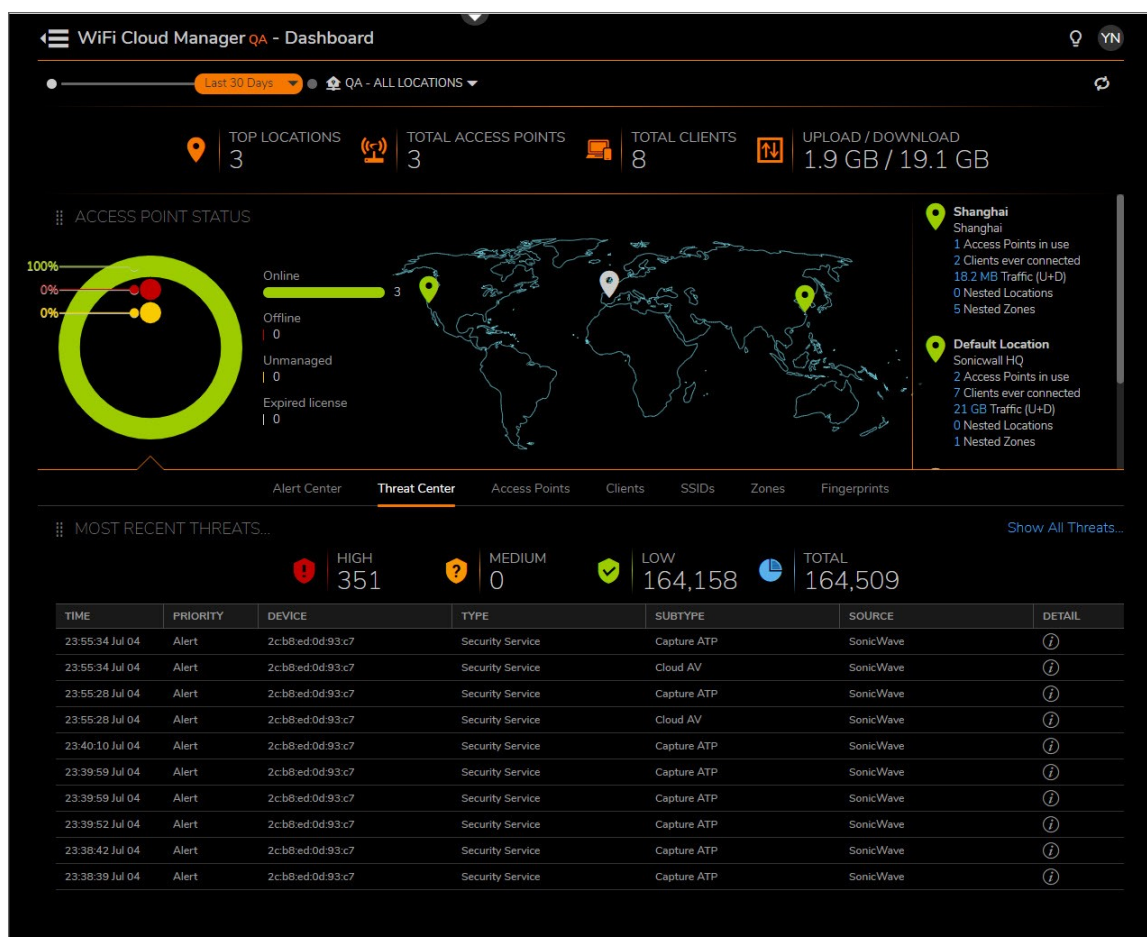
- The deployment details regarding the total number of devices and total traffic appear when you hover over each access point location on the map.
- The time slider tool at the top of the screen, can be used to adjust the time period displayed.



The choices are:

- **Last Day:** events that have taken place within the previous 24 hours
- **Last Week:** events that have taken place within the previous 7 days
- **Last 30 Days:** events that have taken place within the previous 30 days
- The **Access Point Status** in the top half of the screen displays AP statistics for access points on-line, off-line, unmanaged, and with expired licenses.
- **Alert Center** is the first of seven bars across the middle of the screen that can be clicked to display traffic data summaries and visual overviews. When the main screen first comes up, **Alert Center** is active. Clicking the **Alert Center** bar lists the most recent alerts. The columns display:
 - **Time**
 - **Priority**
 - **Device involved**
 - **Type of alert**
 - **Subtype** (picked up by which type of security policy)
 - **Source access point**

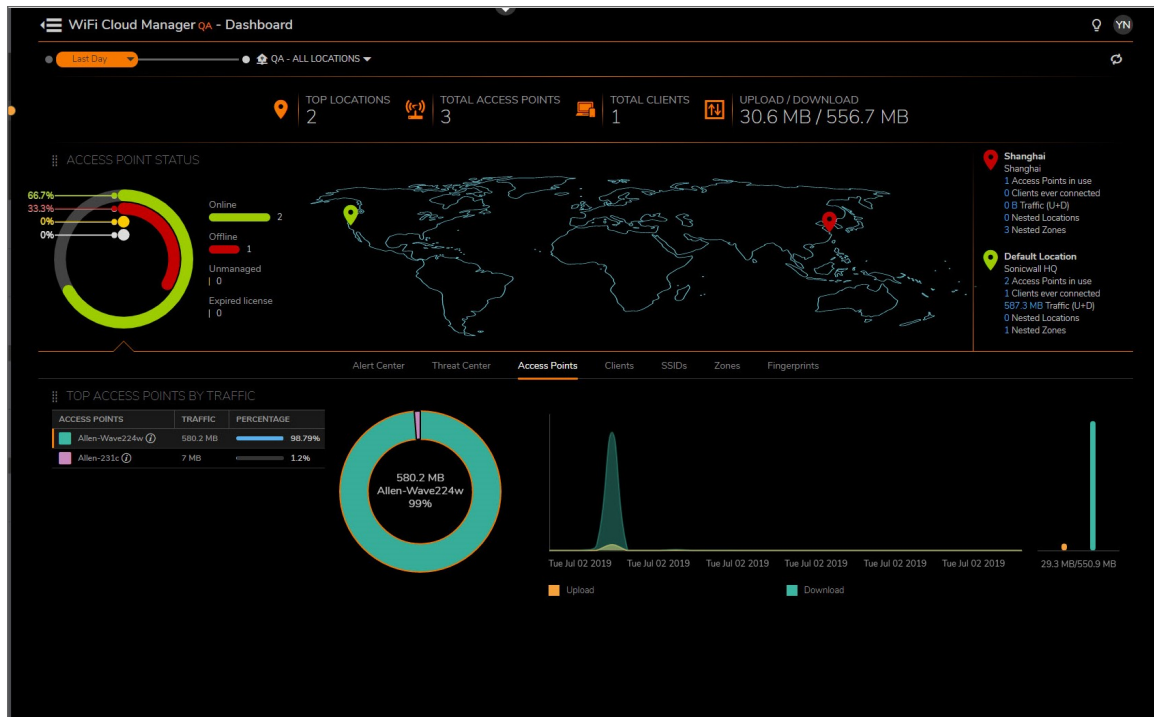
- The **Threat Center** bar shows the same screen but with the most recent threats in the bottom panel.



The columns display:

- **Time**
- **Priority**
- **Device involved**
- **Type of threat**
- **Subtype** (picked up by which type of security policy)
- **Source access point**

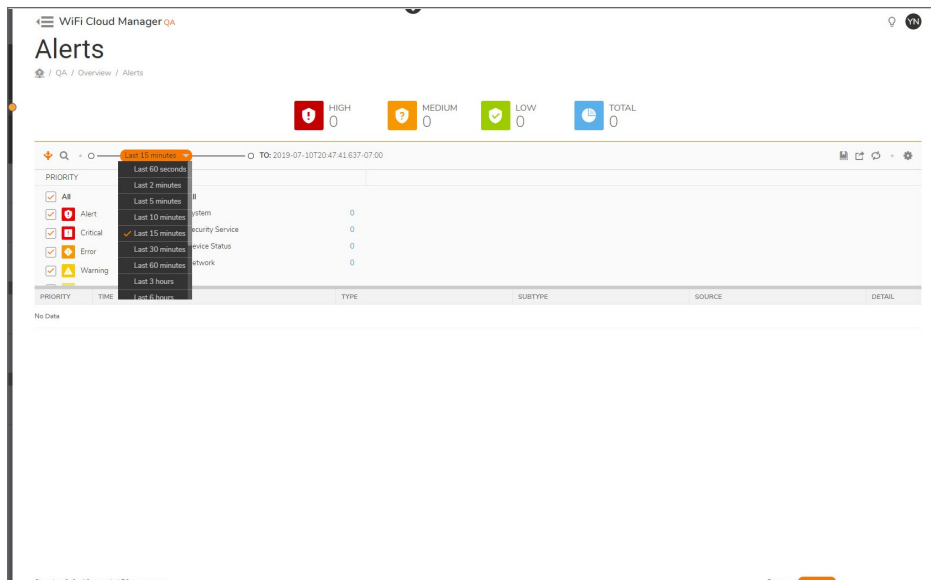
- When the **Access Points** bar is clicked, it lists the top access points by traffic. The top panel still displays the overview of your network and the access point status.



- **Clients** lists the top client devices by traffic.
- The **SSIDs** bar lists the top SSIDs by traffic.
- The **Zones** bar lists the top zones by traffic.
- The **Fingerprints** bar lists the client devices in your hierarchy with the operating system each one is using. In real time, it detects the connection of all client devices to your access points, and monitors their activity to display the top fingerprints by traffic.

Alerts

Right below **Dashboard** on the navigation pane are the **Alerts**, with detailed information about the alerts detected in your network. There is a time line that can be set for several different time periods. The first column shows the **Priority** of each alert and its criticality.



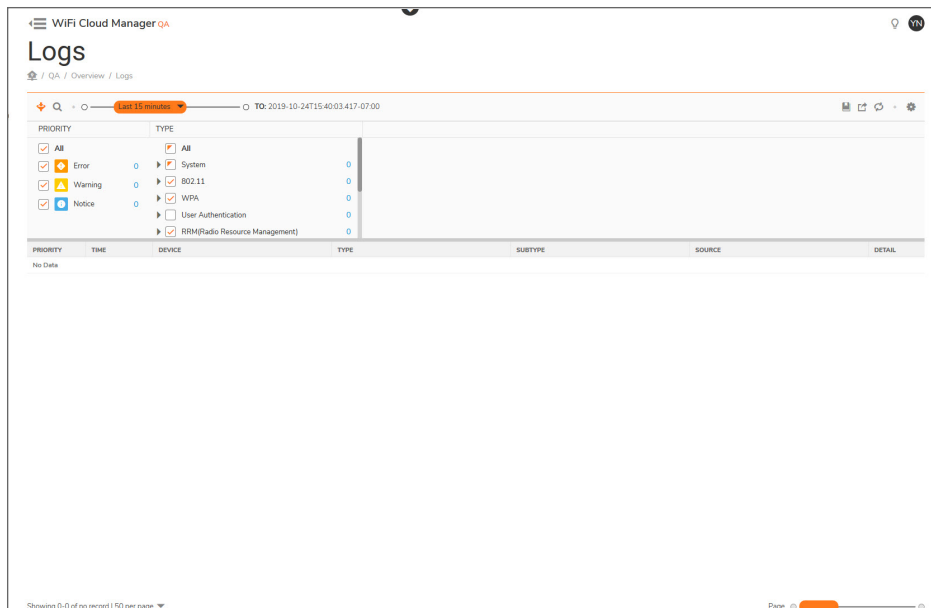
Threats

The **Threats** option brings up a similar screen detailing the threats during the chosen time period.

One of the options in the upper part of the **Threats** page is a check box to activate or deactivate **Wireless Intrusion Detection and Prevention (WIDP)** in the Wireless Network Manager. You can configure this feature on the **Policies > Policy Hierarchy > WIDP** page. (Refer to [WIDP Support](#) for more information). WIDP can detect and prevent attacks from rogue access points in the network.

Logs

Wireless Network Manager has a dedicated event log page. Selecting this option gives an overview of the logs requested for the chosen time period.



In the top section, check the boxes for the **Priority** and the **Type** of log collection to enable. The main types to choose from include:

- **All** - Clicking this option allows all logs to be collected.
- **System** - This option includes:
 - **CPU Status**
 - **Memory Status**
 - **Watchdog**
 - **Schedule**
- **802.11** - This option includes:
 - **Association**
 - **Disassociation**
 - **Mac Filter**
 - **Authentication**
 - **Deauthentication**
 - **Neighbor Report**
 - **WNM Sleep**
 - **BSS Transition**
- **WPA (Wi-Fi Protected Access)**
 - **WPA Group Key**

- **WPA Handshake**
- **WPA MIC Failure**
- **EAP** (Extensible Authentication Protocol)
- **User Authentication** - This option logs information about Guest Authentication.
- **RRM (Radio Resource Management)** - This option includes:
 - **Band Steering**
 - **Auto Channel**
 - **RSSI Threshold**
- **Network** - This option makes these options available:
 - **SSL VPN**
 - **3G/4G/LTE Modem**
- **BLE (Bluetooth Low Energy)** - This option includes:
 - **System Status**
 - **Command Status**

BLE is configured on the **Policy > Policy Hierarchy** page.

- **Mesh** - This option makes these options available:
 - **Mesh Peer Status**
 - **Mesh Interface**
 - **Mesh Role**
- **Cloud Management** - This option includes **Cloud Command**.
- **Audit** - This option enables logging of these items:
 - Tenant
 - Tenant User
 - Tenant Device
 - Location
 - Zone
 - Policy
 - SSID Group
 - SSID Profile
 - Device
 - Setting
 - Zone Device
 - Floor Plan
 - Floor Plan Device
 - User
 - Firmware
 - Address Object
 - Security Policy
 - Product Matrix
 - Switch
 - Zone Switch
 - Tenant Switch
 - Switch Policy
 - Floor Plan Switch

Using Air Marshal

Use Air Marshal to monitor and configure radio frequency (RF) selections in the Wireless Network Manager hierarchy.

Topics:

- RF Survey
- RF Spectrum
- RF Monitor
- Bluetooth LE

RF Survey

The **RF Survey** pages provide general information and configuration options related to the radio frequencies of the access points.

WiFi Cloud Manager QA

RF Survey

QA / Overview / RF Survey

NETWORK	DEVICE	TYPE	CHANNEL	AUTHENTICATION	THREAT TYPE
QA	☒ All	☒ 5G	152	☒ WPA2-PSK	☒ Unauthorized 265
Shanghai	☒ Online Devices	☒ 2.4G	119	☒ Open	☒ WPA2 73
Default Location				☒ WPA2	☒ Authorized 6
Madrid				☒ WPA-PSK	☒ WEP 2

#	DEVICE	SSID	THREAT TYPE	MAC ADDRESS	RADIO	CHANNEL	AUTHENTICATION	CIPHER	VENDOR	SIGNAL STRENGTH	MAX RATE
	Allen-Wave224v			18:51:69:4b:44:47							
1	Corp_WiFi_Lc		Unauthorized	18:51:69:8E:81:94	36	36	WPA2	AES	SONICWALL	800 Mbps	
2	shcy		Unauthorized	74:6A:C8:F4:9E:80	36	36	WPA2-PSK	AES	NEW H3C TECHNOLOGIES	433 Mbps	
3	Allen-Cloud-9F		Authorized	2C:8B:ED:0D:93:C9	36	36	WPA2-PSK	AES	SONICWALL	866 Mbps	
4	(Mesh)04643975		Unauthorized	2C:8B:ED:0D:93:DB	36	36	WPA2	AES	SONICWALL	866 Mbps	
5	Xiaomi_7152_5G		Unauthorized	8C:9E:BE:23:71:54	36	36	WPA2-PSK	AES	XIAOMI COMMUNICATIONS CO	144 Mbps	
6	Corp_WiFi_g		Unauthorized	18:51:69:8E:81:95	36	36	WPA2	AES	SONICWALL	800 Mbps	
7	Allen-Cloud-9F-101		Authorized	2C:8B:ED:0D:93:CA	36	36	WPA2-PSK	AES	SONICWALL	866 Mbps	
8	abcchina.com-in-5g		Unauthorized	2C:8B:ED:08:F1:73	36	36	WPA2-PSK	AES	SONICWALL	866 Mbps	
9	(Mesh)10622657		Unauthorized	2C:8B:ED:09:F1:85	36	36	WPA2	AES	SONICWALL	866 Mbps	
10	OMTsukoshi-Mia		Unauthorized	2C:8B:ED:08:EE:E9	36	36	WPA2-PSK	AES	SONICWALL	866 Mbps	
	Allen-Wave235a			18:51:69:49:74:43							
	Allen-231c			2c:8b:ed:0d:83:c7							

Showing 1-3 of 3 records | 10 per page

Page 1 of 1

- Choosing **RF Survey** gives a visual overview of the system's environment.
- The bottom panel displays a row with information for each online device.
- Clicking the arrow at the left end of the row expands or collapses the section to show more SSID information.

Discover and Report Unassociated Wireless Clients

Although some wireless clients may not be associated with a specific access point, they will still send occasional probe requests. The access points can collect the information about these clients and trace their locations. The information will be displayed on the **Air Marshal > RF Survey > Discovered Clients** page.

Manually Manage Unauthorized Access Points

You can manually authorize and acknowledge unauthorized access points.

To manually manage an unauthorized access point:

1. Navigate to the **Air Marshal > RF Survey** page.
2. Click **Discovered APs**.
3. Click **Scan Result** to view the list of detected access points.
4. On the right of the access point for which you want to authorize, click the **Authorize** icon.
5. In the **Threat Type** column, the access point now displays as **Authorized**.

To unauthorize an access point:

1. Navigate to the **Air Marshal > RF Survey** page.
2. Click **Discovered APs**.
3. Click **Authorized&Acknowledged** to view the list of authorized access points.
4. On the right of the access point for which you want to unauthorize, click the **Delete** icon.
5. In the **Scan Result** table, in the **Threat Type** column, the access point now displays as **Unauthorized**.

RF Spectrum

The **RF Spectrum** page lists the access points in your hierarchy, with the details of the Radio Quality on each of the bands it is on. Clicking on the right end of the row brings up details of the RF Spectrum, if it is supported on that device.



The **RF Spectrum** page displays the RF Spectrum and the Channel Utilization of the device. If the device is on two bands, click the band number in the upper left corner to show that band information. Hovering over parts of the charts gives readouts and averages.

RF Monitor

The **RF Monitor** feature provides Radio Frequency (RF) improvements to support spectrum visualization and analytics. RF interference can be better mitigated through the improved tools available on the RF Monitor screen.

WiFi Cloud Manager LOCAL

RF Monitor

/ [xlin_tenant_name](#) / Air Marshal / RF Monitor

Q - TO: 2019-11-06T10:10:48.349+08:00

GENERAL FRAME SETTING

- ☒ All
- ☒ Long Duration

MANAGEMENT FRAME

- ☒ All
- ☒ Management Frame Flood
- ☒ Null Probe Response
- ☒ Broadcasting Deauthentication
- ☒ Valid Station with invalid SSID
- ☒ Wardenreiter Detection

DATA FRAME

- ☒ All
- ☒ Unassociated Station
- ☒ NetStumbler Detection
- ☒ EAPOL Packet Flood
- ☒ Weak WEP IV

TIME	CLIENT	TYPE	SUBTYPE	VENDOR	RADIO TYPE	RSSI	RATE	ENCRYPT	DEVICE
10:08:37 Nov 06	B4:27:8D:51:3E:65	Management Frame	Ad-Hoc Station Detection	Unknown	802.11n	-88	Unknown	None	1881:69:76:75:9c
10:08:24 Nov 06	18:81:69:09:01:45	Management Frame	Null Probe Response	SONICWALL	802.11n	-73	1	None	1881:69:76:75:9c
10:08:11 Nov 06	74:6A:C8:F4:A8:20	General Frame	Long Duration	NEW H3C TECHNOLOGIES	802.11n	-88	54	None	1881:69:76:75:9c
10:05:43 Nov 06	D4:4E:D0:86:FD:5D	Data Frame	Weak WEP IV	Unknown	802.11n	-83	Unknown	None	1881:69:76:75:9c
10:03:18 Nov 06	18:91:1A:C7:F4:90	Management Frame	Null Probe Response	Unknown	802.11n	-53	54	None	1881:69:76:75:9c
10:03:15 Nov 06	18:81:69:A8:49:93	Management Frame	Ad-Hoc Station Detection	SONICWALL	802.11n	-50	54	None	1881:69:76:75:9c
10:03:10 Nov 06	10:5B:AD:01:19:2B	General Frame	Long Duration	MEGA WELL LIMITED	802.11n	-89	54	None	1881:69:76:75:9c

These include automated RF channel interference detection, and powerful tools for administrators needing to troubleshoot at deeper layers of the RF environment, and perhaps manually adjust radio settings.

One of the columns of data collected is the RSSI (Received Signal Strength Indicator). This is an indication of whether the signal is strong enough to get a good connection.

① | **NOTE: RF Monitor** is disabled by default.

To activate RF Monitor:

1. Navigate to **Policies > Network Policies**.
2. Select the network policy for which you want to enable RF monitoring.
3. Navigate to **Policies > Policy Hierarchy > WIDP**.
4. Activate **RF Monitoring**.
5. Change the duration of the **Measurement Interval (Seconds)** if you want it to be different from the default value.
6. Click **OK**.

Bluetooth LE

The **Bluetooth LE** page displays information about Bluetooth Low Energy (BLE) scan for each device.

#	DEVICE	MAC ADDRESS	RSSI	UUID	MAJOR	MINOR	POWER
1	Allen-Wireless	18:31:68:ab:44:f7	-94		0	0	0
2		1fa7f5:3e:13:82	-87		0	0	0
3		1e:0b:9f:44:94:82	-68		0	0	0
4		33:99:5e:4c:9a:89	-75		0	0	0
5		9e:00:03:cd:93:a1	-68		0	0	0
6		6c:c5:15:c2:23:aa	-72		0	0	0
7		39:14:2c:c4:70:37	-65		0	0	0
8		3a:65:a0:75:32:28	-81		0	0	0

BLE is available for transferring small amounts of data between nearby devices. The screen gives information about all the devices, or only those that are online.

For each device, it displays:

- Device name
- MAC Address
- RSSI
- UUID
- power information.

① | **NOTE:** BLE Scan reporting is only supported on SonicWave 224w models.

Managing Your Network

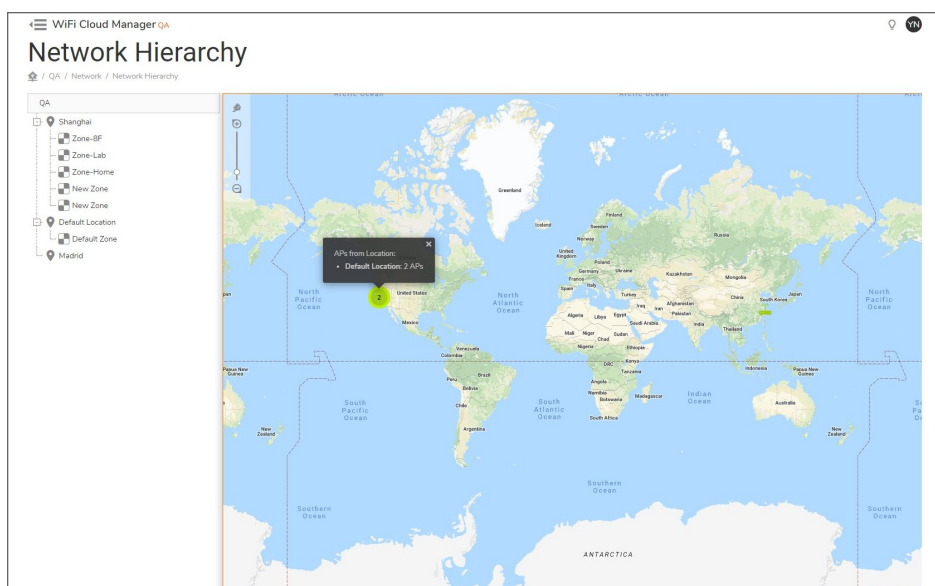
The **Network** page helps you configure your network.

Topics:

- [Network Hierarchy](#)
- [Zones](#)
- [Devices](#)

Network Hierarchy

After you have configured your network hierarchy, use the **Network Hierarchy** page to add, delete, edit, and copy locations, edit and delete zones, and manage zone policies in your tenant hierarchy.



For more information on setting up your hierarchy in Wireless Network Manager, refer to the *Wireless Network Manager Getting Started Guide*. This and other documentation are available under the product name “Secure

Cloud Wireless” on the SonicWall support website at: <https://www.sonicwall.com/support/technical-documentation/>.

Zones

The **Zones** page displays Information about all the zones you have created. You can configure your zones using this page.

ZONE	HIERARCHY	NETWORK POLICY	DEVICE COUNT
Zone-224w	ShanghaiZone-224w	Policy-224w	1

STATUS	NAME	MAC ADDRESS	IP ADDRESS	MODEL	MESH
Online	Allen-Wave224w	18b1.69ab.4417	192.168.88.240	SONICWAVE 224W	

ZONE NAME	HIERARCHY	NETWORK POLICY	DEVICE COUNT
Zone-Lab	ShanghaiZone-Lab	Policy-231o	1
New Zone	ShanghaiNew Zone	Default Policy	0
New Zone	ShanghaiNew Zone	Default Policy	0
Default Zone	Default Location/Default Zone	Default Policy	1

Icon Definition

- Click this icon to add a new zones.
- Click this icon to export data into an Excel or PDF file.
- Click this icon to refresh or reload the page.
- Click this icon to delete the selected options.
- Click this icon to select the grid settings or the required columns. This helps you to view or hide the selected columns and customize the data with the desired fields.

- Select a Zone on the bottom panel to see its place in the:
 - Zone name
 - Hierarchy
 - Network Policy
 - access point (AP) Device Count
- To add a zone, click on the **Add +** on the top right of the page.
- To Edit, Copy, Transfer Devices, or Delete a zone, hover over the options on the right end of the row.
- The **Transfer Devices** option makes it possible to move a device from one zone to another in one step.

- By expanding the **Zone** row, you get more information about each of the Zone Devices. This includes its:
 - Status (online or not)
 - Name
 - MAC Address
 - IP Addresses
 - Mesh Group (if it is part of one)

Devices

The **Devices** page provides options for different types of devices:

- **Access Point Devices** that are part of your **Network Hierarchy** host the **Client Devices** (the phones and computers that communicate through them).
- **Access Points** provides configuration and management information about access points. When you initially log onto Wireless Network Manager, all the SonicWave access points registered under your **MySonicWall** account are listed as inventory on this screen.

STATUS	NAME/FRIENDLY NAME	TAGS	COUNTRY/REG...	IP ADDRESS	LICENSED	RADIOS	RADIO QUALITY	SSL-VPN	LOCATION
Online	Lu_621/Lu_621			192.168.168.144 (4.35.65.189)	Licensed (2023/12/22)	5g 2.4g	5g 91% 2.4g 42%		Default Location
Offline	LL_681/LL_681			192.168.168.62 (140.207.81.26)	Licensed (2023/08/25)	5g 2.4g	N/A		Default Location
Offline	alica_621/alisa_621			192.168.168.65 (140.207.81.26)	Licensed (2023/03/04)	5g 2.4g	N/A		suzho

There is a filter icon on the left which lets you choose the devices to be displayed.

The middle panel shows the **Network** structure with the **Status** summary of each of the access points:

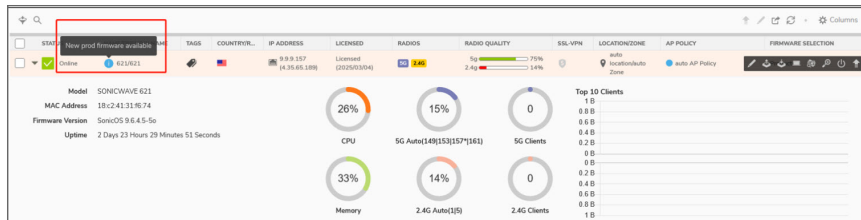
- **With AP managed, you will have options as Online, Offline, and Unmanaged.**
- **License** information
- **Model**

Configuration options for each access point in your network are made available by hovering along the right of the screen.

One of the columns in the bottom chart shows a colored **S** to show whether **SSL VPN** is enabled or not for that device. If the **S** is:

- green: the SSL VPN is connected.
- red: the SSL VPN is disconnected.
- gray: the SSL VPN is disabled.

If your firmware needs upgrading, a blue icon is displayed on left of AP name. Hover over the icon and it shows as **New firmware available**.



A **Configuration** screen comes up when you click on **Config/Edit** on the right of the SonicWave row.

- **General**
- **Radio**
- **Port Settings**
- **SSL VPN**

Topics:

- **Viewing the Wireless Client Journey**
- **Managing Switch Policies**
- **Using Tags to Manage Access Points and SSIDs**
- **Upgrading the Firmware for Specific Access Points**

General

You can configure the access point to use one of these **Route Modes**:

- **Bridge Mode**
- **Configuring NAT Mode**

Bridge Mode

The screenshot shows the 'Config SonicWave: 231c-xhu' interface. At the top, there are three tabs: 'General' (selected), 'Radio', and 'SSL-VPN'. Below the tabs is a section titled 'SYSTEM' with a dropdown arrow. It contains several fields: 'Name' (231c-xhu), 'Description' (empty), 'Country/Region' (US), 'Friendly Name' (231c-xhu), 'Route Mode' (Bridge, selected from a dropdown), 'Tags' (device taggg, with a plus button), and 'SNMP Engine ID' (800022250318B169AB561C). Below the SYSTEM section is a section titled 'MANAGEMENT' with a dropdown arrow. It contains two fields: 'Admin User Name' (admin) and 'New Password' (Leave blank if no change, with a refresh button).

To change the SonicWave mode to Bridge mode:

1. Click **General**.
2. Select **Bridge** from the **Route Mode** list.

Configuring NAT Mode

Wireless Network Manager provides SonicWave NAT mode in addition to the previous bridge mode.

Config SonicWave: 231c-xhu

General Radio SSL-VPN

SYSTEM

Name 231c-xhu ⓘ

Description

Country/Region US

Friendly Name 231c-xhu

Route Mode NAT

Mesh isn't supported on NAT mode device.

Tags device taggg +

SNMP Engine ID 800022250318B169AB561C

IP ADDRESS

Mode ☒ DHCP ☐ Static

4G/LTE FAILOVER & LOAD BALANCING

Enable USB Modem ☒

Enable USB Modem GUI Proxy in Standalone UI ☒

Mode ☒ Failover ☐ Load Balancing

MANAGEMENT

Admin User Name ⓘ admin

New Password ⓘ Leave blank if no change ⓘ

Cancel OK

NAT mode is usually used on single access point deployment. With NAT mode, the user does not need to set up a special DHCP server for the client. SonicWave sets up a DHCP server for each VAP automatically

ⓘ | **NOTE:** Mesh network is not supported for devices configured to use NAT mode.

ⓘ | **NOTE:** 4G/LTE mode is only supported on NAT mode.

To change the SonicWave mode to NAT mode:

1. Click **General**.
2. Select **NAT** from the **Route Mode** list.

When NAT mode is configured, **Static IP Address** configuration is supported.

To configure a static IP address:

1. Navigate to the **Network > Devices** page.
2. Select **Access Points**.
3. On the right of the device row, click **Config/Edit**. The **Config SonicWave** page displays.
4. Click **General**
5. Verify that the route mode is set to **NAT**.
6. In the **IP Address** section:
 - a. Set the mode to **Static**.
 - b. Set the static IP settings in the associated fields.
7. Click **OK**.

To configure for a DHCP IP address:

1. Navigate to the **Network > Devices** page.
2. Select **Access Points**.
3. On the right of the device row, click **Config/Edit**. The **Config SonicWave** page displays.
4. Click **General**
5. Verify that the route mode is set to **NAT**.
6. In the **IP Address** section, set the mode to **DHCP**.
7. Click **OK**.

Radio

The **Radio** page provides the administrator with control over Band Selection and various configuration options for each of the two available bands, 2.4 GHZ and 5 GHZ.

Config SonicWave: Allen-Wave224w

General

Radio

Port Setting

▼ BAND SELECTION

Band Selection

Dual band operation (2.4 & 5 GHz enabled)

Band Steering

Prefer 5GHz

▼ 2.4GHZ

Radio Mode

802.11n/g/b Mixed

Radio Band

Auto

Radio Channel

Auto

Transmit Power

Full Power

Auto Channel Selection to be 1, 6 and 11 Only

☐

Minimum bitrate(Mbps)

Lower Density

Higher Density

1

2

5.5

6

9

11

12

18

24

36

48

54

▼ 5GHZ

Radio Mode

802.11ac/n/a Mixed

Radio Band

Auto

Radio Channel

Auto

Transmit Power

Full Power

Minimum bitrate(Mbps)

Lower Density

Higher Density

6

9

12

18

24

36

48

54

Cancel

OK

Wireless Data Traffic Minimum Rate Control on the **Configure SonicWave** page improves wireless efficiency, since transfers at lower rates takes up excess available air time. Roaming improves with this feature, since, by disabling slow (*i.e.* bad) connections, the system forces devices to roam earlier.

SSL VPN

This feature provides supports for SSL-VPN connections to SonicWallSecure Mobile Access (SMA) appliances.

Wireless Network Manager Administration Guide
Managing Your Network

27

When the SonicWave is in standalone mode, the administrator can configure SSL-VPN settings from the web management interface. The SonicWave wireless access point will then launch a AvConnect client and control process to provide the secure tunnel for wireless client access.

The screenshot shows the 'Config SonicWave: 224w_f3fc' web interface. At the top, there are four tabs: 'General', 'Radio', 'SSL-VPN' (which is selected and highlighted with an orange border), and 'Port Setting'. Below the tabs, there are three expandable sections: 'SETTINGS', 'CERTIFICATE', and 'OTHERS'. In the 'SETTINGS' section, the 'SSL-VPN' toggle switch is turned on. In the 'CERTIFICATE' section, the 'Client Certificate' dropdown menu is set to 'Not Applied'. In the 'OTHERS' section, the 'Allow LAN2/LAN3/LAN4 SSL-VPN Security Tunnel Access' toggle switch is turned on. At the bottom right of the interface, there are 'Cancel' and 'OK' buttons.

Topics:

- [Settings](#)
- [Certificate](#)
- [Others](#)

Settings

To activate the SSL-VPN options for a device:

1. Navigate to **Network > Devices**.
2. Hover over the right section for device you want to configure until the icons appear.
3. Click the **Configure** (pencil) icon.
4. Click the **SSL-VPN** tab.
5. In the **Settings** section, click the **SSL-VPN** slider to activate SSL-VPN support.
6. Enter the values for the options for **SSL-VPN** connection.
7. Click **OK**.

Certificate

You can specify which client certificate should be used for the policy.

To specify a client certificate:

1. Navigate to **Network > Devices**.
2. Hover over the right section for device you want to configure until the icons appear.
3. Click the **Configure** (pencil) icon.
4. Click the **SSL-VPN** tab.
5. In the **Certificate** section, from the Client Certificate list, select the certificate you want used for the policy.
6. Click **OK**.

Others

This section allows you to allow your LAN connections SSL-VPN security tunnel access.

To allow SSL-VPN security tunnel access:

1. Navigate to **Network > Devices**.
2. Hover over the right section for device you want to configure until the icons appear.
3. Click the **Configure** (pencil) icon.
4. Click the **SSL-VPN** tab.
5. In the **Others** section, click the **Allow LAN2/LAN3/LAN4 SSL-VPN Security Tunnel Access** slider to allow SSL-VPN security tunnel access.
6. Click **OK**.

Port Settings

Wireless Network Manager provides a way for the user to enable or disable the LAN switch port. By default, the switch ports are down. To access this feature, edit the chosen device on this screen.

① | **NOTE:** This feature is only available for the SonicWave 224w.

Config SonicWave: 224w

General
Radio
Port Setting

PORT	POE
☒ Pass Through	--
☒ LAN 4 / PoE Out	☒
☐ LAN 3	--
☒ LAN 2	--

Cancel
OK

Wireless Network Manager provides Failover and Load Balancing support with 4G/LTE USB modems in SonicWave under cloud management.

By clicking on **Config/Edit** in the device row), then clicking on the **General** tab, you can edit a device on the **Config SonicWave** screen. (**NOTE:** The access point must be a model with a USB port.) The WAN load balance mode selections appear when the switch is in NAT mode.

Config SonicWave: 432_External

General
Radio
SSL-VPN

SYSTEM

Name
432_External ⓘ

Description

Country/Region
US

Friendly Name
432_External

Route Mode
NAT

☒ Mesh isn't supported on NAT mode device.

Tags
+

SNMP Engine ID
800022250318B1697B701C

IP ADDRESS

Mode
☒ DHCP
☐ Static

4G/LTE FAILOVER & LOAD BALANCING

Enable USB Modem
☒

Enable USB Modem GUI Proxy in Standalone UI
☒

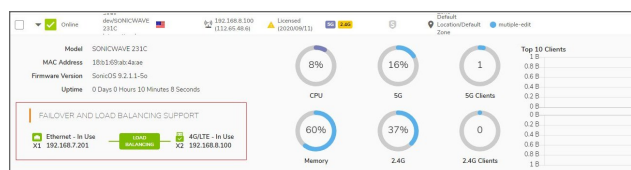
Mode
☒ Failover
☐ Load Balancing

MANAGEMENT

Admin User Name
admin

New Password
Leave blank if no change

When applied, these indicators are displayed:



The **Clients** page displays status information for the Client Devices, as seen below. At the top, there is a time line that can be slid from left to right to show:

- Last Day
- Last Week
- Last 30 Days.

It also displays the operating system used by each one of the Client Devices.

The screenshot shows the 'Devices' page in the SonicWave interface. It has a top navigation bar with 'ACCESS POINTS [9]', 'CLIENTS [56]', and 'SWITCHES [1]'. Below this is a filter bar with 'Filter (270 results) 192.168.8.100 131.05.40.6'. The main table has columns: NETWORK, STATUS, OS, PHYSICAL NODE, LOCATION/NAME/AP, SSB, RADIO, CONNECTION QUALITY, and RSSI. The table lists various devices, including 'sonicwall Products', 'Default Location', '400location@45', 'hosing', 'china1', and 'New location111'. Each device has a status (Connected or Disconnected), an OS (Linux, Windows, Windows Phone, MacOS, iPad iOS, iPhone iOS), and a physical node (e.g., 20M42 (2x2) 802.11n). The connection quality is shown as a percentage and a signal strength indicator.

The bottom panel has columns that give more information about each device.

Viewing the Wireless Client Journey

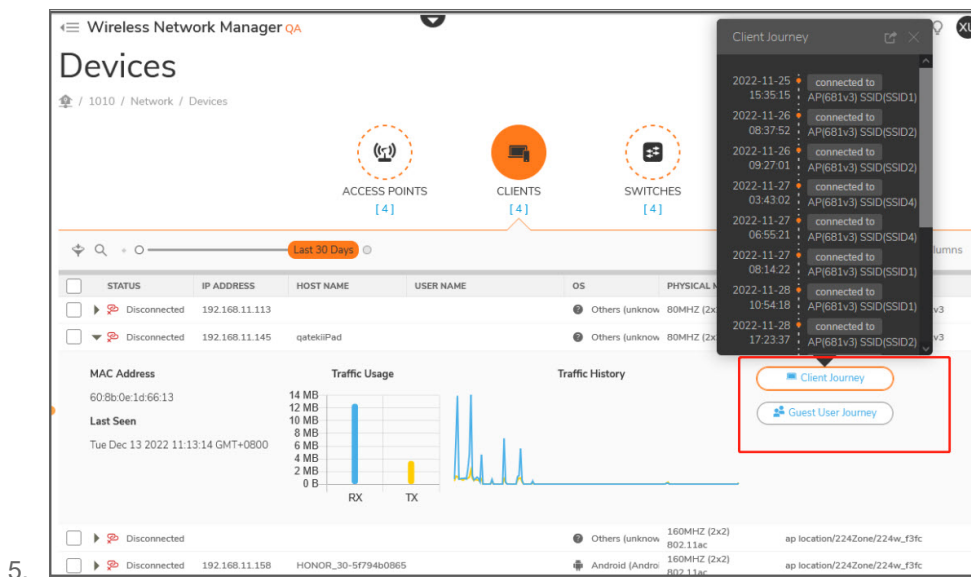
Wireless client journey is a feature administrators can track the behavior of wireless clients connected to a SonicWave, such as connection and disconnection of the wireless client.

To view the wireless client history:

1. Navigate to **Network > Devices**.
2. Click **Clients** from the items available at the top of the page. All of the wireless clients connected through SonicWave wireless access points are listed in the table.
3. Hover over a specific device to access the different icons :

-  Displays the logs.
-  Click to add the devices to the Client MAC Address Group. When you want to add a client mac to group, you must go to address group page to create a new group (if address group page has no groups), then click this button in client page, and you will see the group you added.
 ⓘ | **NOTE:** You can only select one group.
 Address group page will display the client mac information in the group and the client mac AO will be displayed in address objects page.
-  Disconnects the connected clients device. It takes around 5 minutes for the changes to take into effect.
 This button remains gray and can't be clicked when client is disconnected. When client status is connected, the button can be clicked.
 By clicking this button, the clients SSID gets disconnected. But this entry will not be changed in 5 minutes. After 5 minutes, the entry client status will be changed to disconnected.
-  Status of the sign-on
 - Navigate to **Policies > SSID Policies** page to edit SSID the connected client. Go to **Guest Portal** page, not only click-through option, select other options besides **None**.
 - After using client to connect SSID, you will be redirected to login website page. If this option is selected upon login, this icon changes to and **'log out user'**.
 - To login again, navigate to the website and enter the credentials.
 - After 5 minutes, the user name will be changed to unauthenticated, and gets disabled and displayed as **'user has been logout'**.
 - When you don't login to this page, the client host username will be unauthenticated, and the button gets disabled and displays as **'user has been logout'**
 - When Guest Portal type is selected as first option **None** and connects to SSID, this button remains gray and is displayed as **'guest disabled'**.
-  Edits the host name field.

4. Click on a specific wireless client to displays the details for that device.



The information displayed for the wireless client includes:

- MAC Address
- status
- IP address
- host name
- user name
- operating system
- physical mode
- location, zone, and access point
- SSID
- radio
- connection quality
- RSSI
- vendor
- last seen time

The **Traffic History** graph displays the current and historical traffic for the device.

There are two kind of client journey messages listed in the wireless client details

- **Client Journey** - connection and disconnection times of the client
- **Guest Journey** - behavior of any guest users who logged in using that wireless client

① | **NOTE:** The maximum tracking period for a device is 30 days.

Managing Switches Using Wireless Network Manager

You can use Wireless Network Manager to manage features of connected SonicWall Switches.

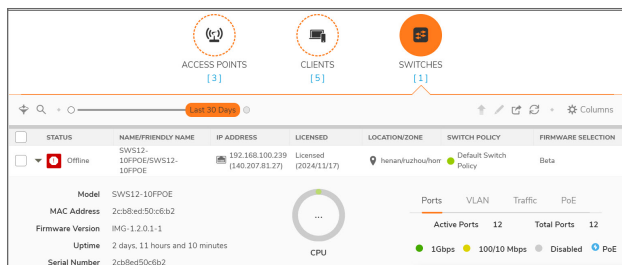
These Switch management features are supported by Wireless Network Manager in this release:

- Dashboard
- Network IPv4 Network
- System Information
- User Management
- ARP Global
- ARP Table
- Authentication
- Firmware Images - Upgrade
- DHCP Snooping - settings
- DHCP Relay
- Port Settings - QoS
- Port Settings - POE
- Port Settings - Security - 802.1x
- Port Settings - ACL Binding (IPv4)
- Port Settings - ACL Binding (IPv6)
- Port Settings - Advanced
- STP - Settings - Bridge Priority
- LBD - Global
- Link Aggregation
- Jumbo Frames
- MAC Address Table - Static MAC address
- MAC Address Table - Dynamic MAC address
- LLDP - Global Settings
- IGMP Snooping
- Multicast Filtering
- QoS
- Port Statistics
- Static Routes (IPv4)
- Static Routes (IPv6)
- IPv6 Neighbor Discovery (ND)
- IPv6 address of VLAN
- 802.1x
- DoS
- ACL Management
- 802.1Q
- Voice VLAN
- Log

NOTE: For the Switch to be managed by Wireless Network Manager, the switch firmware must be version 1.0.0.3-12s or higher. It is highly recommended that you upgrade the Switch firmware to version 1.1 once it is being managed by Wireless Network Manager.

To manage a Switch:

1. .Navigate to **Network > Devices**.
2. Click **Switches**.
3. Select the Switch you want to manage and hover over the far right section of the row to access the management icons.



For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on the SonicWall support website at: <https://www.sonicwall.com/support/technical-documentation/>.

Topics:

- **Managing Switch Policies**

Upgrading the Firmware for Specific Access Points

Wireless Network Manager, administrators can upgrade the firmware for specific SonicWave access points managed by Wireless Network Manager.

To upgrade the firmware for an access point:

1. Navigate to **Network > Devices**.
2. On the right of the access point for which you want to upgrade the firmware, click the **Upgrade** icon. The **Firmware Upgrade** dialog displays.
3. From the **Firmware Selection** list, select the type of firmware upgrade you want to perform:
 - **Production**: the latest approved firmware release
 - **Beta**: the latest Beta version firmware for the device
 - **Patch**: the latest patch release to currently installed firmwareThe version number of the associated firmware selection will be displayed.
4. Click **Upgrade**.
5. When the **Upgrade command sent to online access points** message displays, click **OK**.

SonicWave Diagnostics

You can use the Diagnostics to test the connections of your SonicWave wireless access points.

Topics:

- [Testing Connectivity With Your Gateway or DNS Addresses](#)
- [Testing Connectivity With Ping, Traceroute, or NSLookup](#)

Testing Connectivity With Your Gateway or DNS Addresses

You can test the connectivity of the SonicWave with your gateway or DNS addresses.

To test the connectivity of a SonicWave with your gateway or DNS addresses:

1. Navigate to the **Network > Devices** pages.
2. On the row for the device you want to test, hover over the far right area until the configuration icons appear.
 - ① | **IMPORTANT:** The device must be online.
3. Select the **Diagnostics** (magnifier) icon. the **Diagnose SonicWave** page displays.
4. In the **Gateway, DNS Connectivity** section, click **Test** next to the diagnostic test you want to run. The

results will be displayed next to that **Test** button.

5. Click **Close** to close the **Diagnose SonicWave** page.

Testing Connectivity With Ping, Traceroute, or NSLookup

You can use the Diagnostics to test the connections of your SonicWave using either through pings or a tracerout.

To test the connectivity of a SonicWave using pings or a tracerout:

1. Navigate to the **Network > Devices** pages.
2. On the row for the device you want to test, hover over the far right area until the configuration icons appear.
❗ | IMPORTANT: The device must be online.
3. Select the **Diagnostics** (gear) icon. the **Diagnose SonicWave** page displays.
4. In the **Diagnostics with Ping or Traceroute** section, select the **Tool** you want to use:
 - **Ping**
 - **Traceroute**
 - **NSLookup**
5. In the **IP Address/Hostname** field, enter the IP address or fully qualified domain name (FQDN) you want to test.
6. Click **Test**. The results will be displayed below the **Result** section.
7. Click **Close** to close the **Diagnose SonicWave** page.

Managing Policies

The **Policies** page includes:

- **Policy Hierarchy**
- **SSID Policies**
- **Network Policies.**

NAME / SSID	BAND SELECTION	SECURITY	SSL-VPN	AUTHENTICATION	MAX CLIENT	VISIBILITY	ACTIVE
Default SSID Group							
Allen-Cloud-SF	2.4G 5G			WPA2AUTOPSK	32		
Allen-Cloud-SF-SSL	2.4G 5G			WPA2PSK	32		
Allen_test1							
SSID-221a							
SSID-224w							
xxx							
xxx							
xxxx							

On the Wireless Network Manager pages, Network Policies, Security Policies, and SSIDs are marked with different symbols, so they can be clearly distinguished from each other:

- **Network Policies** have a colored ball
- each type of **Security Policy** has its own square symbol
- **SSIDs** are labeled with a Wi-Fi symbol

The color of the symbol changes with its status:

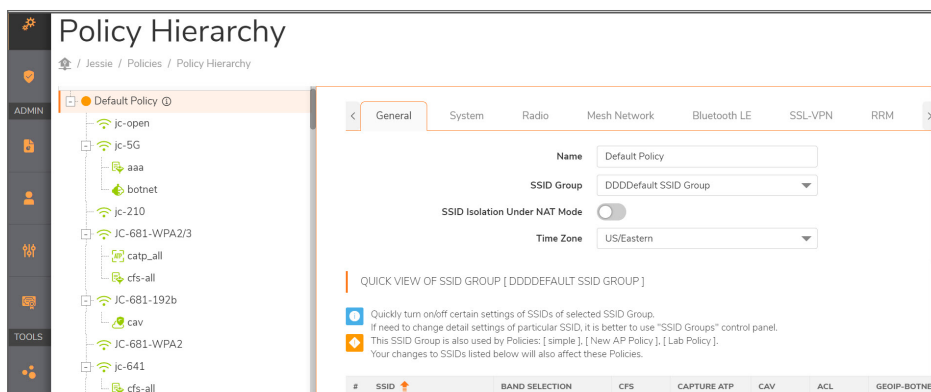
- The **Network Policy** ball is orange if it is in a default condition, or blue if it has been manually configured. When it is blue, it still retains its default settings, but in addition it has those that were manually set. Clicking on a **Network Policy** blue ball returns it to its default condition.
- The square **Security Policy** symbol can be green, fully enabled, orange, partially enabled, or gray, not enabled, as indicated by the screen tips when you hover over the symbol.

Topics:

- [Policy Hierarchy](#)
- [SSID Policies](#)
- [Network Policies](#)

Policy Hierarchy

The **Policy Hierarchy** page provides settings for monitoring, creating and managing the policies on your network. The middle pane gives an overview of your network policy structure, with the Tenant/Group at the top.



Topics:

- [Select a Network Policy](#)
- [Select an SSID](#)
- [Select a Security Policy](#)

Select a Network Policy

Selecting a Network Policy in the hierarchy structure brings up these information fields where changes can be made:

- [General](#)
- [System](#)
- [Radio](#)
- [Mesh Network](#)
- [Bluetooth LE](#)
- [SSL VPN](#)
- [RRM \(Radio Resource Management\)](#)
- [WIDP Support](#)
- [802.1X](#)

- Port Settings
- ALG
- SNMP

General

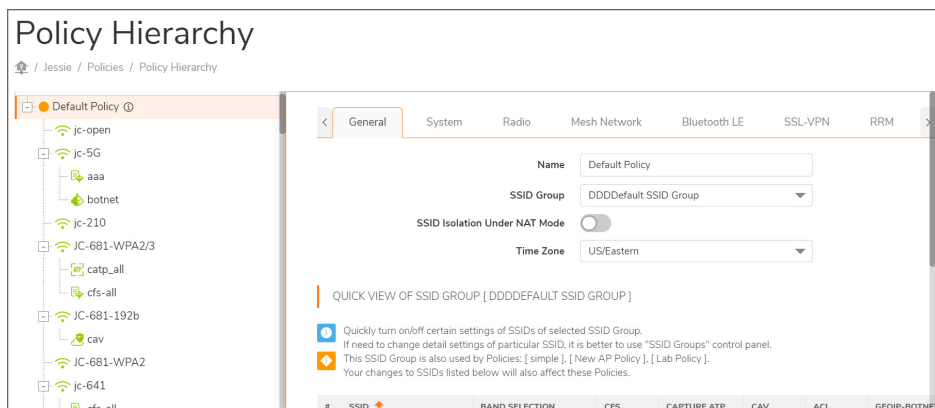
At the top of the screen is the **Name** of the policy and the **SSID Group** it applies to. **Default Policy**, at the top of the hierarchy, is the policy that is always in effect, no matter which other policies are applied for a particular **SSID**. It is an automatic attribute of the **Tenant/Group** through the access points used in the hierarchy, and it applies to the entire hierarchy.

Next is the choice to enable or disable **SSID Isolation Under NAT Mode**. This feature allows clients to be isolated even when they connect to the same SSID. It also isolates the clients between SSIDs.

The last field is for the **Time Zone**.

QUICK VIEW OF SSID GROUP - Gives a list of the SSID's in the group, with a table of configurations applied to them. These are explained below:

- **Band Selection** - You can change the band for the SSID.
- **CFS** - Content Filtering Service is a web filtering security service that blocks inappropriate, unproductive, and illegal or malicious web content according user specifications. The table shows if this service is active on the SSID or group of SSIDs.
- **Capture ATP** - Capture Advanced Threat Protection is a cloud-based feature that analyzes files and determines if the file is malicious or acceptable.
- **CAV** - Cloud AV is a security policy that provides real-time file-virus scanning and reporting without consuming local computing resources. A record of the analysis is kept for a selected period of time.
- **ACL** - Access Control is a policy that manages access to mac address objects and access object groups over time. It prevents unnecessary duplication when a similar or the same packet issue is detected.
- **Geo-IP & Botnet** - These two blocking features are shown or activated on this screen.
 - **Geo-IP** allows network administrators to block connections to or from a particular geographic location. It uses the IP address to determine the location of the intended connection.
 - A **Botnet** can be used to steal data, send spam, and allow an attacker to access a device and its connection. This feature is activated and configured by the administrator to block Botnet access to the network.
- **SSL VPN** - This selection enables or disables SSL VPN.
- **Authentication** - This column gives the authentication details for the SSID.
- **SSID** - This is a toggle to enable or disable visibility of the SSID.
- **Active** - This toggle activates or deactivates the SSID.
- **App Control** - This toggle activates or deactivates application control.

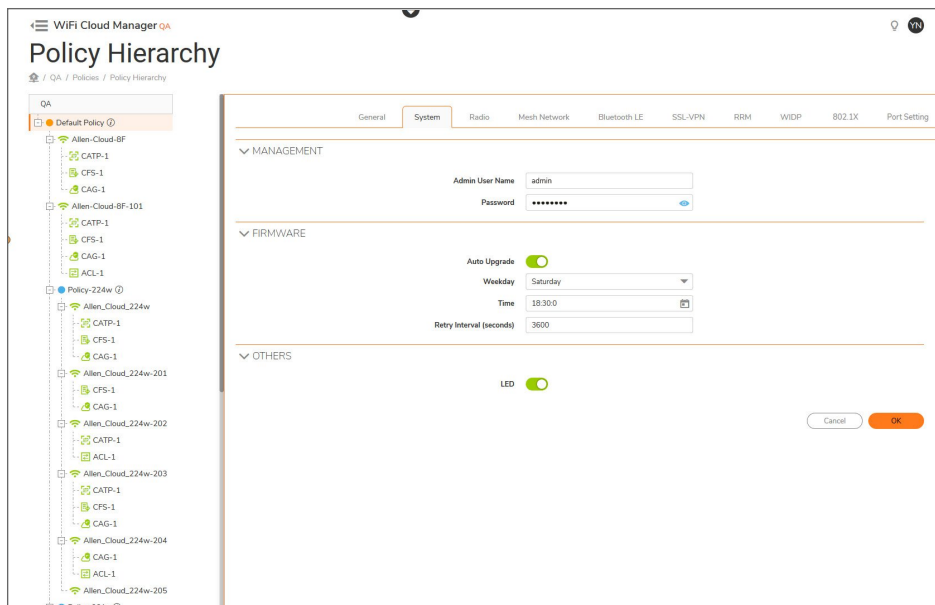


System

When you click **Policies > Policy Hierarchy > Select a network policy > System**, these panels appear on the right screen:

- **Management**, at the top, has an **Admin User Name** field and a **Password** field.
- **Firmware** has a toggle to **Auto Upgrade** the firmware, and time information for the upgrade.
- **Others** has a toggle to choose whether the **LED** is on or off.

Click **OK** to return to the **General** screen.



Radio

Radio gives toggled choices concerning **Short Guard Interval** and **Aggregation**, along with fields in which to enter information. You can enter:

- **Beacon Interval**
- **RTS Threshold**
- **Maximum Client**
- **Client Inactivity Timeout**
- **Wi-Fi Multimedia Profile**

Each of these is available for 2.4 GHZ and 5 GHZ.

The screenshot shows the 'Policy Hierarchy' interface in the WiFi Cloud Manager. On the left, a tree view shows the policy structure under 'QA', including 'Default Policy', 'Allen_Cloud_SF', 'Allen_Cloud_SF-101', 'Policy-224w', and 'Policy-231w'. The main panel displays the 'Radio' settings for two frequency bands: 2.4GHz and 5GHz. For each band, the following settings are visible: 'Short Guard Interval' (toggle), 'Aggregation' (toggle), 'Beacon Interval (ms)' (100), 'RTS Threshold (bytes)' (2346), 'Maximum Client' (32), 'Client Inactivity Timeout (seconds)' (300), 'RSSI' (toggle), and 'RSSI Threshold(dBm)' (-75). At the bottom right, there are 'Cancel' and 'OK' buttons.

On the **Radio** screen, there is a field for enabling or disabling RSSI, and for setting a threshold limit. in a high density Wi-Fi deployment, the user can set a desired RSSI Threshold on SonicWave by using this feature. When a SonicWave goes off to prevent a low RSSI client connection, the client device can navigate to a nearby access point and get a higher connection rate and quality.

Click **OK** to return to the **General** screen.

Mesh Network

Wireless Network Manager Mesh Network is a feature that gives extra flexibility to the communication between the access points and the router. With Mesh Network, the access point devices are in constant communication among themselves to monitor the traffic that is passing in and out of the system. This constant communication makes it possible for them to reroute packets along alternate paths dynamically, if there is an advantage to doing so.

- If **Mesh Radio** is enabled, the **Bluetooth LE advertisement** is enabled in access points for mobile APP connect.
- For the **Mesh Radio** bandwidth, you can choose:
 - **5 GHZ**
 - **2.4 GHZ**
 - **Disabled**

You can also choose the RSSI.

Click **OK** to return to the **General** screen.

Bluetooth LE

At **Policies > Policy Hierarchy > Select any network policy > Bluetooth LE**, you can choose whether **Advertisement** and **iBeacon** are enabled. There is also a field for filling in the **UUID** if **iBeacon** is enabled. If it is required, a valid UUID must be entered before you can exit this screen. If the **Advertisement** toggle is disabled, there are no other choices on this screen.

Click **OK** to return to the **General** screen.

SSL VPN

This feature provides supports for SSL-VPN connections to SonicWallSecure Mobile Access (SMA) appliances.

When the SonicWave is in standalone mode, the administrator can configure SSL-VPN settings from the web management interface. The SonicWave wireless access point will then launch a AvConnect client and control process to provide the secure tunnel for wireless client access.

Config SonicWave: 224w_f3c

General Radio **SSL-VPN** Port Setting

▽ SETTINGS

SSL-VPN ☐ ⓘ

▽ CERTIFICATE

Client Certificate ☐ Not Applied ⓘ

▽ OTHERS

Allow LAN2/LAN3/LAN4 SSL-VPN Security Tunnel Access ☐

Cancel OK

Topics:

- [Settings](#)
- [Certificate](#)
- [Others](#)

Settings

To activate the SSL-VPN options for a device:

1. Navigate to **Network > Devices**.
2. Hover over the right section for device you want to configure until the icons appear.
3. Click the **Configure** (pencil) icon.
4. Click the **SSL-VPN** tab.
5. In the **Settings** section, click the **SSL-VPN** slider to activate SSL-VPN support.
6. Enter the values for the options for **SSL-VPN** connection.
7. Click **OK**.

Certificate

You can specify which client certificate should be used for the policy.

To specify a client certificate:

1. Navigate to **Network > Devices**.
2. Hover over the right section for device you want to configure until the icons appear.
3. Click the **Configure** (pencil) icon.
4. Click the **SSL-VPN** tab.
5. In the **Certificate** section, from the Client Certificate list, select the certificate you want used for the policy.
6. Click **OK**.

Others

This section allows you to allow your LAN connections SSL-VPN security tunnel access.

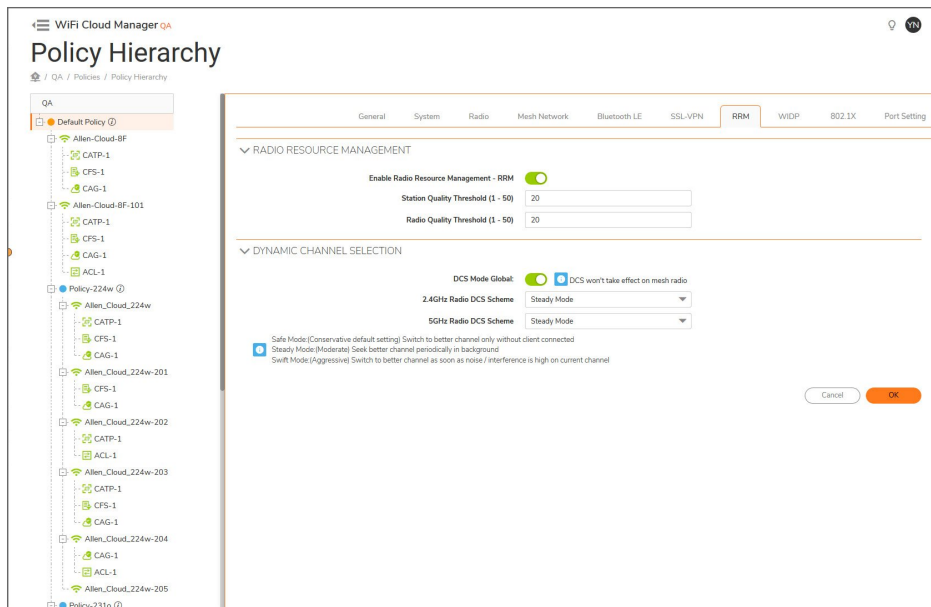
To allow SSL-VPN security tunnel access:

1. Navigate to **Network > Devices**.
2. Hover over the right section for device you want to configure until the icons appear.
3. Click the **Configure** (pencil) icon.
4. Click the **SSL-VPN** tab.
5. In the **Others** section, click the **Allow LAN2/LAN3/LAN4 SSL-VPN Security Tunnel Access** slider to allow SSL-VPN security tunnel access.
6. Click **OK**.

RRM (Radio Resource Management)

The RRM page contains these sections:

- **Radio Resource Management**
- **Dynamic Channel Selection**



Global DCS helps choose the proper channel for the SonicWave devices. Based on the DCS algorithm, the system uses RRM to take action dynamically, directing the client device to the AP that can give it the best signal. Global DCS is not available on SonicWave appliances that do not have a scan radio, such as the SonicWave 224w.

Radio Resource Management

To configure the Radio Resource Management options:

1. Navigate to **Policies > Policy Hierarchy > RRM**.
2. In the **Radio Resource Management** section, click the **Enable Radio Resource Management - RRM** slider to activate or deactivate RRM.
3. In the **Station Quality Threshold (1 - 50)** field, enter the threshold value for the station quality. The default value is 20.
4. In the **Radio Quality Threshold (1 - 50)** field, enter the threshold value for the radio quality. The default value is 20.

Dynamic Channel Selection

Wireless Network Manager supports Global DCS with RRM in the cloud.

To activate Dynamic Channel Selection:

1. Navigate to **Policies > Policy Hierarchy > RRM**.
2. In the **Dynamic Channel Selection** section, click the **DCS Mode Global** slider to activate or deactivate Dynamic Channel Selection.

To configure Dynamic Channel Selection:

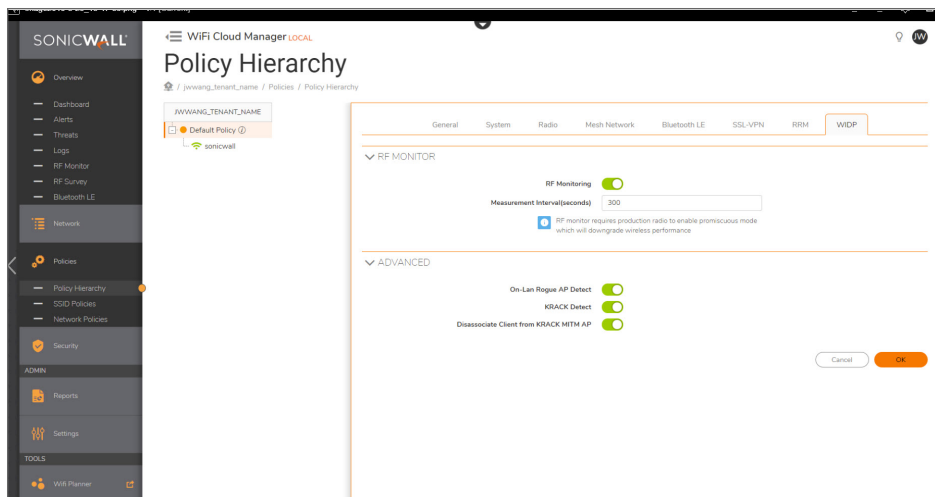
1. Navigate to **Policies > Policy Hierarchy > RRM**.
2. Locate the **Dynamic Channel Selection** section.
3. From the **2.4GHz Radio DCS Scheme** list, select the mode you want to use:
 - **Safe Mode:** This is a conservative mode that switches to a better channel, but only when no client devices are connected. This is the default setting.
 - **Steady Mode:** This is a moderate mode that checks periodically for a better channel in the background.
 - **Swift Mode:** This is a more aggressive mode that switches to better channel as soon as a high level of noise or interference is detected on the current channel.
4. From the **5 GHz Radio DCS Scheme** list, select the mode you want to use:
 - **Safe Mode:** This is a conservative mode that switches to a better channel, but only when no client devices are connected. This is the default setting.
 - **Steady Mode:** This is a moderate mode that checks periodically for a better channel in the background.
 - **Swift Mode:** This is a more aggressive mode that switches to better channel as soon as a high level of noise or interference is detected on the current channel.

WIDP Support

Wireless Network Manager supports Wireless Intrusion Detection and Prevention (WIDP). WIDP support provides:

- On-LAN AP detection
- Radio Frequency monitoring
- Detection and prevention of attacks from rogue access points. These are unregistered, unauthorized APs within the network.

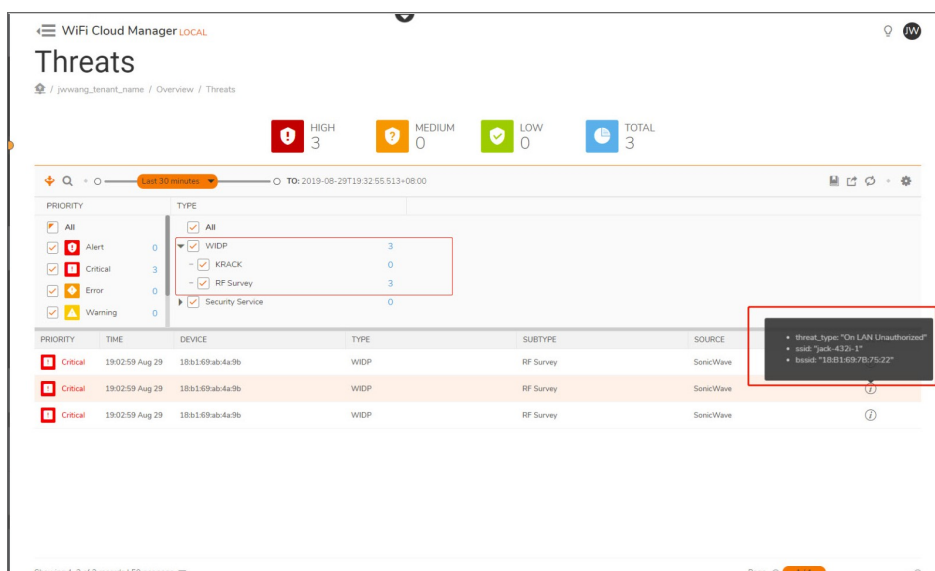
You can configure WIDP in the wireless cloud platform from the **Policies > Policy Hierarchy > WIDP** screen.



There are two sections on the screen, **RF Monitor** and **Advanced**. Click to activate specific functions for devices with this policy. Advanced functions only works for SonicWave access points with scan radio.

These screens show how the information from these features appear on the WCM management interface.

LAN ROGUE AP DETECTION AND ATTACK DETECTION AND PREVENTION



RF MONITOR

TIME	CLIENT	TYPE	SUBTYPE	VENDOR	RADIO TYPE	RSSI	RATE	ENCRYPT	DEVICE
17:16:49 Oct 22	90:61:AE:C6:6D:3A	Data Frame	Weak WEP IV	INTEL CORPORATE	802.11n	-31	54	None	2c:8b:bd:0e:93:c7
17:16:05 Oct 22	18:81:98:9C:AD:AD	Management Frame	Ad-Hoc Station Detection	SONICWALL	802.11n	-71	54	None	2c:8b:bd:0e:93:c7
17:16:04 Oct 22	18:81:98:9C:9C:FA	Management Frame	Null Probe Response	SONICWALL	802.11n	-58	1	None	2c:8b:bd:0e:93:c7
17:14:46 Oct 22	18:81:98:AB:33:54	General Frame	Long Duration	SONICWALL	802.11n	-91	54	None	18:81:98:ab:44:f7
17:08:28 Oct 22	98:97:DE:44:8A:8B	Management Frame	Ad-Hoc Station Detection	Unknown	802.11n	-47	1	None	18:81:98:ab:44:f7

802.1X

① | **NOTE:** 802.1X is currently only for SonicWave 224 models.

802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to permit or deny network connectivity based on the identity of the end user or device.

802.1X enables port-based access control using authentication. An 802.1X-enabled port can be dynamically enabled or disabled based on the identity of the user or device that connects to it.

802.1X uses these protocols:

- **Extensible Authentication Protocol (EAP):** The message format and framework defined by RFC 4187 that provides a way for the supplicant and the authenticator to negotiate an authentication method (the EAP method).
- **EAP method:** Defines the authentication method; that is, the credential type and how it is submitted from the supplicant to the authentication server using the EAP framework. Common EAP methods used in 802.1X networks are EAP-Transport Layer Security (EAP-TLS) and Protected EAP-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2).
- **EAP over LAN (EAPoL):** An encapsulation defined by 802.1X for the transport of the EAP from the supplicant to the switch over IEEE 802 networks. EAPoL is a Layer 2 protocol.
- **RADIUS:** The de facto standard for communication between the switch and the authentication server. The authenticator extracts the EAP payload from the Layer 2 EAPoL frame and encapsulates the payload inside a Layer 7 RADIUS packet.

To activate 802.1X support for a device:

1. Navigate to **Policies > Network Policies**.
2. Hover over the right section for device you want to configure until the icons appear.
3. Click the **Configure** (pencil) icon. The **Edit Policy: Default Policy** page displays.
4. Scroll to and click the **802.1X** tab.
5. Fill in the values needed for the **EAP Settings** and **RADIUS Server**, and **RADIUS Accounting Server**.
6. Click the **Port Setting** tab.
7. Select the device you want to configure.
8. In the **802.1X** column, activate the slider for the ports for which you want to use the 802.1X protocol.
9. Click **OK**.

ALG

Wireless Network Manager 4.3 support the SIP and H.323 VoIP protocols. These protocols are widely used by voice gateways, hardware terminals (such as IP phones), and software clients (like Netmeeting, Gnomemeeting and OpenPhone).

Wireless Network Manager supports these calling models:

- **Internal Endpoint Call External Endpoint Through Gatekeeper/SIP-Server:** The internal endpoint and the external endpoint are registered with a gatekeeper/SIP-server outside of the SonicWave wireless access points. The internal endpoint calls the external endpoint by calling its email address, user name or even a phone number.
- **External Endpoint Call Internal Endpoint Through Gatekeeper/SIP-Server:** The internal endpoint and the external endpoint are registered with a gatekeeper/SIP-server outside of the SonicWave wireless access points. The external endpoint calls the internal endpoint by calling its email address, user name or even a phone number.
- **Internal Endpoint Call Another Internal Endpoint Through Gatekeeper/SIP-Server:** The internal endpoint A and the internal endpoint B are registered with a gatekeeper/SIP-server outside of their SonicWave wireless access points. They call each other by calling the peer's email address, user name or even a phone number.

To activate a ALG protocol:

1. Navigate to **Policies > Network Policies**.
2. Hover over the right section for device you want to configure until the icons appear.
3. Click the **Configure** (pencil) icon. The **Edit Policy: Default Policy** page displays.
4. Scroll to the right and click the **ALG** tab.
5. Activate **H.323 Transformations** to use the H.323 protocol.
6. Activate **SIP Transformations**, **FTP NAT Transformation**, **TSFT NAT Transformation** to use the SIP

protocol.

7. Click **OK**.

Select an SSID

SSIDs are marked with the Wi-Fi symbol. They sometimes depend only on the Default Policy, and sometimes have other network policies applied to them. They can also have Security Policies applied, such as CFS-1 and ACL-1. Selecting an SSID in the middle pane of the **Policy > Policy Hierarchy** page brings up several options for configuring the SSIDs in your network.

Topics:

- [General](#)
- [Advanced](#)
- [Security Policies](#)
- [Guest Portal](#)

General

Selecting an SSID displays the **General** page with these sections:

- [Basic](#)
- [Authentication](#)
- [Others](#)

Some of the fields on this page are read-only, and some require information.

Basic

- **SSID Name** - This is populated with the name of the SSID you selected in the middle pane.
- **Active** - This toggle indicates whether the SSID is active or not.
- **AP Tags Availability** - From the AP Tags Availability list, select the tag(s) you want to apply to the SSID.
- **Schedule** - In this field, you can select a schedule for this SSID among those you have created, or you can leave it **Not Applied**.
- **Maximum Clients** - The maximum clients this SSID can service is usually fixed.
- **Clients Layer 2 Isolation** - Selecting this option adds Layer 2 Isolation.

Authentication

- **Authentication Type** - This field allows you to choose an authentication type for the SSID.
- **Cipher Type** - Auto is the only choice for the cipher type in this case.

- **Group Key Interval (seconds)** - Select this option for the Group Key Interval in seconds.
- **PMF Option** - The PMF option can be enabled, disabled, or required.
- **Strict rekey** - **Disabling the strict rekey process** can potentially help improve connectivity in environments with a lot of wireless interference.
- **Operate Channel Validation** - This option is enabled when you choose the authentication as WPA3.
- **PSK Type** - Choose Unique PSK, Multiple PSK, Multiple PSK with Radius using the radio button. When multiple PSK is selected, you need to add a client PSK setting. Click the + icon from **MULTIPLE PSK** to add client PSK global policy. From the **Client MAC Address Group** dropdown, choose the desired policy and enter the passphrase. Click **Add** to continue.

① | **NOTE:** To assign VLAN ID, you need to enable VLAN.

If you choose Multiple PSK with Radius, you need to input **EAP Setting** options like number of server tries, primary server retry interval (in minutes), NAS identifier, NAS IP Address.

For Radius server and Radius Accounting Server, Server IP address for the respective ports and server secret key has to be provided.

- **Passphrase** -A passphrase is required before you can complete any configuration changes.

Others

- **Hide SSID in Beacon** - This is an option for the activation/deactivation of visibility.
- **WDS Access Point** - This selection shows whether this access point is part of a WDS (Wireless Distribution System). A WDS is a method for extending the reach of a network of access points by making some of them dependent on others.
- **VLAN ID** - This item provides the id for the VLAN.

Dynamic VLAN Support

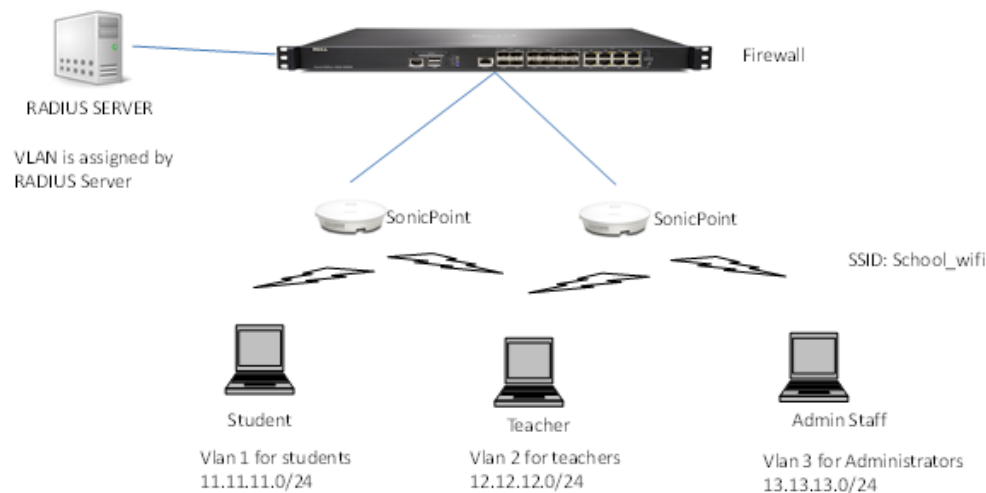
Dynamic VLAN support allows wireless clients to connect to access points using the same SSID (EAP) broadcasted by multiple SonicWave wireless access points. Wireless clients are assigned to different VLAN subnet by the RADIUS server according to their user groups and RADIUS server policy. Wireless clients do not need to connect to a specified SSID for their user group.

The RADIUS server assigns a VLAN ID to a user based on these attributes:

- IETF 64 (Tunnel Type): this is set to VLAN.
- IETF 65 (Tunnel Medium Type): this is set to 802.
- IETF 81 (Tunnel Private Group ID): this is set to VLAN ID.

In this example, only one SSID is broadcasted school-wide. Students, teachers, administration staff all connect to same SSID. The RADIUS server assigns them to different zones or subnets based on their login ID.

DYNAMIC VLAN EXAMPLE



To configure dynamic VLAN settings:

1. Navigate to the **Policies > SSID Policies** page.
2. Select an existing SSID or create a new one.

3. In the **Authentication** section, set the **Authentication Type** to one of the **WPA - EAP** authentication types.
① | **NOTE:** Dynamic VLAN SSIDs can only be configured when the authentication type is set to one of **WPA - EAP** authentication types.
4. In the **Others** section, set the VLAN ids. Toggle the button on or off to enable or disable Dynamic VLAN ID Assignment.

Advanced

All of the selections on the **Advanced** page can be toggled to enable and disable specific features.

Topics:

- [Band Selection](#)
- [IEEE802.11R](#)
- [IEEE 802.11K](#)
- [IEEE802.11V](#)
- [SSL-VPN Security Tunnel Access](#)
- [DNS](#)

Band Selection

- **2.4G Hz** - You can choose either band or both for this SSID.
- **5G Hz** - You can choose either band or both for this SSID.

▼ BAND SELECTION

2.4G Hz

☒

5G Hz

☒

IEEE802.11R

- **Enable IEEE 802.11r**

▼ IEEE 802.11R

Enable IEEE 802.11r

Enable FT over DS

Enable IEEE 802.11r Mix Mode

☒

☐

☒

IEEE 802.11K

- Enter Neighbor Report

▼ IEEE 802.11K

Enable Neighbor Report

☒

IEEE802.11V

- Enable BSS Transition Management
- Enable WNM Sleep Mode

▼ IEEE 802.11V

Enable BSS Transition Management

Enable WNM Sleep Mode

☐

☒

SSL-VPN Security Tunnel Access

- Allow SSL-VPN Security Tunnel Access

▼ SSL-VPN SECURITY TUNNEL ACCESS

Allow SSL-VPN Security Tunnel Access

☒

DNS

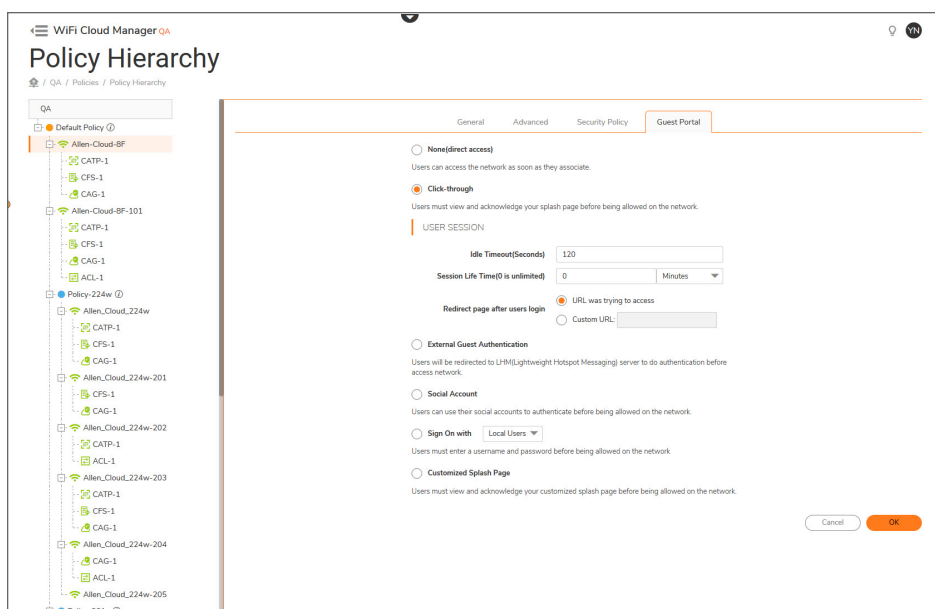
- Proxy Client DNS Request On Bridge Mode

Security Policies

The **Security Policies** tab allows you to select which security policies to apply to this SSID. Some of the security policies might have several versions, created to be applied separately to SSIDs or groups of SSIDs. All of the policies configured on your network are available for activation.

Guest Portal

From the **Guest Portal** page you can choose the type of authentication to require of users wanting to sign on to a session, and the details of the session. You can choose what type of access you will allow and which type of credentials must be presented. When you click in the box next to the access type, more access and user session options appear.



For this service, there is a customized screen for Cloud Captive Portal and Guest Services support. A captive portal is a web page (also called a splash screen) displayed before guests can access the Internet using a desktop or mobile device. Captive portals allow administrators to block Internet access until the guest has completed some defined process, such as looking at an acceptable use policy screen and clicking on a button indicating agreement to the terms of the policy.

If the guest user attempts to access any other pages before successful authentication has been completed, they will be redirected back to the authentication page.

Currently Wireless Network Manager supports the following six authentication methods, as seen on the screen above:

- **None (direct access)** - If this method is selected, there is no authentication.
- **Click-through** - The user must view and acknowledge your splash page.
- **External Guest Authentication** - The user is redirected for outside authentication.
- **Social Account** - The social account splash page is shown below:
- **Sign On with** - The user must enter a user name and password before being allowed on the network.
- **Customized Splash Page** - The user must view and acknowledge your customized splash page before being allowed on the network.



Click **OK** to apply your selections.

Sign-on Settings

Topics:

- [Sign-on with Local Users Authentication](#)
- [Sign-on with RADIUS Server Authentication](#)
- [Sign-on with LDAP Server Authentication](#)
- [Sign-on with Active Directory Server Authentication](#)
- [Sign-on with One-Time Passwords](#)
- [Sign-on with SAML Authentication](#)

Sign-on with One-Time Passwords

Customers must get their one-time password by email or SMS before being allowed to connect to the network.

To use One-Time Password authentication for sign-on:

1. Navigate to **SSID Policies**.
2. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
3. Click the **Guest Portal** tab.
4. Select **Sign On with**.
5. Select **One-time Password** from the list.

6. In the **One-Time Password** section, enter whether the one-time password should be delivered by **Email**, **SMS**, or both.

① **NOTE:** To use SMS to send one-time passwords, must **Configuring Twilio Billing for SMS** on the **General > Settings** page.

Configuring Twilio Billing for SMS

To configure Twilio billing for SMS:

1. Create a Twilio SMS account
 - a. Create a Twilio SMS account at www.twilio.com
 - b. Enter in credit card information to create an account with full privileges.
 - c. Purchase a phone number with Programmable SMS capabilities.
 - d. Record your Account SID and the Authentication Token values on your main twilio.com/user/account page.
2. Configure Twilio billing in Wireless Network Manager
 - a. Open the Wireless Network Manager Dashboard.
 - b. Navigate to the **Settings > General** page.
 - c. In the **Twilio SMS Setting** section, enter your:
 - **Twilio Account Sid**
 - **Auth Token**
 - **Twilio Phone Number**

You will now be billed on a per-SMS basis via Twilio. Prices can range by country; the typical cost per SMS ranges from \$0.01 per SMS for the United States to over \$0.10 per SMS for certain carriers in Europe. A complete, up-to-date pricing list is available at <https://www.twilio.com/sms/pricing#outbound-pricing>.

Sign-on with LDAP Server Authentication

To use LDAP server authentication for sign-on:

1. Navigate to **SSID Policies**.
2. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
3. Click the **Guest Portal** tab.
4. Select **Sign On with**.
5. Select the LDAP server you want to use for authentication.
6. In the **LDAP Server** section, configure the settings as required for your organization.

Sign-on with Active Directory Server Authentication

To use Active Directory server authentication for sign-on:

1. Navigate to **SSID Policies**.
2. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
3. Click the **Guest Portal** tab.
4. Select **Sign On with**.
5. Select the Active Directory server you want to use for authentication.
6. In the **Active Directory Server** section, configure the settings as required for your organization.

Sign-on with RADIUS Server Authentication

① | **NOTE:** Customers must sign in using their RADIUS username and password before being allowed to connect to the network.

After a user enters their username and password:

1. Those credentials will be passed to the SonicWave.
2. The SonicWave will create a RADIUS authentication packet and send it to the RADIUS server.
 - If the RADIUS server successfully authenticates the credentials: it replies with a `Access-Accept` packet to the SonicWave.
 - If the RADIUS server cannot authenticate the credentials: it replies with a `Access-Reject` packet to the SonicWave.

These RADIUS authentication methods are supported:

- PAP
- CHAP
- MSCHAPv1
- MSCHAPv2

The RADIUS server must be configured for at least one of those methods.

① | **NOTE:** MSCHAPv1 or MSCHAPv2 is recommended.

The SonicWave will first attempt to send the RADIUS packet using MSCHAPv2 and MSCHAPv1 authentication. If both of those authentication methods fail, it will then attempt to send the RADIUS packet using CHAP and PAP authentication.

To use RADIUS Directory server authentication for sign-on:

1. Navigate to **SSID Policies**.
2. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
3. Click the **Guest Portal** tab.

4. Select **Sign On with**.
5. Select the RADIUS Directory server you want to use for authentication.
6. In the **RADIUS Server** section, configure the settings as required for your organization.

Sign-on with SAML Authentication

When creating IDP application on SAML provider, following SSO URL and SP Entity ID needs to be provided.

Single Sign On URL: <https://auth.mysonicwave.com/lhmap/saml/?acs>

Audience URI (SP Entity ID): <https://auth.mysonicwave.com/lhmap/saml/metadata/>

To use SAML authentication for sign-on:

1. Navigate to **SSID Policies**.
2. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon. The **Edit SSID** page displays.
3. Click the **Guest Portal** tab.
4. From **Sign On with** dropdown, select **SAML**. Input the URL in Server ID and Authentication Service. Choose the certificate from the list.

SAML

Server ID (or Issuer URL)

https://app.onelogin.com/saml/metadata/c9742e:

Authentication Service (IdP SSO) URL

https://sonicwall2-dev.onelogin.com/trust/saml2'

IdP X.509 Public Certificate

aa

5. From **USER SESSION**, enter Idle Timeout (in seconds) and Session Life time (in minutes).
6. You can choose to redirect the users to a URL you were trying to access or to a custom URL.

USER SESSION

Idle Timeout(Seconds)

120

Session Life Time(0 is unlimited)

4

Minutes

Redirect page after users login

☐ URL were trying to access
 ☒ Custom URL:

www.sonicwall.com

Customized Splash Page

Enhancements to customizing the splash page include:

- [Use a Linked Image on the Customized Splash Page](#)
- [Collect User Feedback from a Customized Splash Page](#)

Use a Linked Image on the Customized Splash Page

You can now use a linked image instead of a static image on your customized splash page.

To use a linked image:

1. Navigate to the **Policies > SSID Policies** page.
2. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon.
3. Select the **Guest Portal** tab.
4. Select **Customized Splash Page**.
5. Click the **Customize Splash Page** (pencil) to the right.
6. Select the **Brand** tab.
7. From the **Poster File** list, select ****use url****.
8. In the field that appears below, enter the URL where the image is located.
9. Click the checkmark on the top right of the page to save your changes.
10. Click **OK** to save all of your changes.

Collect User Feedback from a Customized Splash Page

You can add a link on the login page that opens a new screen where users can provide their feedback and contact information.

To add a user feedback form:

1. Navigate to the **Policies > SSID Policies** page.
2. Hover over right section of the line of the SSID you want to configure. When the icons appear, click the **Edit** (pencil) icon.
3. Select the **Guest Portal** tab.
4. Select **Customized Splash Page**.
5. Click the **Customize Splash Page** (pencil) to the right.
6. Select the **Actions** tab.
7. Activate **Feedback Enabled**.
8. Click the checkmark on the top right of the page to save your changes.
9. Click **OK** to save all of your changes.

Select a Security Policy

Security Policies in the policy hierarchy are represented by their symbols. Each type of Security Policy has a different symbol, which carries through all the pages in Wireless Network Manager. When they are applied to an SSID, the symbol is green.

Clicking the **Security Policy** symbol in the policy hierarchy brings up a page with editable configuration selections the user can pick for that of type of policy.

The **Security Policy** pages provide you with the options to configure each type of security policy selected from the **Policy Hierarchy**. For more information, refer to **Security**.

Topics:

- **CFS (Content Filtering Service)**
- **CATP (Capture Advanced Threat Protection)**
- **CAV (Cloud Gateway Anti-Virus)**
- **ACL**
- **Geo-IP & Botnet**

CFS (Content Filtering Service)

Clicking a CFS policy in the middle pane brings up a screen with these parts:

- **General**
- **Category**
- **URI List**
- **Enabling or Disabling Reputation**

General

- **Name** - This is the name of the policy selected in the middle pane.
- **Enable** - This is a toggle for enabling or disabling this policy.
- **View Only** - This is a toggle for logging the occurrence of sites with the selected content, but still allowing them to pass through.

Category

This part of the page has a list of options for types of sites that can be blocked by this policy. Make your selection, or click **Select All** to block files in all the categories listed.

URI List

This section of the screen is for the creation of Whitelists and Blacklists.

- ## Enabling or Disabling Reputation

NOTE: This option will take effect only if the Category filtering is enabled.

✓

REPUTATION

Enable Reputation

i

Selected All

1. High Risk

2. Suspicious

3. Moderate Risk

4. Low Risk

5. Trustworthy

6. URL without Reputation

- General
- File Types
- Protocols
- MD5 Exclusion List

- **Name** - This is the name of the CATP policy you have selected.
- **Enable** - This toggle allows you to enable and disable this policy.

- **Block Until Verdict** - This toggle allows you to make a decision about uncertain files. If preprocessing decides that a file is uncertain, it is sent to CATP for further analysis. You can choose to take a chance on the uncertain file if you are confident that it is probably safe, or at least not too dangerous. If you prefer to wait for further analysis to confirm its safety, you can select **Block Until Verdict**.
 - **Max File Size (KB)** - the maximum size of files allowed to be downloaded.
- ① **NOTE:** For some SonicWave models, the maximum size will be reduced to 5120KB due to the memory limitations of those specific access points.

File Types

This part of the page has check boxes where you can pick which file types you want supported by CATP.

Protocols

This part of the page lists the protocols that can be selected for the CATP policy:

- HTTP
- SMTP

MD5 Exclusion List

This part of the page is available for creating lists for exclusion from blocking, or discarding lists that have been created.

CAV (Cloud Gateway Anti-Virus)

This selection is a **Cloud AV Security Policy** named CAV-1.

- [General](#)
- [File Types](#)
- [Protocols](#)
- [MD5 Exclusion List](#)

General

- **Name** - This is the name of the CAV policy you have selected.
 - **Enable** - This toggle allows you to enable and disable this policy.
 - **Block Until Verdict** - This toggle allows you to make a decision about uncertain files. If preprocessing decides that a file is uncertain, it is sent to CAV for further analysis. You can choose to take a chance on the uncertain file if you are confident that it is probably safe, or at least not too dangerous. If you prefer to wait for further analysis to confirm its safety, you can select **Block Until Verdict**.
 - **Max File Size (KB)** - the maximum size of files allowed to be downloaded.
- ① **NOTE:** For some SonicWave models, the maximum size will be reduced to 5120KB due to the memory limitations of those specific access points.

File Types

This part of the page has check boxes where you can pick which file types you want supported by CAV.

Protocols

This part of the page lists the protocols that can be selected for the CAV policy:

- HTTP
- SMTP

MD5 Exclusion List

This part of the page is available for creating lists for exclusion from blocking, or discarding lists that have been created.

ACL

This selection is an ACL policy that is configured on this network. This feature provides Virtual Access Point (VAP) Bandwidth Management control on SonicWave appliances under Wireless Network Manager.

The **ACL** page has these parts:

- [General](#)
- [Authentication/Association MAC Filtering](#)
- [ACL](#)
- [Bandwidth Management](#)

General

- **Name** - This is the name of the ACL policy selected.
- **Enable** - This policy can be enabled or disabled.

Authentication/Association MAC Filtering

- **Action** - The mode can be either Allow, Deny, or Disabled.
- **Client MAC Address Group** - The name of the address group.
- **Destination** -
- **Service** -
- **Log** -

ACL

Wireless Network Manager provides support for Layer 2 (L2), Layer 3 (L3), and Layer 4 (L4) access control list (ACL) support for SonicWave access points.

- **Action** - The mode can be either Allow, Deny, or Disabled.
- **Client MAC Address Group** - The name of the address group.

Bandwidth Management

- **Enable** - You can select to enable or disable bandwidth management.
- **Direction** - Choose one of these:
 - **Both directions**
 - **Client to AP**
 - **AP to Client**
- **Down Min/Max Rate (kbps)** - Downstream minimum and maximum rates.
- **Up Min/Max Rate (kbps)** - Upstream minimum and maximum rates.
- **All Clients** - This is a toggle to enable or disable all clients. If you want to apply this configuration to all clients, select **All Clients**. If you want to apply it only to an restricted IP group, toggle **All Clients** off, and set the **Client IP Group** in the field that appears below the **All Clients** field.
- **Client IP Group** - Select the **IP Group** to which these selections apply. This field is only available when **All Clients** is off.

Geo-IP & Botnet

For information about configuring these security policies, refer to [Security](#).

APP Control

To create a new application control policy:

1. Navigate to **Security > Security Policies**.
2. On the **Access Points** tab, click Add (+). The **Add New Security Policy** dialog displays.
3. In the **Name** field, enter a name for your new security policy.
4. From the **Type** list, select **APP Control Security Policy**.
5. Click **Next**.
6. In the **General** section, select **Enable** to activate the new policy.
7. In the **App Rules** section, click Add (+) to associate security rules with the policy.
8. Click **OK**.

The new policy is now displayed in the list of available security policies.

SSID Policies

The **Policies > SSID Policies** page is used for creating and managing SSID policies. The table of SSIDs and SSID groups has fields for **Name** (of group)/**SSID**, **Band Selection**, and **Security**, which shows which security policies are applied to the SSID or to the group.

The next columns are:

- **SSL VPN**
- **Authentication**
- **Max Clients**
- **Visibility**
- **Active**

These settings apply only to the individual SSIDs.

Hovering over the:

- items in the **Security** column of this screen brings up details about the security policy indicated for this SSID or this group.
- row brings up options to:
 - **Edit** and **Delete** for individual SSIDs
 - **Edit**, **Add**, **Copy**, and **Delete** for SSID groups

Topics:

- [Adding SSID Security Policies](#)
- [Editing SSID Security Policies](#)

Adding SSID Security Policies

Click on the **+ Add** on an SSID group row to bring up this **Add SSID** screen. These are the same fields you consulted or configured in the [Select an SSID](#) section from the central pane of the **Policy > Policy Hierarchy** screen. These fields are applied to the new SSID you are adding.

General - For RADIUS Accounting Support, go to **Policies > SSID Policies > Add** (in the SSID row) > **General > Authentication Type WPA2 - EAP**. The page allows you to configure RADIUS accounting support on the new SSID for this authentication type.

RADIUS SERVER

Server 1 IP

Server 1 Port

Server 1 Secret

Server 2 IP

Server 2 Port

Server 2 Secret

RADIUS CoA Support ☐ ⓘ

RADIUS ACCOUNTING SERVER

Server 1 IP

Server 1 Port

Server 1 Secret

Server 2 IP

Server 2 Port

Server 2 Secret

Click **RADIUS CoA Support** if you want to enable the connected devices to act as a RADIUS dynamic authorization server and respond to RADIUS Change of Authorization (CoA) and disconnect messages sent by the RADIUS server.

Editing SSID Security Policies

Click on **Edit/Config** on an SSID row to display the **Edit SSID** screen. These are the same fields you consulted or configured in the **Select an SSID** section from the central pane of the **Policy > Policy Hierarchy** screen. Now these fields are applied to a new SSID you have selected from the **SSID Policy** screen.

- **PMF - Policies > SSID Policies > Edit** (in an SSID row) > **General / Authentication** provides an approved amendment to the IEEE 802.11 standard to protect wireless management frames, the IEEE 802.11W-2009. It is also known as the Protected Management Frames (PMF) standard. The chosen SSID can be edited so the PMF option is:
 - **Disabled**
 - **Enabled**
 - **Required**
- **WDS** - The bottom of the screen has a toggle to select whether this access point is part of a Wireless Distribution System (WDS). A WDS is a group of access points associated together in such a way as to

expand the range of the signal availability.

Edit SSID for Default SSID Group

General

Advanced

Security Policy

Guest Portal

▼ BASIC

SSID Name

Allen-Cloud-8F

Active

☒

Schedule

schedule_1_working_days_hours

Maximum Clients

32

Clients Layer 2 Isolation

☐

▼ AUTHENTICATION

Authentication Type

WPA2 - AUTO - PSK

Cipher Type

AUTO

Group Key Interval (seconds)

86400

PMF Option

Disabled

Passphrase

✓ Disabled

Enabled

Required

▼ OTHERS

Visible in Beacon

☒

WDS Access Point

☐

VLAN ID

0

Vlan Id will be used only in bridge mode.

Cancel

OK

The **Edit SSID** page can also be used to configure the RADIUS Accounting Server. This configuration option is available on the **Policies > SSID Policies > Edit/Config > SSID Edit** screen.

Network Policies

The options on the **Network Policies** page are used to create and manage network policies. When you click **Add** + on the top right, or **Edit/Config** in a policy row, you see pages with the same information fields for consulting or configuring as those discussed in [Select a Network Policy](#).

Using Tags to Manage Access Points and SSIDs

By default, all access points in a network broadcast all of their enabled SSIDs simultaneously. While this is desired for most deployment situations, there may be cases where specific SSIDs should only be broadcast from a specific access point or group of access points. Tags can be used to partition your wireless network into both physical- or security-based segments, and for basic management purposes.

Topics:

- [Using Tags to Manage Access Points](#)
- [Using Tags to Manage SSIDs](#)

Using Tags to Manage Access Points

Tags can be used to partition your wireless network into both physical- or security-based segments, and for basic management purposes.

Topics:

- [Adding Tags to an Access Point](#)
- [Removing Tags Associated with an Access Point](#)
- [Viewing Tags Associated with an Access Point](#)

Adding Tags to an Access Point

To add a tag to an access point:

1. Navigate to **Network > Devices**.
2. On the right of the access point for which you want to add a tag, click the **Edit** icon.
3. Click the **General** tab.
4. Next to **Device Tags**, click the plus icon (+). the **Add Device Tag** dialog displays.
5. In the **Device Tag** field, enter the name for the tag you want to create.

6. Click **OK** to save the tag.
7. Click **OK** to save the configuration changes for the access point.

Removing Tags Associated with an Access Point

To remove a tag associated with an access point:

1. Navigate to **Network > Devices**.
2. On the right of the access point for which you want to delete a tag, click the **Edit** icon.
3. Click the **General** tab.
4. Next to **Device Tags**, click the (X next to the tag you want to delete.
5. Click **OK**.

Viewing Tags Associated with an Access Point

To view the tags associated with an access point:

1. Navigate to **Network > Devices**.
2. On the right of the access point to which you want to view the associated tags, hover over the **Tag** icon. The tags associated with the access point will display in a small popup window.

Using Tags to Manage SSIDs

By default, all access points in a network broadcast all of their enabled SSIDs simultaneously. While this is desired for most deployment situations, there may be cases where specific SSIDs should only be broadcast from a specific access point or group of access points. Tags can be used to partition your wireless network into both physical- or security-based segments, and for basic management purposes.

Topics:

- [Adding Tags to an SSID Group](#)
- [Removing Tags from an SSID Group](#)
- [Viewing Tags Associated with an SSID Group](#)

Adding Tags to an SSID Group

To add a tag to an SSID group:

1. Navigate to **Policies > SSID Policies**.
2. On the right of the SSID to which you want to add a tag, click the **Edit** icon.

3. From the **AP Tags Availability** list, select the tag(s) you want to apply to the SSID.
4. Click **OK**.

Removing Tags from an SSID Group

To remove a tag from an SSID group:

1. Navigate to **Policies > SSID Policies**.
2. On the right of the SSID to which you want to remove a tag, click the **Edit** icon.
3. From the **AP Tags Availability** list, click the **(X)** next to the tag you want to delete.
4. Click **OK**.

Viewing Tags Associated with an SSID Group

To view the tags associated with an SSID group:

1. Navigate to **Policies > SSID Policies**.
2. On the right of the SSID to which you want to view the associated tags, hover over the **Tag** icon. The tags associated with the SSID group will display in a small popup window.

Wi-Fi Multimedia (WMM) Profiles

Wireless Network Manager allows you to create and manage Wi-Fi Multimedia (WMM) profiles and assign them to specific SonicWave access points.

Topics:

- [Creating Wi-Fi Multimedia \(WMM\) Policies](#)
- [Enabling Wi-Fi Multimedia \(WMM\) Policies](#)

Creating Wi-Fi Multimedia (WMM) Policies

To create an WMM profile:

1. Navigate to **Policies > WMM Profiles**.
2. Click the plus icon (+) at the far right of the table. The **Add WMM Profile** dialog displays.
3. In the **Name** field, enter a name for the profile.
4. In the **Description** field, enter a short description for the profile. (This is optional.)

5. In the fields provided, enter the values required for your WMM profile.
6. Click **OK**.

Enabling Wi-Fi Multimedia (WMM) Policies

To enable an WMM profile for an access point:

1. Navigate to **Network > Devices**.
2. On the right of the access point for which you want to enable a WMM profile, click the **Edit** icon.
3. Click the **Radio** tab.
4. From the **WMM Profile** list, select the WMM profile you want applied to the access point.
5. Click **OK**.

Managing Switch Policies

Topics:

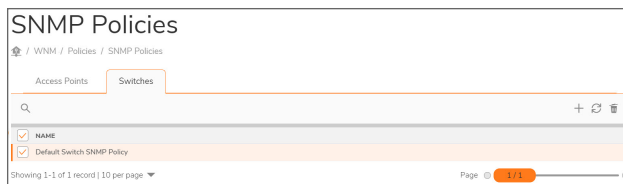
- [Adding Switch Policies](#)
- [Editing Switch Policies](#)

For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on the SonicWallSonicWall support website at: <https://www.sonicwall.com/support/technical-documentation/>.

Adding Switch Policies

To add a Switch policy:

1. Navigate to **Policies > SNMP Policies**.
2. Go to **Switches**.
3. Click the Add (+) icon to create a policy. The **Switch Config** page displays.



4. Set the options for the new policy.

- ① | **NOTE:** You only need to set the options where you want them to be different from the **Default Switch Policy**. If you want the change to affect all Switches, edit the **Default Switch Policy** instead of creating a new Switch policy.

5. Click **OK**.

For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on the SonicWall support website at: <https://www.sonicwall.com/support/technical-documentation/>.

Editing Switch Policies

To edit a Switch policy:

1. Navigate to **Policies > Switch Policies**.
2. Click the **Edit** (pencil) icon to edit an existing policy. The **Switch Config** page displays.
① | **NOTE:** To change the policy options for all of the Switches, edit the **Default Switch Policy**.
3. Update the options for the existing policy.
4. Click **OK**.

For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on the SonicWall support website at: <https://www.sonicwall.com/support/technical-documentation/>.

Managing SNMP Policies

Wireless Network Manager provides support for SNMP v3 for SonicWave devices.

Topics:

- [Setting the SNMP ID](#)
- [Adding SNMP Policies](#)
- [Editing SNMP Policies](#)
- [Deleting SNMP Policies](#)
- [Setting SNMP Policies](#)

Setting the SNMP ID

Each SNMP agent maintains local information to be used in SNMP v3 message exchanges so that the agent receives incoming messages and sends Trap messages to a manager.

- ① | **IMPORTANT:** The **SNMP Engine ID** must be defined before SNMP v3 can be enabled.

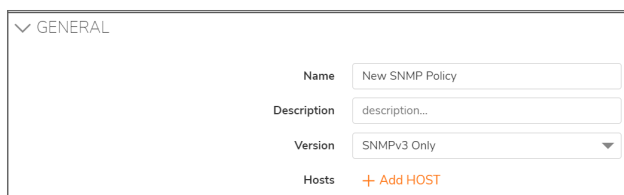
To set the SNMP ID:

1. Navigate to **Network > Devices**.
2. On the far right of the line in the list for the device you want to configure, click the **Edit (pencil)** icon.
3. Click the **General** tab.
4. In the **System** section, in the **SNMP Engine ID** field, enter the SNMP engine ID.
5. Click **OK**.

Adding SNMP Policies

To add an SNMP policy:

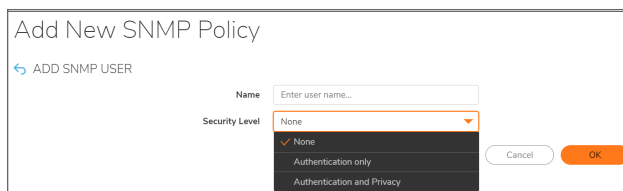
1. Navigate to **Policies > SNMP Policies**.
2. Click the **Add Policy** icon (+) at the top left of the table. The **Add New SNMP Policy** dialog displays.
3. In the **General** section:
 - a. In the **Name** field, enter a name for the policy.
 - b. In the **Description** field, enter a brief description for the policy. (This field is optional.)
 - c. From the **Version** list, select the SNMP version to which the policy should apply.



The screenshot shows the 'Add New SNMP Policy' dialog with the 'GENERAL' tab selected. It contains the following fields and controls:

- Name:** A text input field with the value 'New SNMP Policy'.
- Description:** A text input field with the placeholder text 'description...'.
- Version:** A dropdown menu currently showing 'SNMPv3 Only'.
- Hosts:** A section with a '+ Add HOST' button.

- d. Add Hosts by clicking **+ Add HOST**.
4. In the **User** section:
 - a. Click the **Add User** icon (+) at the top left of the table. The **Add SNMP User** dialog displays.
 - b. In the **Name** field, enter the name for the user.
 - c. From the **Security Level** list, list the security level you want applied to the user:
 - **None**
 - **Authentication only**
 - **Authentication and Privacy**



The screenshot shows the 'Add New SNMP Policy' dialog with the 'User' section selected. It contains the following fields and controls:

- ADD SNMP USER:** A button with a plus icon.
- Name:** A text input field with the placeholder text 'Enter user name...'.
- Security Level:** A dropdown menu with a list of options: 'None' (selected), 'Authentication only', and 'Authentication and Privacy'.
- Buttons:** 'Cancel' and 'OK' buttons.

- d. From the **Authentication Method** list, select authentication method you want used.
 - e. In the **Authentication Key** field, enter the authentication key.
 - f. From the **Encryption Method** list, select encryption method you want used. (**Authentication and Privacy** only)
 - g. In the **Encryption Key** field, enter the encryption key. (**Authentication and Privacy** only)
 - h. Click **OK**.
5. Click **OK** to add policy.

Editing SNMP Policies

To edit an SNMP policy:

1. Navigate to **Policies > SNMP Policies**.
2. Click the **Edit** icon (pencil) on far right of the line in the table where the policy is listed. The **Edit SNMP Policy** dialog displays.
3. Make any changes needed to the fields. (Refer to [Adding SNMP Policies](#) for more information about each of the fields.)
4. Click **OK**.

Deleting SNMP Policies

To edit an SNMP policy:

1. Navigate to **Policies > SNMP Policies**.
2. Click the **Delete** icon (trashcan) on far right of the line in the table where the policy is listed. A confirmation dialog displays.
3. Click **OK**.

Setting SNMP Policies

To set an SNMP policy:

1. Navigate to **Policies > AP Policies**.
2. Create a new policy or edit an existing one.
3. The **Add Policy** or **Edit Policy** dialog displays.
4. Click **SNMP**.
5. From the **SNMP Policy** list, select the SNMP policy you want to apply for the device.

For information on creating SNMP policies, refer to [Adding SNMP Policies](#).

Managing Switch SNMP Policies

Wireless Network Manager provides support for Switch SNMP for SonicWave devices.

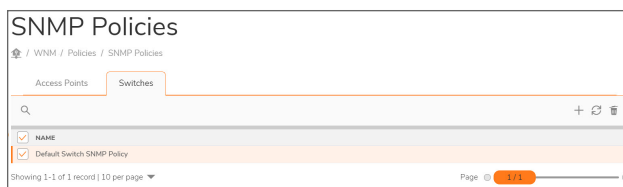
Topics:

- [Adding Switch SNMP Policies](#)
- [Editing Switch SNMP Policies](#)

Adding Switch SNMP Policies

To add a Switch policy:

1. Navigate to **Policies > SNMP Policies**.
2. Go to **Switches** tab.
3. Click the Add (+) icon to create a policy. The **Switch SNMP Policy** page displays.



4. Enter the **Switch Policy Name**.
5. Create a new user name in the User Management tab by clicking **+ Create User Account**.
6. Enter details in the **Firmware** tab.
7. In the **SNTP** tab, enter the SNTP Server, Port and Timezone.
8. In **Management VLAN** section, enter the **VLAN ID** and choose the configuration option from the dropdown list.
9. Click **OK**.

- ① | **NOTE:** You only need to set the options where you want them to be different from the **Default Switch Policy**. If you want the change to affect all Switches, edit the **Default Switch Policy** instead of creating a new Switch policy

For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on the SonicWall support website at: <https://www.sonicwall.com/support/technical-documentation/>.

Editing Switch SNMP Policies

To edit a Switch SNMP policy:

1. Navigate to **Policies > Switch Policies**.
2. Click the **Edit** (pencil) icon to edit an existing policy. The **Switch Config** page displays.
① | **NOTE:** To change the policy options for all of the Switches, edit the **Default Switch Policy**.
3. Update the options for the existing policy.
4. Click **OK**.

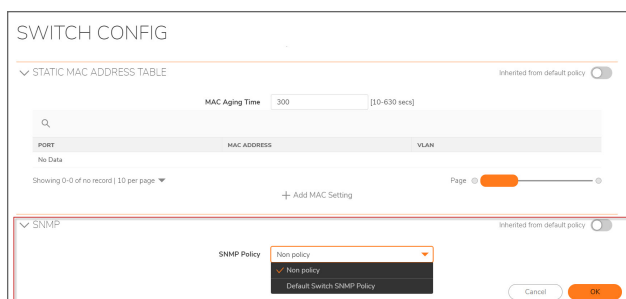
For more information on configuring and using the SonicWall Switch, refer to the *Switch Administration Guide*. This and other documentation are available under the product name “Switch” on the SonicWall support website at: <https://www.sonicwall.com/support/technical-documentation/>.

Applying Switch SNMP Policies

Once you have created a Switch SNMP policy, you can apply the object you created. This information applies to any security policy you create.

To apply SNMP Switch Policies:

1. Navigate to **Policies > Switch Policies**.
2. Open an existing switch policy or create a new policy.
3. Go to **System** tab and scroll down to **SNMP** section.
4. Choose the policy from the dropdown list.



The screenshot shows the 'SWITCH CONFIG' page. The 'STATIC MAC ADDRESS TABLE' section is expanded, showing a table with columns for PORT, MAC ADDRESS, and VLAN. Below the table, there is a search bar and a 'MAC Aging Time' field set to 300. The 'SNMP' section is also expanded, showing a dropdown menu for 'SNMP Policy' with options: 'Non policy', 'Non policy', and 'Default Switch SNMP Policy'. The 'Default Switch SNMP Policy' is selected. There are 'Cancel' and 'OK' buttons at the bottom right of the SNMP section.

5. Click **OK**.

Disabling the Strict Rekey

When there is a lot of wireless interference, the connection to SonicWave can encounter performance issues. Disabling the strict rekey process can potentially help improve connectivity in those environments.

To disable the strict rekey:

1. Navigate to **Policies > Policy Hierarchy**.
2. Select a device.
3. Select the **General** tab.
4. In the **Authentication** section, click **Strict Rekey** to the off position.

① | **NOTE:** The **Strict Rekey** option is only available for WPA-PSK and WPA-EAP settings.

① | **IMPORTANT:** While disabling **Strict Rekey** can improve connectivity when there is significant wireless interference, it provides a less secure connection.

Security

Topics:

- [Security Policies](#)
- [Address Objects](#)
- [Schedule Objects](#)
- [App Objects](#)

Security Policies

The **Security Policies** page displays all of the security policies that have been configured on your network and provides options for managing, adding, and editing security policies. These policies add extra layers of security beyond that available from [Network Policies](#). Hovering over the right end of each row enables:

- **Edit/Config**
- **Copy**
- **Delete**

The columns display the following information:

- **Name** - is the distinct name that was given to the policy by the administrator when it was created or last edited. If desired, it can include information about what type of policy it is.
- **Applied SSID Group** - is the group of SSIDs to which the policy is applied.
- **Type** - gives the symbol of the security policy in the appropriate color (green for on, red for off). Hovering over the security policy symbol gives a screen tip saying which type of policy it is and whether or not it is enabled.
- **Active** - toggles on and off for this security policy.
- **Schedule** - shows the applied scheduled policy.

Only licensed security policies can be applied to an SSID or SSID group managed in your Wireless Network Manager network. If you try to apply a policy that is not licensed, a screen tip appears indicating that this policy needs to be licensed.

Wireless Network Manager advanced security services include these policies:

- [Content Filtering Service](#)
- [Capture Advanced Threat Protection](#)
- [Cloud Anti-Virus](#)
- [Access Control Policies](#)
- [Geo-IP & Botnet](#)
- [Application Control](#)

Content Filtering Service

The Wireless Network Manager Content Filtering Service (CFS) is a web-filtering service that blocks inappropriate, unproductive, and illegal or malicious web content according to your specifications. CFS inspects web page traffic based on HTTP and HTTPS protocols, and blocks or logs websites based on pre-configured blacklists and whitelists. CFS includes tools for creating and applying policies that allow or deny access to sites based on individual or group identity, time of day, and over 90 other categories you pre-select. This feature is based on SonicWave Virtual Access Point (Virtual SSID) architecture. All user configuration is VAP (Virtual Access Point)-based.

Topics:

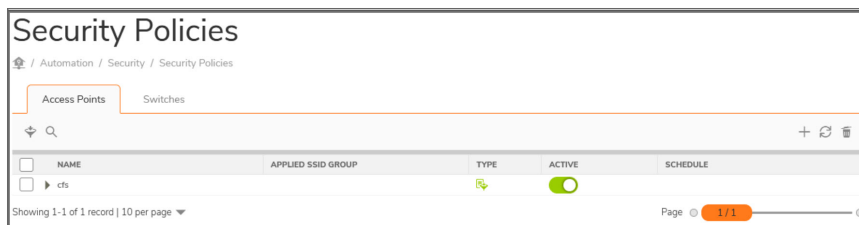
- [Creating Content Filtering Service Security Policies](#)
- [Editing Content Filtering Service Categories](#)
- [Adding Sites to the Whitelists and Blacklists](#)

Creating Content Filtering Service Security Policies

You can create CFS security policies and select which categories you want them to block.

To create a CFS security policy:

1. Navigate to **Security > Security Policies**.
2. Click **Add +**. The **Add New Security Policy** page displays.



3. In the **Name** field, enter a name for the policy.
4. In the **Type** field, select **CFS Security Policy** from the drop down list.
5. Click **Next**. The **Add New Security Policy** screen displays.

Add New Security Policy

Name:

Type: CFS Security Policy

Cancel OK

6. Toggle **Enable** to enable the CFS policy you are creating. From the dropdown list, choose the **Schedule**.

GENERAL

Enable: ☒

Schedule: Not Applied

View Only: ☐

Monitor All Web Accesses: ☐

Block On Rating Failure: ☐

7. Click **View Only** if you want CFS to log website access instead of blocking the websites.
8. Select **CFS Categories** based on your requirements. To select all the categories, click **Select All**.
9. When you click **OK**, the CFS policy is enabled and listed on the **Security > Security Policies** page according to the criteria you have chosen.

Editing Content Filtering Service Categories

The CFS categories that provide customization options for blocking specific types of websites can be changed at any time.

To edit Content Filtering Service categories:

1. Navigate to **Security > Security Policies**.

Security Policies

sonicwall Products / Security / Security Policies

Access Points Switches

NAME	APPLIED SSID GROUP	TYPE	ACTIVE	SCHEDULE	
CFS2_mixed	231o_Group, 400 Group, test_add_new_group		☒	mixed_new	Edit + ↺ 🗑️
CFS3	231o_Group, 400 Group		☒		Edit + ↺ 🗑️

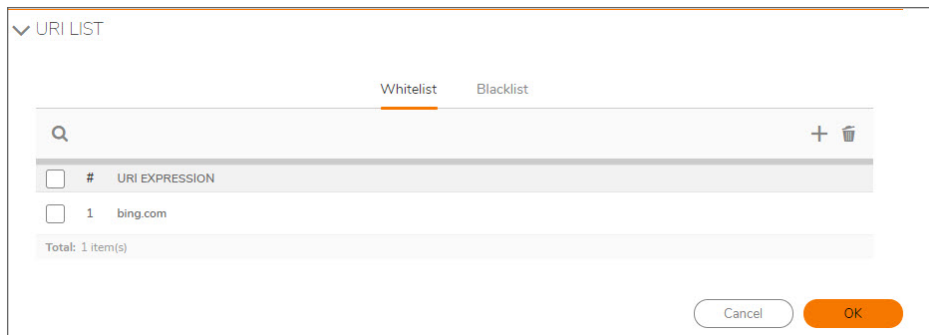
2. Click **Edit/Config** next to the policy you want to change. The **Edit Security Policy** page displays.
3. Click **Select All** to select all Content Filtering Service categories, or choose specific categories to block specific types of websites.
4. Click **Submit** to apply the Content Filtering Service policy.

Enabling or Disabling Reputation

You can enable or disable this section by toggling the button to on or off.

NOTE: This option will take effect only if the Category filtering is enabled.

Select individual options by using the checkbox or select all of the options by clicking **Selected all**.



5. A site can be removed from a list by clicking **Delete** before clicking **OK**.

Customizing Blockpage

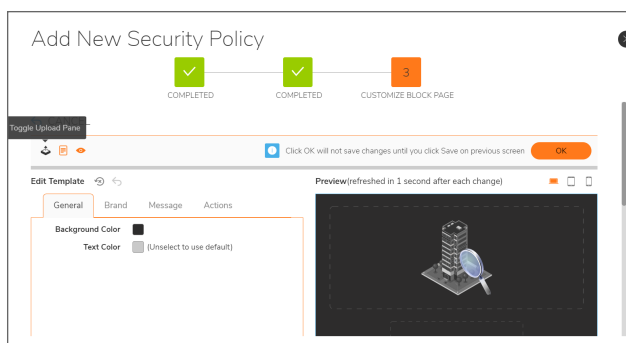
You can fully customize the web page that is displayed to the user when access to a blocked site is attempted.

The customized block message can be done when you are creating CFS, CATP, Cloud AV security policies. You can also edit the existing policies by clicking **Edit** icon and apply the customized blockpage to the selected policies.

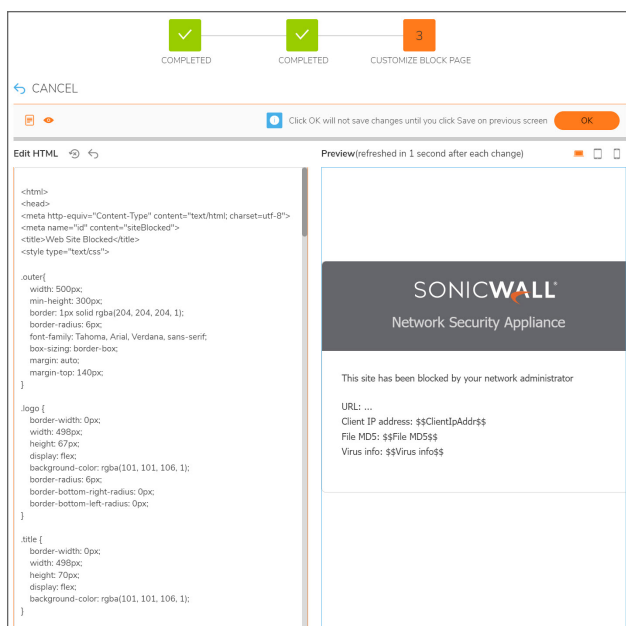
To customize a blockpage:

1. Navigate to **Security > Security Policies**.
2. Click Add **+**. The Add New Security Policy page displays.
3. Enter a name and choose the type of Policy and click **Next**.
4. In the Advanced page, choose the options and click **Next**.
5. In Customize Block Page, choose the options using the radio buttons.
 - **None** - When selected, the customize blockpage will be disabled. This is the default option.
 - **Using URL** - Choose this option if you would like to redirect to a specific URL. Enter the URL in **Input URL** text box.
 - **Using Template** - You can customize a template and show a personalized blockpage. Click the Edit icon and choose the template and error message to be displayed. A preview is displayed on the right view instantly for you to view the message and make changes.

You can also upload a picture by clicking **Toggle Upload Pane** and choose an image.



- **Using HTML** - You can customize the block page by HTML. Click the edit icon and edit the HTML.



6. It is important to save the changes before proceeding to the next screen. Click **Save**.

Applying a Security Policy to an SSID Group

Once you have created a Security Policy, such as a CFS or CATP policy, you can apply it to an SSID Group. This information applies to any security policy you create.

To apply a security policy to an SSID group:

1. Navigate to **Policies > SSID Policies**. A page displays that lists all of your SSID groups and the security policies applied to them.
2. Click **+ Add** at the top right to bring up the **Add SSID Group** page. This gives you the choice to create a new SSID group to which you can apply this policy.

3. Add an **SSID Group Name** and click **OK**. You have created an SSID Group to which you can apply the policy. It can be seen on the **SSID Policies** screen.
4. Click **+ Add** on the right side of the screen in the row for your SSID Group. The **Add SSID** screen displays. The name of the SSID you are adding appears in the title line of the page.
5. Click the **General > Basic**.
6. Enter the **SSID Name** you created.
7. Authenticate with your passphrase.
8. Click the **Security Policy** tab.
9. From the drop down list, select the type of policy you want to apply.
10. Click **OK**.
11. On the **SSID Policies** screen, click to expand the SSID Group you created and show your SSID.
12. The **Security** column shows that the security policy is applied.
13. If you want to edit the SSID Group to have a different policy applied, click **Config/Edit** at the end of the row to go to the Edit SSID, with the name of the group in the title line.
14. Click **Security Policy** and select the policy to be applied.
15. Click **OK**, to see in the **Security** column that the correct policy has been applied.

Capture Advanced Threat Protection

Capture Advanced Threat Protection (Capture ATP) is a cloud-based feature that analyzes files and determines if the file is malicious or acceptable. Capture ATP inspects files of up to 10MB, and is able to block threats before they can do any damage. All files submitted to Capture ATP are preprocessed before analysis, and separated in three categories. Malicious files are quarantined, while acceptable files are delivered directly to the client. If preprocessing determines a file to be malicious or acceptable, the file is not further analyzed by Capture ATP. Only the third category, those whose status cannot be immediately determined, are submitted to Capture ATP for complete analysis. Until this complete analysis is performed, Capture ATP works on the basis of Block Until Verdict if this option is selected. With Block Until Verdict, no files are delivered to the client before they pass rigorous analysis and are determined to be acceptable.

A streamlining feature called MD5 Hash Exclusion lists allows you to upload an MD5 hash and compare it with the SonicWall database of specified hash exclusions. This can speed up the analysis of files that are similar or the same as files that have recently been received for analysis.

Capture ATP supports many configurations of file types (archive files, executable files, Microsoft Office, Microsoft Office Extended , or PDF files). In order to expedite the process, the user has the possibility of excluding certain known files from file inspection, and either allow them or block them automatically.

① | **NOTE:** Wireless Network Manager supports the HTTP, SMTP, and FTP protocols.

For more information about Capture ATP, see the latest SonicOS *Security Configuration* administration documentation available under the product name Secure Wireless Access on the SonicWall support website at: <https://www.sonicwall.com/support/technical-documentation/>.

Topics:

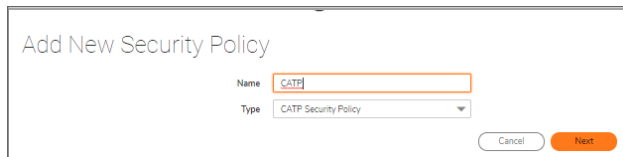
- [Creating Capture Advanced Threat Protection Security Policies](#)
- [Adding an MD5 Hash to the Exclusion List](#)

Creating Capture Advanced Threat Protection Security Policies

In order to take advantage of Capture Advanced Threat Protection (CATP or Capture ATP), create Capture ATP security policies as described below and select the categories of files you want to block. Once you have created a policy, apply it to an SSID group as explained in [Applying a Security Policy to an SSID Group](#).

To create a Capture ATP security policy:

1. Navigate to **Security > Security Policies**.
2. Click **Add +** to add a new security policy. The **Add New Security Policy** page displays.
3. Enter the name of the policy.
4. From the **Policy Type** list, select **CATP Security Policy**.
5. Click **Next**. The **Details** page displays. The name of the policy you created is filled in the top field.



6. Click **Enable** to enable the Capture ATP policy you have selected. Unselect it to disable the policy.
7. Choose the **Schedule** from the dropdown list.
8. Click the **Block Until Verdict** to enable to decide whether questionable files should be allowed to pass. If you are not concerned about their safety, you can allow them. If you do not want to take the chance of their being dangerous, select **Block Until Verdict**.
9. Optionally, you can set a **Maximum File Size**. The default maximum size is 10240 bytes. For SonicWave 231c/224w/231o models, the maximum size will reduce to 5120KB due to limited memory."

The following table shows the maximum size supported on the models:

Models	Maximum size
SonicWave231c/231o/224w	5,120 KB
SonicWave432i/432e/432o	10,240 KB
SonicWave621	1,024 KB
SonicWave641/681	10,240 KB

10. You can set the acceptable files types by checking any of the **File Types** boxes.

11. Select the protocol(s) which you want to use.
12. Click **OK** to save your selections.

The policy is now listed on the **Security > Security Policies** page.

Adding an MD5 Hash to the Exclusion List

To add an MD5 hash to the exclusion list for a CATP policy:

1. Navigate to **Security > Security Policies**.
2. Click **Edit/Config** next to the CATP policy. The **Edit Security Policy** screen displays.

3. In the **MD5 Exclusion List** section at the bottom of the screen, click the **+** icon. The policy-specific **Edit Security Policy** screen appears, allowing you to add an MD5 Hash to the MD5 Exclusion List.
4. Type the 32-digit hexadecimal number in the **MD5 Hash** field.

5. Click **Add**.
6. Click **OK**.

The MD5 hash is added to the **MD5 Exclusion List**.

Cloud Anti-Virus

Cloud Anti-Virus (Cloud AV) is an advanced feature of Wireless Network Manager. This cloud-based anti-virus service provides real-time file virus scanning and reporting without consuming local computing resources. Multi-Engine Cloud AV is supported on the SonicWave appliance. Once you have created Cloud AV security policies, you can add them to an SSID group by following the steps in [Applying a Security Policy to an SSID Group](#).

To create a new Cloud AV policy:

1. Navigate to **Security > Security Policies**.
2. Click **Add +**. The first **Add New Security Policy** displays.
3. In the **Name** field, enter the name of the security policy you want to add.
4. From the **Type** list, select **Cloud-AV Security Policy**.
5. Click **Next**.
6. When the second **Add New Security Policy** screen displays, click **Enable** to enable the security policy you created.

Access Control Policies

Access Control Policies (ACL) manage access to MAC Address Objects and Access Object groups. Once you have created and configured the security policy, you can apply it to an SSID group as explained in [Applying a Security Policy to an SSID Group](#).

Topics:

- [Creating Mac Address Objects](#)
- [Creating Address Object Groups](#)
- [Creating and Editing Access Control Policies](#)

Creating and Editing Access Control Policies

Create or edit Access Control Policies (ACLs) to allow or deny access to address objects or address groups.

To create or edit an access control policy:

1. Navigate to **Security > Security Policies**.
2. Click **Add +** or **Config/Edit**. The **Add/Edit New Security Policy** page displays.
3. Enter an **ACL Policy Name**.
4. From the **Type** list, select **ACL Security Policy**.
5. Click **Next**. The **Add/Edit New Security Policy** screen displays.
6. Click **Enable** to enable the access control security policy.
7. In the **ACL** section, Select **Deny** or **Allow** from the mode menu.
8. From the **Address Group** list, select an address group or create an address object group from the **Security > Security Objects** page. For more information, refer to [Applying a Security Policy to an SSID Group](#).
9. In the **Bandwidth Management** section, click **Enable** to enable bandwidth management.
10. Configure the other fields in the section.

11. Be sure **All Clients** is disabled, so that you can apply this new policy to a group of SSIDs.
12. Select the **Client IP Group** on the field that appears when you disable **All Clients**.
13. For the **Client IP Group**, select a new ACL security object .
14. Click **OK** to apply the changes.
15. Navigate to **Policies > SSID Policies**.
16. Click **+ Add** on the end of the row SSID for **Default SSID Group**. The **Add SSID for Default SSID Group** screen displays.
17. Click **Security Policy**.
18. Choose the policy you want applied from the drop down list.
19. Click **OK** to apply the ACL policy.

The ACL policy is configured and added to the list.

Creating Mac Address Objects

To create a MAC address object:

1. Navigate to **Security > Address Objects**

NAME	DETAILS	TYPE	REFERENCE	DESCRIPTION
pc_mac	add:07:af:5a:0a:0a:07	MAC	*Network Policy: *SSID Profile:	the mac of pc
ipv4_win10_pc	10.10.10.10	HOST	*Network Policy: *SSID Profile:	ip address of win10 pc
phone_mac	02:00:0c:00:00:00	MAC	*Network Policy: *SSID Profile:	

2. Click **Add +**. The **Add Address Object** screen displays.

NAME	DETAILS	TYPE	REFERENCE	DESCRIPTION
pc_mac	add:07:af:5a:0a:0a:07	MAC	*Network Policy: *SSID Profile:	the mac of pc
ipv4_win10_pc	10.10.10.10	HOST	*Network Policy: *SSID Profile:	ip address of win10 pc
phone_mac	02:00:0c:00:00:00	MAC	*Network Policy: *SSID Profile:	

3. Enter a **Name** for the address object.
4. Enter a **Description** for the address object.
5. From the **Type** list, select **MAC**.

6. Enter the **MAC Address** for the address object.
7. Click **OK**.

The MAC address is added to the **Address Objects** list.

Address Objects

The **Security > Address Objects** page provides options for creating or editing security objects. The objects can be edited as:

- **Address Objects**
- **Address Groups**

The **Address Objects** page displays a list of address objects with their applied security policies, where you can configure or delete object.

NAME	DETAILS	TYPE	REFERENCE	DESCRIPTION
☐ pc_mac	d0:37:45:6a:0c:b7	MAC	*Network Policy: *SSID Profile:	the mac of pc
☐ ipv4_win10_pc	10.103.50.186	HOST	*Network Policy: *SSID Profile:	ip address of win10 pc
☐ phone_mac	12:3e:76:50:28:af	MAC	*Network Policy: *SSID Profile:	

Creating Address Object Groups

To create an address object groups:

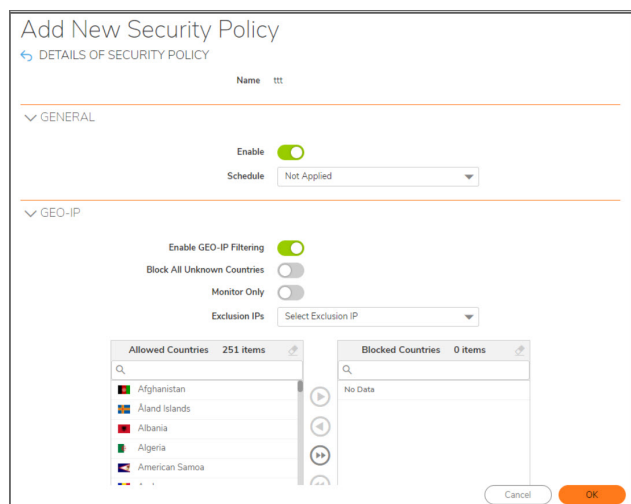
1. Navigate to **Security > Address Groups**.
2. Click **Add +**. The **Add Address Group** page displays.

3. On this screen, you can choose the settings for the group.
Fill in the group name and description, then add or remove settings by moving them left or right.
4. Click **OK** to add the address group.

The Address Group is added to the list.

Geo-IP & Botnet

These two security features provide extra safety by allowing you to choose specific countries to block, or to block attacks from Botnets. These are networks of compromised computers transmitting malware, spam, or other destructive files. Each of these features need separate licenses, available from [MySonicWall](#).



The bottom two sections of the **Add New Security Policy** page give you the option of enabling Geo-IP and/or Botnet blocking on this policy.

1. Fill in your GEO-IP and Botnet choices, including any IPs you wish to exclude from the ban.
2. Click **OK** to apply the selections you have made.

Application Control

Application awareness is crucial to application control, which is an important feature of modern firewall systems. There are types of applications that Wireless Network Manager can detect include:

- application protocols: such as FTP and SSH, which represent communications between hosts
- clients: such as web browsers and email clients, which represent software running on the host
- web applications: such as MPEG video and Facebook, which represent the content or requested URL for HTTP traffic

Wireless Network Manager allows SonicWave access points to detect applications and control their activities on your network. Wireless Network Manager identifies applications in network traffic according to the characteristics specified in the detector. For example, the system can identify an application by an ASCII pattern in the packet header.

Topics:

- App Objects
- APP Control

Schedule Objects

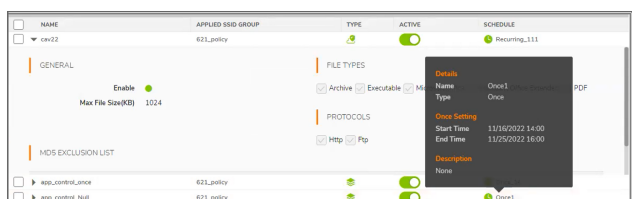
Scheduling device activation or deactivation and other processes can automate some of the administrator's tasks.

NAME	TYPE	DAYS OF WEEK	TIME	START TIME	END TIME	REFERENCE	DESCRIPTION
Recurring_9-14	Recurring					*SSID Groups: *Security Policies: catp	
Recurring	Recurring					*SSID Groups: *Security Policies: Copy of app_control...	
test_mixed	Mixed			11/16/2022 10:30	12/16/2022 11:00	*SSID Groups: *Security Policies: catp_mixed, GeolP_mi...	
Mixed	Mixed			12/07/2022 09:00	12/08/2022 16:00	*SSID Groups: *Security Policies: app_control_mixed, ca...	
Once1	Once			11/16/2022 14:00	12/13/2022 16:00	*SSID Groups: *Security Policies: cfs_once11	
Schedule_Recurrin	Recurring					*SSID Groups: *Security Policies:	
Once_out	Once			11/10/2022 10:00	12/08/2022 15:31	*SSID Groups: *Security Policies:	

To schedule device activation or deactivation and other processes:

1. Navigate to **Security > Schedule Objects**.
2. Click **Config/Edit** (on the schedule row). You can set a schedule for the VAP (Virtual Access Point) on the SonicWave appliance to become activated or deactivated.
3. Click **Add +** top right to create a Schedule Object.
4. On the first **Add Schedule Object** screen, select the details of your new schedule object.
5. On the next **Add Schedule Object** screen, click **Add +** to select schedule information .
6. In the **Time** section, drag the selections along the time bar to choose the start and end times.
7. Click **OK** to apply your settings
8. Click **OK** again to return to the **Schedule Objects** list.
9. Go to **SSID Settings** and select the schedule object you created.
10. Apply this SSID to the SonicWave appliance you wish to configure.

The security policy becomes activated or deactivated in the SonicWave appliance according to the selected schedule.



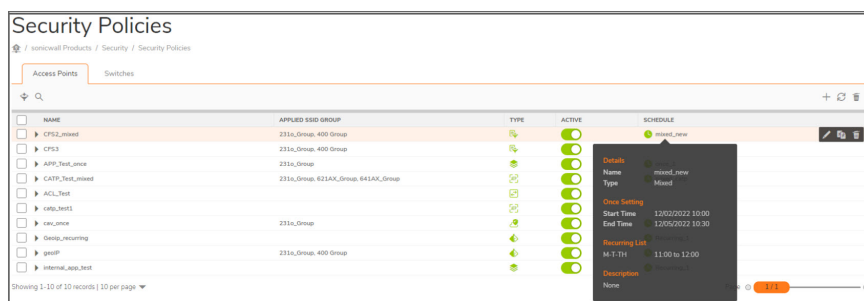
Scheduling VAP Security Policy

Scheduling VAP Security Policy activation or deactivation and other processes can automate some of the administrator's tasks. VAP Security Policy Schedule is a function that schedule the corresponding security policy at a specified time or periodically.

- **Security Policy:** CFS, CATP, CAV, APP Control, GeoIP_Botnet.
- **Schedule mode:** Once Schedule Mode, Recurring Schedule Mode, Mixed Schedule Mode.

To schedule VAP security policy activation or deactivation :

1. Navigate to **Security > Schedule Objects**.
2. Click **Config/Edit** (on the schedule row). You can set a schedule for the VAP Security Policies on the SonicWave appliance to become activated or deactivated.
3. Click **Add +** top right to create a Schedule Object.
4. On the first **Add Schedule Object** screen, select the details of your new schedule object.
5. On the next **Add Schedule Object** screen, click **Add +** to setting schedule information .
6. In the **Time** section, drag the selections along the time bar to choose the start and end times.
7. Click **OK** to apply your settings
8. Click **OK** again to return to the **Schedule Objects** list.
9. Go to **Security Policies**, apply the schedule object you created to the security policies [including CFS, CATP, CAV, App Control, Geoip_Botnet policy]



10. Go to **SSID Settings** and apply the security policies you created to SSID profile.

Edit CFS_Test_1 for 641AX_Group

General
Advanced
Security Policy
Guest Portal

CFS Policy

CATP Policy

CAV Policy

ACL Policy

GeolP-Botnet Policy

APP Control Policy

CFS2_mixed
Not Applied
CFS2_mixed
CFS3
Not Applied
Not Applied
Not Applied
Not Applied

11. Apply this SSID to the SonicWave appliance you wish to configure.
- Schedule the corresponding security policy at a specified time OR periodically.
- The security policy becomes activated or deactivated in the SonicWave appliance according to the selected schedule.

App Objects

The **Security > App Objects** page provides options for creating or editing application objects.

The **App Objects** tab displays the available application objects

App Objects

WNM4.1
Security
App Objects

App Objects
App Group

Columns

CATEGORY	NAME	APPLIED SECURITY POLICIES	DESCRIPTION
▶ app-protocols			
▶ file-transfer			
▶ mail			
▶ messaging			
▶ social-media			
▶ media-streaming			
▶ uncategorized			

Showing 1-7 of 7 records | 10 per page
Page 1/1

App Group

The **App Group** tab displays the available application groups. You can also create, modify, and delete on this tab.

App Objects

App Group

+

•

Columns

☐	NAME	CATEGORY	TYPE	APPLIED SECURITY POLICIES	DESCRIPTION
☐	▶ app_test_group		GROUP	app_control_Recurring	
☐	▶ app_group2		GROUP	Copy of app_control_Re,	
☐	▶ app_group11		GROUP	app_control_mixed	

Showing 1-3 of 3 records | 10 per page

Page

1 / 1

To create a new App Group:

1. Navigate to **Security > App Objects**.
2. Click the **App Group** tab.
3. Click Add (+). The **Add App Group** dialog displays.

ADD APP GROUP

Group Name

Internal Apps

Description

Testing Internal Apps

view category: Select Category ▼

SSH

FTP

DNP3

MODBUS

IMAP

add

remove

view category: file-transfer ▼

SMTP

Cancel

OK

4. Specify a group name and description.
5. From the list, select **app-protocols**.
6. In list on the left, select the protocols you want included in your new App Group.
7. Click **Add**.
8. Click **OK**.
9. Add a schedule object in **WNM schedule objects** page.

Add New Security Policy

← DETAILS OF SECURITY POLICY

Name: internal_app_test

GENERAL

Enable: ☒

Schedule: Recurring_1

APP RULES

#	GROUP	ACTION	DIRECTION	DOWN RATE	UP RATE
1	internal app	block			

Total: 1 item(s)

Cancel OK

- Go to **Security Policies** Page, open the App Control policy you need to edit, and apply schedule.

Edit 641_App_Control_1 for 641AX_Group

General Advanced **Security Policy** Guest Portal

CFS Policy: Not Applied

CATP Policy: Not Applied

CAV Policy: Not Applied

ACL Policy: Not Applied

GeoIP-Botnet Policy: Not Applied

APP Control Policy: internal_app_test

Not Applied
APP_Test_once
✓ internal_app_test

Cancel Save

- Go to **SSID Policies**, apply the app control policy created in the above step to SSID profile.

Admin

Topics:

- [Reports](#)
- [Users](#)
- [Settings](#)
- [Certificates](#)

Reports

The administrator can generate reports by navigating to the **Admin > Reports** page. Reports can be formatted and delivered as PDF documents.

Topics:

- [Generating Report Tasks](#)
- [General Settings](#)

Generating Report Tasks

REPORT TASKS							
GENERAL SETTINGS							
+ Create Report Task							
#	REPORT ID	REPORT NAME	TYPE	REQUESTED AT	REPORT GENERATE...	STATUS	
☐	1	62ce816614b9df68712f2abc	99	On-Demand	Wed Jul 13 2022 13:55:10 GMT+0530	Mon Jul 18 2022 15:30:18 GMT+0530	Ready
☐	2	62ce813114b9df68712f2abb	88	On-Demand	Wed Jul 13 2022 13:54:17 GMT+0530	Wed Jul 13 2022 13:54:22 GMT+0530	Ready
☐	3	62ce812214b9df68712f2aba	77	On-Demand	Wed Jul 13 2022 13:54:02 GMT+0530	Wed Jul 13 2022 13:54:08 GMT+0530	Ready
☐	4	62ce806e14b9df68712f2ab9	66	On-Demand	Wed Jul 13 2022 13:51:02 GMT+0530	Wed Jul 13 2022 13:51:08 GMT+0530	Ready
☐	5	62ce805e345a577ab099c1f6	55	On-Demand	Wed Jul 13 2022 13:50:46 GMT+0530	Wed Jul 13 2022 13:50:51 GMT+0530	Ready
☐	6	62ce804d345a577ab099c1f5	44	On-Demand	Wed Jul 13 2022 13:50:29 GMT+0530	Wed Jul 13 2022 13:50:38 GMT+0530	Ready
☐	7	62ce8031345a577ab099c1f4	33	On-Demand	Wed Jul 13 2022 13:50:01 GMT+0530	Wed Jul 13 2022 13:50:08 GMT+0530	Ready
☐	8	62ce801e345a577ab099c1f3	22	On-Demand	Wed Jul 13 2022 13:49:42 GMT+0530	Wed Jul 13 2022 13:49:48 GMT+0530	Ready
☐	9	62ce8000345a577ab099c1f2	11	On-Demand	Wed Jul 13 2022 13:49:12 GMT+0530	Wed Jul 13 2022 13:49:22 GMT+0530	Ready

To generate a report:

1. Navigate to **Admin > Reports > REPORT TASKS**.
 2. Click the icon **Create Report Task**.
 3. Enter the **Report Name**.
 4. Choose the Report Type as
 - **On-demand Report** - When selected this option, you need to choose the options from the Interval as last 24 hours, 7 days, 30 days.
 - **Scheduled Report** - When selected this option, you can set a time for the reports to be generated. You can have reported sent via email in addition to being able to download them from Wireless Network Manager.
- Choose **Frequency**, **Time** and **Scheduled On time**.

Create Report Task

CONFIGURATION

Report Name

Report

Report Type

☐ On-demand Report
 ☒ Schedule Report

Frequency

Week

Time

9 : 30

☐ Scheduled On

Tuesday

Send Report By Email

☒

BCC To Email address

johnsmith@gmail.com

+ Add Email Address

CONTENT

☒ Executive Summary
 ☒ Recommendations
 ☒ Statistics

☒ Security (Client Security Service Details)
 ☒ Inventory
 ☒ Topology

Cancel

OK

5. Click the toggle to enable or disable to **Send Report By Email** to activate sending the report by email.
6. In the **BCC To Email address** field, enter the email address to which you want the reports to be sent.
7. To send the report to additional email addresses:
 - Click the plus sign (+) next to **Add Email Address**.
 - Enter the email address to which you want the reports to be sent.Repeat these steps to send the report to additional email addresses.
Click the **X** next to an email address to remove it from the list.
8. From the **CONTENT** section, select the information to be included in the reports to be generated. Each report can be configured differently by making different selections on this screen.
9. Click **OK**.

General Settings

REPORT TASKS GENERAL SETTINGS

BASIC INFO

Prepared For test_report_scheduled

Location Millpitas

Prepared By John

Contact Phone Number 13525357311

Contact Email Address johnsmith@gmail.com

REPORT LOGO

Please select file to upload

Save

To configure the settings:

1. Navigate to **Admin > Reports > GENERAL SETTINGS**.
2. Fill in the fields on the screen for:
 - **Prepared for**
 - **Location**
 - **Prepared By**
 - **Contact Phone Number**

- **Contact Email Address**
3. Upload a logo to be displayed in the PDF report.
 4. Click Save icon on the top right or click **Save**.

Users

The **Users** page displays a list of all of the current users. There are columns for

- **Name**
- **Type**
- **Description**
- **Created at**
- **Expire Time**
- **Quota**

NAME	TYPE	DESCRIPTION	CREATED AT	EXPIRE TIME	QUOTA
test	Guest		2022-10-28 14:35:40	Never	
test1	Guest	per_day	2022-10-27 14:50:08	Never	
test3	Guest	per_month	2022-10-27 15:35:23	Never	
test2	Guest	per_week	2022-11-01 10:49:05	Never	
test5	Guest		2022-12-05 14:27:29	Never	
wmao@comcast.com	Admin		2019-10-22 13:43:13	Never	

You can **Edit** or **Delete** the user from the icons on the right end of the row.

Configuring User Quota Control

The user quota control feature provides quota control based on the user's account. The quota can be specified as a session lifetime, or a transmit and/or receive traffic limit. With a cyclic quota, a user can not access the Internet upon meeting the account quota until the next cycle (day, week, or month) begins. If the quota cycle is Non Cyclic, the user is unable to access the Internet upon meeting the quota.

ADD USER

Name: John Smith

Description: Sonicwall Guest User

Password: ••••••••

Quota Cycle Type Setting: Non Cyclic

Session Lifetime (0 to disable): 60 Minutes

Receive limit (0 to disable): 10000 MB

Transmit limit (0 to disable): 10000 MB

Never Expire: ☒

Cancel OK

To configure the quota for the user:

1. Navigate to **Admin > Users**. Select Accounts
2. Click add icon on the right view of the screen.
3. Enter the details of the user
 - **Name** - Enter the name of the user.
 - **Description** - Enter a description (not mandatory)
 - **Password** - Set a password.
 - **Quota Cycle Type Setting** - From the Quota cycle type setting list, select:
 - Non Cyclic (default)
 - Per Day
 - Per Week
 - Per Month
 - **Session Lifetime (0 to disable)** - Specify the duration for how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account.
 - **Receive Limit (0 to disable)** - Enter the amount (in MB) the amount of data the user can receive. The range is from 0 (no data can be received) to 9999 MB to Unlimited (default).
 - **Transmit Limit (0 to disable)** - Enter the amount (in MB) of data the user can send. The range is from 0 (no data can be sent) to 9999 MB to Unlimited (default).
 - **Never Expire** - Toggle on or off to set to never expire.
 - Click **OK**.

Settings

The Settings page provides an option for upgrading SonicWave access point firmware and syncing with MySonicWall.

Topics:

- [General](#)
- [Firmware](#)
- [Notification Center](#)

General

On the **General** page, administrators can fill in **Syncing** and **Firmware** information.

The screenshot shows the 'General' settings page in the 'WiFi Cloud Manager'. The page is divided into three main sections: 'SYNCING', 'TWILIO SMS SETTING', and 'TIME SETTING'. In the 'SYNCING' section, there is a 'Sync with MySonicWall' label and a 'Start Syncing' button. The 'TWILIO SMS SETTING' section contains three input fields: 'Account Sid' (with a sample value), 'Auth Token' (with a sample value), and 'Twilio Phone Number' (with a sample value). The 'TIME SETTING' section has a 'Time Zone' dropdown menu with 'Calcutta, Chennai, Mumbai, New ...' as the selected option. A 'Save' button is located at the bottom right of the page.

The **Syncing** section provides a **Start Syncing** button that initiates syncing with MySonicWall. You might need to do this if you have been making changes to your hierarchy or devices. Check the box next to the firmware on your tool. There is a choice on the right side of the screen for upgrading, if required.

Client Timezone

Administrators can configure the time zone for their connected devices. When the administrator first logs in, the default time zone is set based on the information in their [MySonicWall](#) account. In Wireless Network Manager 4.3, administrators can set the time based on their needs.

To set the timezone:

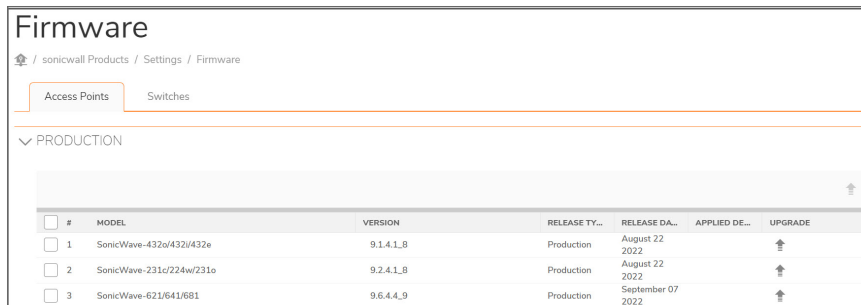
1. Navigate to the **Settings > General** page.
2. In the **Time Setting** section, select the time zone you want from the **Time Zone** list.

3. Click **Save** to save the changed settings.

After setting the time zone, when the administrator exports the log file or receives any notification emails, the time will be displayed according to their time zone setting.

Firmware

Administrators can selectively upgrade specific devices in order to install firmware upgrades or patches within their environment.



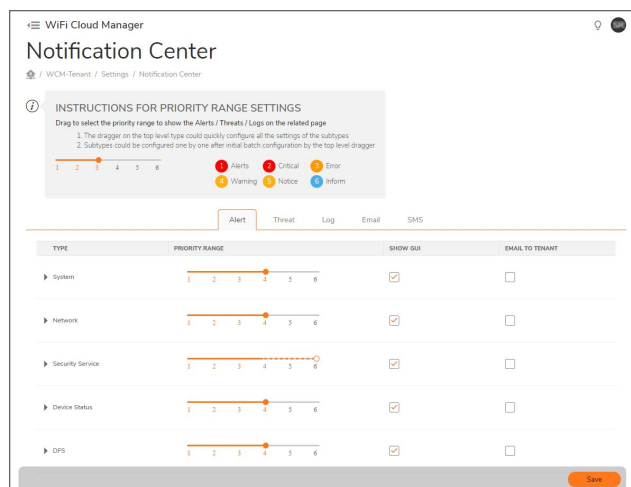
#	MODEL	VERSION	RELEASE TY...	RELEASE DA...	APPLIED DE...	UPGRADE
1	SonicWave-432e/432i/432e	9.1.4.1_8	Production	August 22 2022		⬆
2	SonicWave-231c/224w/231e	9.2.4.1_8	Production	August 22 2022		⬆
3	SonicWave-621/641/681	9.6.4.4_9	Production	September 07 2022		⬆

To update the firmware:

1. Navigate to the **Settings > Firmware** page.
2. In the **Upgrade** column, select the icon to upgrade the device.
3. When the **Upgrade command sent to online access points message** displays, click **OK**.

Notification Center

The **Notification Center** page provides Wireless Network Manager administrators with options for filtering the information they receive.



Clicking on these options display pages where you can make selections concerning notifications:

- **Alert**
- **Threat**
- **Log**
- **Email**
- **SMS**

Within these **Types** are several subtypes that can be brought up by expanding the main type. These pages have an easy-to-use interface for setting priorities for each of the related screens. The dragger makes it easy to select the desired priority for each event, since they can be set both as a batch and individually. Instructions for the use of this tool are on the screen.

- The **Alert** page has a table to select each **Type** of alert put out by Wireless Network Manager:
 - **Priority Range**
 - **Show GUI**
 - **Email to Tenant**

The **Types** are set in groups:

- **System**
- **Network**
- **Security Service** (which includes **CFS**, **Capture ATP**, **Cloud AV**, **GeoIP**, **Botnet**, **App Control**.)
- **Device Status**
- **DFS**
- **Switch** (which includes **CLI**, **Web**, **System**, **LBD**, **RESTful**, **POE**.)

- The **Threat** page has types for WIDP (Wireless Intrusion Detection & Prevention):
 - **WIDP**
 - **Security Service**
- The **Log** page shows several choices for the **Type** of log notifications available. They are:
 - **System**
 - **802.11**
 - **802.1X**
 - **WPA**
 - **DFS**
 - **RRM (Radio Resource Management)**
 - **User Authentication**
 - **Network**
 - **BLE (Bluetooth Low Energy)**
 - **Mesh**
 - **Cloud Management**
 - **Audit**
 - **Switch**
- The **Email** page displays the frequency of the notifications and a list of the email addresses where copies should be sent.

The screenshot shows the 'Notification Center' interface in the 'WiFi Cloud Manager'. The breadcrumb trail is 'WCM-Tenant / Settings / Notification Center'. There is an informational box titled 'INSTRUCTIONS FOR PRIORITY RANGE SETTINGS' with a drag slider and three priority levels: 1. Error (red), 2. Warning (yellow), and 3. Notice (blue). Below this, there are tabs for 'Alert', 'Threat', 'Log', 'Email' (which is selected), and 'SMS'. The 'Email' tab contains the 'EMAIL LOG AUTOMATION' section. It includes a 'Frequency' dropdown set to 'Weekly', an 'Every' dropdown set to 'Sunday', and a time field set to '16 : 00'. There is a text input field for 'Cc notification to email address' and a '+ Add Email Address' button. A 'Save' button is located at the bottom right of the page.

These can be determined by the administrator, and changed at any time.

SMS Event Notifications

You can receive notifications via SMS when certain events occur.

To activate SMS notifications:

1. If you have done so already, set up your [Configuring Twilio Billing for SMS](#).
2. Navigate to **Settings > Notifications Center**.
3. In the **SMS Settings** section, enter the telephone number to which the SMS notifications should be sent.
4. In the Events section, select the events for which you want SMS notifications. The available events include:
 - **Cpu High Utility**
 - **Memory High Utility**
 - **Radar Detection**
 - **Firmware Upgrade**
 - **Device On/Offline**
 - **Device License Expired**
 - **WIDP KRACK**
5. Click **Save**.

Wireless Guest TOTP Authentication

The Time-Based One Time Password is a multi-factor authentication scheme that enabled third party integration to generate secure time-based OTP via third party authentication Apps such as Google authenticator, Microsoft authenticator etc.

TOTP is an alternative to traditional two-factor authentication methods. TOTP passwords keep on changing and are valid for only short window in time, because of which TOTP is considered more secure OTP solution. Before logging into guest authentication, you need to make sure to have an active internet service to view the code in the application.

To add Totp User:

1. Navigate to **Admin > Users**. Select **Time-based-One-time-Password**.
2. Click  add icon on the right view of the screen.
3. Enter the details of the user
 - **Name** - Enter the name of the user.
 - **Description** - Enter a description (not mandatory)
 - **Quota Cycle Type Setting** - From the Quota cycle type setting list, select:
 - Non Cyclic (default)
 - Per Day

- Per Week
- Per Month
- **Session Lifetime (0 to disable)** - Specify the duration for how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account.
- **Receive Limit (0 to disable)** - Enter the amount (in MB) the amount of data the user can receive. The range is from 0 (no data can be received) to 9999 MB to Unlimited (default).
- **Transmit Limit (0 to disable)** - Enter the amount (in MB) of data the user can send. The range is from 0 (no data can be sent) to 9999 MB to Unlimited (default).
- **Never Expire** - Toggle on or off to set to never expire.
- Click **OK**.

To generate Totp User:

1. Navigate to **Admin > Users**. Select **Time-based-One-time-Password**.
2. Click  add icon on the right view of the screen.
3. Enter the details of the user
 - **User Name Prefix** - Enter the username.
 - **Number of Accounts** - Specify the number of accounts (in numbers).
 - **Quota Cycle Type Setting** - From the Quota cycle type setting list, select:
 - Non Cyclic (default)
 - Per Day
 - Per Week
 - Per Month
 - **Session Lifetime (0 to disable)** - Specify the duration for how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The field cannot exceed 4 characters.
 - **Receive Limit (0 to disable)** - Enter the amount (in MB) the amount of data the user can receive. The range is from 0 (unlimited) to 999999999 MB to maximum (the field cannot exceed 9 characters)
 - **Transmit Limit (0 to disable)** - Enter the amount (in MB) the amount of data the user can receive. The range is from 0 (unlimited) to 999999999 MB to maximum (the field cannot exceed 9 characters)

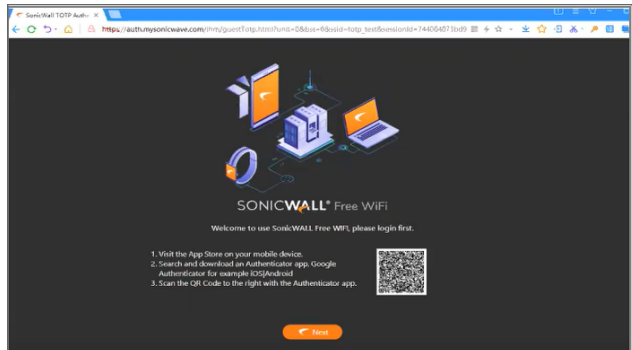
- **Backup Generated Users to Email** - Enter an email address to receive the code. Please note that an active internet connection is needed to receive the code.
- Click **OK**.

To delete Totp User:

1. Navigate to **Admin > Users**. Select **Time-based-One-time-Password**.
2. Check the box of the user to delete.
3. Click **Delete Totp User** icon.

User Authentication through Totp

When the user log in for the first time, a QR code is displayed on the screen. You need to install an authenticator app like Google Authenticator to scan the QR code.



Once the QR code is scanned, it displays a unique code on your phone screen. Enter the 6 digit code to login.

For the subsequent logins, you can specify the username and login to the guest portal.

- ① **NOTE:** To reconnect using the wireless connection again, you need to enter the 6 digit code through the splash screen to login.

Certificates

Topics:

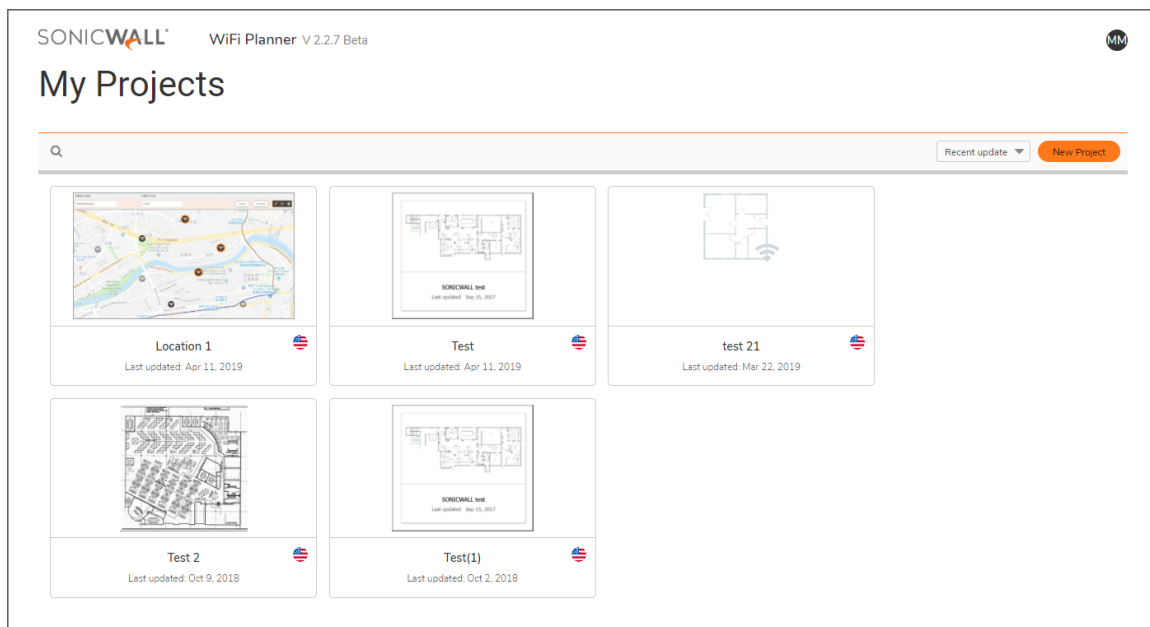
- [Certificate for Guest Portal SAML Authentication](#)

Certificate for Guest Portal SAML Authentication

Wireless Network Manager supports the use of the certificates for Active Directory (AD) and Guest Portal SAML authentication.

Using the WiFi Planner

WiFi Planner is in the **Tools** section at the bottom of the navigation pane. Click on **WiFi Planner** to access the login for the tool.



After using Wireless Network Manager to configure your network hierarchy, policies, and SSIDs as described in the *Wireless Network Manager Getting Started Guide* and the other sections in this guide, use the WiFi Planner to determine optimal SonicWave access point placement. WiFi Planner simulates deployment with SonicWall wireless products in your Wireless Network Manager zones. You can

- create and configure new projects and floor plans
- upload, scale, and manage existing floor plans
- include or exclude specific areas from Wi-Fi coverage

WiFi Planner can also be used to plan and configure access point deployment for security networks managed by a SonicWall network security appliance.

For more information about the WiFi Planner, refer to the *WiFi Planner User Guide*. The *Wireless Network Manager Getting Started Guide*, the *WiFi Planner User Guide*, and other documentation are available under the product name “Secure Cloud Wireless” on the SonicWall support website:

<https://www.sonicwall.com/support/technical-documentation/>.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

About This Document

Wireless Network Manager Administration Guide
Updated - May 2023
232-005776-00 Rev E

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035